Journal of Algebra and Its Applications
Vol. 7, No. 5 (2008) 647–662

ON GROUP FACTORIZATIONS USING FREE MAPPINGS

VLADIMIR BOŽOVIĆ* and NICOLA PACE†

Department of Mathematical Sciences
Florida Atlantic University, 777 Glades Road
Boca Raton, Florida 33431, USA
**vladobozovic@yahoo.com*
†npace@fau.edu

Received 5 March 2008
Accepted 29 April 2008

Communicated by I. M. Isaacs

We say that a collection of subsets $\alpha = [B_1, \ldots, B_k]$ of a group G is a *factorization* if $G = B_1, \ldots, B_k$ and each element of G is expressed in a unique way in this product. By using a special type of mappings between groups A and B, called *free mappings*, we exhibit an algorithmic way to construct nontrivial factorizations of a group G, such that $G \cong A \times B$. In Lemma 3.2 we give a simple way to construct free mappings. It turns out that this approach has greater importance when G is an abelian group. We give illustrative examples of this method in the cases $\mathbb{Z}_p \times \mathbb{Z}_p$ and $\mathbb{Z}_p \times \mathbb{Z}_q$ where p and q are different prime numbers. An interesting connection between free mappings and Rédei's theorem, with a number theoretic implication, is given.

Keywords: Group factorizations; free mappings; factoring finite groups by subsets; transformations of factorizations; factorizations of direct products.

1. Introduction

In the mathematical literature one finds two different approaches to defining *group factorizations*, depending on whether a group G is abelian or nonabelian. In the case of an abelian group G, a *factorization* is a collection of subsets $\alpha = [B_1, \ldots, B_k]$ such that every element $g \in G$ has a unique representation $g = s_1 s_2 \cdots s_k$, where $s_i \in B_i$ for $1 \leq i \leq k$. The subsets B_i, $1 \leq i \leq k$ of G are called the *blocks* of the factorization. In the nonabelian case, the term *factorization* has frequently been reserved for the case where the blocks are subgroups of the group G. However, there exists the notion of a *logarithmic signature*, given in [4] for an arbitrary group G, that completely agrees with the meaning of factorization in the abelian case. In this paper, we will use a unified definition of *group factorization* for both the abelian and nonabelian case. It should be emphasized that the theory of group factorizations is much more developed in the abelian case. To the best of our knowledge, there are just a few papers that treat factorizations of nonabelian groups where the blocks are considered more generally as sets, rather than subgroups, for example [4, 5]. On the other hand, much work has been done when the blocks are subgroups, see for instance [3].

In the abelian case, another term for factorization is *tiling*. This evokes the connection to combinatorics and geometry. Indeed, about 1900, Minkowski conjectured that:

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, 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 sublattice, connects the vast field of tilings and abelian groups. In general, factorization questions are relevant to the theory of numbers, tilings, packings and covering problems.

On the other hand, "group factorizations" is a topic that, besides its theoretical beauty, has practical use in graph theory, coding theory, number theory and modern cryptography. Group factorizations are the main tool for cryptosystems such as PGM and MST1. Therefore, finding new ways of factorization is both of great theoretical and practical interest.

In our paper, we obtain factorizations of groups of the form $A \times B$, where A and B are groups. Our approach relies on the construction of a pair of mappings between A and B given in Lemma 3.2. Although there are no restrictions on the groups A and B, it turns out that there is a greater significance of this approach in the case where A and B are abelian groups. In Sec. 2, we give an overview of the existing results that are important for our work. In Sec. 3, the concept of *free mappings* is introduced and a basic tool is given for constructing new factorizations. Section 4 is treating the abelian case, with particular emphasis on the illustrative cases $\mathbb{Z}_p \times \mathbb{Z}_p$ and $\mathbb{Z}_p \times \mathbb{Z}_q$ where p and q are different prime numbers. An interesting connection between free mappings and Rédei's theorem, with a number theoretic implication, is given.

2. Basic Definitions and Preliminaries

Definition 2.1. We say that a collection of subsets $\alpha = [B_1, B_2, \ldots, B_k]$ is a *factorization* of a group G if $G = B_1 B_2 \cdots B_k$ and every $g \in G$ has the unique factorization $g = s_1 s_2 \cdots s_k$, $s_i \in B_i$, $1 \leq i \leq k$. We call the subsets B_i, the *blocks* of factorization α. The factorization is called *normalized* if each block B_i contains the identity element. When G is a finite group then we say that the *type* of α is $(r_1, r_2, \ldots, r_k)$, where $|B_i| = r_i$ for $1 \leq i \leq k$.

A factorization $\alpha = [B_1, B_2, \ldots, B_k]$ of a group G is said to be *proper* if $|B_i| \neq 1$ and $B_i \neq G$, for every i, $1 \leq i \leq k$. First, we present a result that gives a necessary and sufficient condition for the collection of sets $\alpha = [S, T]$ to be a factorization of group G.

Theorem 2.1. *Let S, T be subsets of G. Then $\alpha = [S, T]$ is a factorization of G if and only if $G = ST$ and $(S^{-1}S) \cap (TT^{-1}) = \{e\}$.*

Proof. Let $\alpha = [S, T]$ be a factorization of G. From the definition, it follows that $G = ST$. Let $g \in (S^{-1}S) \cap (TT^{-1})$. Then, $g = s_2^{-1}s_1 = t_2t_1^{-1}$ where $s_1, s_2 \in S$, $t_1, t_2 \in T$. Clearly, $s_1t_1 = s_2t_2$ and then, $s_1 = s_2$ and $t_1 = t_2$. Hence, $g = e$.

Conversely, suppose that $G = ST$ and $(S^{-1}S) \cap (TT^{-1}) = \{e\}$. We just need to prove that factorization of an arbitrary element $g \in G$ is unique. If $g = s_1t_1 = s_2t_2$ then $s_2^{-1}s_1 = t_2t_1^{-1}$. Since $(S^{-1}S) \cap (TT^{-1}) = \{e\}$, then it follows $s_2^{-1}s_1 = t_2t_1^{-1} = e$, i.e. $s_1 = s_2$ and $t_1 = t_2$, what makes factorization of g unique. □

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

Lemma 2.2. *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*. Denote by $\mathcal{T}(G)$ be the collection of transversal factorizations of G. Note that whenever a group G has a proper subgroup, there exists a proper factorization.

Example 2.3. 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.

Let $\mathcal{R}(G)$ be the collection of factorizations of G where at least one block is a nontrivial subgroup of G.

It is of particular interest to explore conditions under which every factorization of a group G belongs to $\mathcal{T}(G)$ or $\mathcal{R}(G)$. In general, there are stronger results regarding this problem when G is an abelian group. We include one of the milestones in the theory of factorizations of abelian groups, Rédei's theorem.

Theorem 2.2. *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, $1 \le i \le k$. Then at least one of the blocks $B_1, B_2, \ldots, B_k$ is a subgroup of G.*

The following lemma provides a relation between $\mathcal{T}(G)$ and $\mathcal{R}(G)$ under certain conditions.

Lemma 2.4. *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, $1 \le i \le k$. Then $\alpha \in \mathcal{T}(G)$.*

Proof. We give a proof by a repetitive use of Rédei's theorem. It is clear that the claim holds whenever the size of G is a prime number. Suppose now that $|G|$ is not prime. According to Rédei's theorem, there is at least one block of α that is a subgroup of G, say B_1. It is not hard to see that $\beta = [C_2, \ldots, C_k]$ is a factorization of G/B_1, where $C_i = B_iB_1/B_1$. Since α is normalized it follows that $B_i \cap B_j = \{e\}$ for $i \ne j$. Therefore, it must be that $|C_i| = |B_i|$ and then, the sizes of blocks in β are prime numbers. Thus, at least one of the C_i's must be a subgroup, say C_2. Since B_2B_1/B_1 is a subgroup of G/B_1 then B_1B_2 is a subgroup of G. Continuing this process, we have that

$$\{e\} \le B_1 \le B_1B_2 \le \cdots \le B_1B_2 \cdots B_k = G$$

is an ascending chain of subgroups and hence α is a transversal factorization. $\square$

There are examples of groups, as given in [5], for which all factorizations belong to $\mathcal{T}(G)$. For example, every factorization of the dihedral group of order 8 is transversal, while there exists a factorization of alternating group A_5 that is not transversal.

2.1. *Transformations on factorization*

Here, we will assume that $\alpha = [B_1, B_2, \ldots, B_k]$ is a factorization of a group G. By applying certain transformations on α, new factorizations can be obtained. We list some of them.

Fusing blocks. We can create a new factorization β by *fusing* two consecutive blocks of α say B_i and B_{i+1} to a single block $C = \{xy \mid x \in B_i,\ y \in B_{i+1}\}$. Thus, if $g = s_1s_2 \cdots s_is_{i+1} \cdots s_k$ is the factorization of g with respect to α, then the factorization of g with respect to β will be $g = s_1s_2 \cdots s_{i-1}ts_{i+2} \cdots s_k$, where $t = s_is_{i+1}$. In this case, we say that α is a *refinement* of β.

Sandwiching. Let $g_1, g_2, \ldots, g_{k+1}$ be an arbitrary sequence of elements in G. Then $\beta = [C_1, C_2, \ldots, C_k]$ is a factorization of G, where $C_i = g_i^{-1}B_ig_{i+1}$ for $1 \le i \le k$.

Note that when G is an abelian group, then $\beta = [B_1, B_2, \ldots, gB_i, \ldots, B_k]$ is a factorization for any $g \in G$. Consequently, $\gamma = [C_1, C_2, \ldots, C_k]$ is a factorization of G, where $C_i = B_i g_i$ for $g_i \in G, \ 1 \leq i \leq k$.

Exponentiation. Under certain conditions, raising a block of α elementwise to a fixed power induces a new factorization.

In general, it holds that $\beta = [B_k^{-1}, B_{k-1}^{-1}, \ldots, B_1^{-1}]$ is a factorization of group G. In this case we say that β is the *inverse* factorization of α, denoted by $\beta = \alpha^{-1}$. Let $g^{-1} = s_1 s_2 \cdots s_k$ be the factorization of g^{-1} with respect to α. Thus, $g = s_k^{-1} s_{k-1}^{-1} \cdots s_1^{-1}$ is the factorization of g with respect to β. As it has been shown in [6], when G is a finite, abelian group, then $\gamma = [C_1, C_2, \ldots, C_k]$ is a factorization of G, where $C_i = B_i^{m_i}$, and m_i are integer numbers such that $\gcd(m_i, |B_i|) = 1$ for $1 \leq i \leq k$. Note that $\alpha^{-1} \in \mathcal{T}(G)$ whenever $\alpha \in \mathcal{T}(G)$.

Automorphism action. Let ϕ be an automorphism of group G. Then, it follows that $\beta = [C_1, C_2, \ldots, C_k]$ is a factorization of G, where $C_i = \phi(B_i)$ for $1 \leq i \leq k$. Let g be an arbitrary element of G. Let $\phi^{-1}(g) = b_1 b_2 \cdots b_k$ be the unique factorization of $\phi^{-1}(g)$ with respect to α. By applying the automorphism ϕ to the both sides we have that $g = \phi(b_1)\phi(b_2)\cdots\phi(b_k)$. Suppose that $g = \phi(b_1')\phi(b_2')\cdots\phi(b_k')$, where $b_i' \in B_i$, $1 \leq i \leq k$. Then $\phi(b_1 b_2 \cdots b_k) = \phi(b_1' b_2' \cdots b_k')$ and therefore $b_1 b_2 \cdots b_k = b_1' b_2' \cdots b_k'$. We conclude that $b_i = b_i', \ 1 \leq i \leq k$ and accordingly $\phi(b_i) = \phi(b_i'), \ 1 \leq i \leq k$.

3. Free Mappings and Factorizations of $A \times B$

In this section, A and B will denote groups. By introducing a certain class of mappings 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 strictly mean proper factorization.

Definition 3.1. 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 f and g if it holds

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

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 $b_1 \neq b_2$. Two mappings f, g are *chained* if there exists a strong clip of f and g, otherwise we say that they are *free*.

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

Theorem 3.1. *Let $f : A \to B$ and $g : B \to A$ be mappings where A, B are finite groups. Let $S = \{(a, f(a)) | \, a \in A\}$ and $T = \{(g(b), b) | \, b \in B\}$. Then, $\alpha = [S, T]$ is a factorization of $A \times B$ if and only if f, g are free.*

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

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

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 are free.

Conversely, suppose that f and g are free mappings. 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 2.1, 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 3.2. *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* $\mathrm{Im}(g) \subseteq H$. *Then the mappings f, g are free.*

Proof. Suppose that there exists a strong clip (a_1, b_1), (a_2, b_2) of f and 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 $b_2 b_1^{-1} = e$, 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 and 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.

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

Example 3.3. Consider the group

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

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

First, we apply the technique given in Lemma 3.2 in order to find a pair of free mappings. We choose a subgroup H of $\mathcal{S}_3$, say $H = \{id, (1\ 2\ 3), (1\ 3\ 2)\}$. Then, considering the cosets H and $H(1\ 2)$, we can construct a pair of free mappings f, g in the following way:

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

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

The pair of free mappings f, g provides a factorization $\mathcal{S}_3 \times \mathbb{Z}_3 = B_1 \cdot B_2$, 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.

4. The Abelian Case

In this section, we assume that A and B are abelian groups. Let $f : A \to B$ and $g : B \to A$ be a pair of mappings. We define a relation $\mathcal{R}_{f,g}$ on $A \times B$ as $(a_1, b_1)\mathcal{R}_{f,g}(a_2, b_2)$ if and only if (a_1, b_1), (a_2, b_2) is a clip of f, g. It turns out that $\mathcal{R}_{f,g}$ is an equivalence relation.

By using free mappings, we will characterize factorizations of the groups $\mathbb{Z}_p \times \mathbb{Z}_p$ and $\mathbb{Z}_p \times \mathbb{Z}_q$, where p and q are two different primes. In our original approach, we show that all factorizations of $\mathbb{Z}_p \times \mathbb{Z}_q$ must be of the type we introduced in Theorem 3.1. At the end we show an interesting application of Rédei's theorem with a number theoretic implication.

Theorem 4.1. *Let $f : A \to B$ and $g : B \to A$ be mappings between abelian groups A and B. Then, the relation $\mathcal{R}_{f,g}$ is an equivalence relation.*

Proof. $\mathcal{R}_{f,g}$ is reflexive. Let (s, t) be an arbitrary pair from $A \times B$. From $f(s)f(s)^{-1} = tt^{-1}$ and $g(t)g(t)^{-1} = ss^{-1}$, it follows that $(s, t)\mathcal{R}_{f,g}(s, t)$.
$\mathcal{R}_{f,g}$ is symmetric. Let $(s, t)\mathcal{R}_{f,g}(u, w)$. From

$$f(s)f(u)^{-1} = tw^{-1}, \quad g(t)g(w)^{-1} = su^{-1}$$

it follows that

$$f(u)f(s)^{-1} = wt^{-1}, \quad g(w)g(t)^{-1} = us^{-1}$$

which means $(u, w)\mathcal{R}_{f,g}(s, t)$.

$\mathcal{R}_{f,g}$ is transitive. Let $(s,t)\mathcal{R}_{f,g}(u,w)$ and $(u,w)\mathcal{R}_{f,g}(z,r)$. It follows that

$$f(s)f(u)^{-1} = tw^{-1}, \quad g(t)g(w)^{-1} = su^{-1}$$
$$f(u)f(z)^{-1} = wr^{-1}, \quad g(w)g(r)^{-1} = uz^{-1}.$$

By multiplying left and right hand sides of the previous equalities, we obtain

$$f(s)f(z)^{-1} = tr^{-1}, \quad g(t)g(r)^{-1} = sz^{-1}$$

which means $(s,t)\mathcal{R}_{f,g}(z,r)$. □

An immediate consequence of the previous theorem is the following:

Corollary 4.1. *Let $f : A \to B$ and $g : B \to A$ be mappings where A, B are abelian groups. Let $S = \{(a, f(a)) |\ a \in A\}$, $T = \{(g(b), b) |\ b \in B\}$. Then, $\alpha = [S, T]$ is a factorization of $A \times B$ if and only if every equivalence class of $\mathcal{R}_{f,g}$ contains just one element.*

4.1. *A geometric interpretation of the factorizations of* $\mathbb{Z}_p \times \mathbb{Z}_p$

An interesting illustration of our approach is given for the abelian group $\mathbb{Z}_p \times \mathbb{Z}_p$. At the end of this section, we will be able to characterize the factorizations of $\mathbb{Z}_p \times \mathbb{Z}_p$ revealing their connection to free mappings.

The *graph* of a function $f : A \to B$ is the collection of all ordered pairs $(x, f(x)),\ \ x \in A$. We say that a function f is *normalized* if $f(0) = 0$.

First, suppose that f, g is a pair of linear mappings. Let ℓ_1, ℓ_2 be two non-parallel lines

$$\ell_1 : a_1x + b_1y = 0, \quad \ell_2 : a_2x + b_2y = 0,$$

where $a_1, a_2, b_1, b_2 \in \mathbb{Z}_p$. Clearly, the lines ℓ_1 and ℓ_2 generate the affine plane $\mathrm{AG}(2,p) \cong \mathbb{Z}_p \times \mathbb{Z}_p$. Without loss of generality, we can assume that a_2 and b_1 are nonzero elements and then there exist $m_1, m_2 \in \mathbb{Z}_p$ such that

$$\ell_1 : y = m_1x, \quad \ell_2 : x = m_2y.$$

It is easy to check that two mappings

$$\begin{aligned} f : \mathbb{Z}_p &\to \mathbb{Z}_p; & \qquad g : \mathbb{Z}_p &\to \mathbb{Z}_p \\ x &\mapsto m_1x & y &\mapsto m_2y \end{aligned}$$

are free, provided that the lines ℓ_1 and ℓ_2 are not parallel, i.e. $m_1 \cdot m_2 \neq 1$. Thus, we can state the following lemma.

Lemma 4.1. *Let f, g be the mappings defined as*

$$\begin{aligned} f : \mathbb{Z}_p &\to \mathbb{Z}_p; & \qquad g : \mathbb{Z}_p &\to \mathbb{Z}_p \\ x &\mapsto m_1x & y &\mapsto m_2y \end{aligned}$$

where $m_1, m_2 \in \mathbb{Z}_p$ and $m_1 \cdot m_2 \neq 1$. Then, f and g are free and $\alpha = [B_1, B_2]$ is a normalized factorization of $\mathbb{Z}_p \times \mathbb{Z}_p$ where

$$B_1 = \{(x, m_1x) \,|\, x \in \mathbb{Z}_p\}, \quad B_2 = \{(m_2y, y) \,|\, y \in \mathbb{Z}_p\}.$$

By Lemma 4.1, given a pair of non-parallel lines in the affine plane $AG(2,p)$, we can construct a pair of free mappings and hence a factorization of the group $\mathbb{Z}_p \times \mathbb{Z}_p$. Conversely, let us consider a group G of type (p,p) and a normalized factorization $\alpha = [B_1, B_2]$. By Rédei's Theorem 2.2, either B_1 or B_2 is a subgroup of G, and then that block can be seen as a line in the affine plane $AG(2,p)$. Thus, we can state the following lemma.

Lemma 4.2. *Let G be an abelian group of type (p,p). If $\alpha = [B_1, B_2]$ is a normalized factorization of G then, either B_1 or B_2 is a line of the affine plane $AG(2,p)$.*

Note that if $\alpha = [B_1, B_2]$ is a factorization of abelian group of type (p,p) then not necessarily both B_1 and B_2 are lines. Let us consider the following example.

Example 4.3. Let $G = \mathbb{Z}_3 \times \mathbb{Z}_3$ and

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

Then, $\alpha = [B_1, B_2]$ is a factorization of G. Clearly, even if B_1 is a line, factorization α is not of the type given in Theorem 3.1. However, we will see that free mappings have an important role that will lead us to a characterization of factorizations of abelian groups of the type (p,p).

By Lemma 4.2, at least one of the blocks of a factorization of $\mathbb{Z}_p \times \mathbb{Z}_p$ is a line. The case in which the blocks are lines has been discussed in Lemma 4.1. The following lemma provides a characterization in the general case.

Lemma 4.4. *Let A be a subset of $\mathbb{Z}_p \times \mathbb{Z}_p$ and $g : \mathbb{Z}_p \to \mathbb{Z}_p$ defined as $g(y) = my$. Let $B = \{(my, y) \,|\, x \in \mathbb{Z}_p\}$. Then, $\alpha = [A, B]$ is a factorization of $\mathbb{Z}_p \times \mathbb{Z}_p$ provided that $|A| = p$ and*

$$m \notin \left\{ \frac{x_1 - x_2}{y_1 - y_2} \,\middle|\, (x_1, y_1), (x_2, y_2) \in A,\ y_1 \neq y_2 \right\}.$$

Proof. Suppose that $\alpha = [A, B]$ is not a factorization of $\mathbb{Z}_p \times \mathbb{Z}_p$. Then, there exist $(x_1, y_1), (x_2, y_2) \in A$, $(x_1, y_1) \neq (x_2, y_2)$, and $\overline{y}_1, \overline{y}_2 \in \mathbb{Z}_p$, $\overline{y}_1 \neq \overline{y}_2$, such that

$$(x_1, y_1) + (m\overline{y_1}, \overline{y_1}) = (x_2, y_2) + (m\overline{y_2}, \overline{y_2}).$$

Note that $y_1 \neq y_2$ and

$$m(\overline{y_1} - \overline{y_2}) = x_2 - x_1, \quad \overline{y_1} - \overline{y_2} = y_2 - y_1.$$

Hence,

$$m = \frac{x_1 - x_2}{y_1 - y_2}$$

which contradicts the given assumption. $\square$

Theorem 4.2. *Let f be a mapping $f : \mathbb{Z}_p \to \mathbb{Z}_p$ and $g : \mathbb{Z}_p \to \mathbb{Z}_p$ defined as $g(y) = my$, where $m \neq 0$. The mappings f, g are free, provided that*

$$m^{-1} \notin \left\{ \frac{f(x_1) - f(x_2)}{x_1 - x_2} \,\middle|\, x_1, x_2 \in \mathbb{Z}_p,\ x_1 \neq x_2 \right\}.$$

Furthermore, if $g(x) = 0$, then f, g are free mappings for every f.

Proof. This follows from the previous lemma with $A = \{(x, f(x)) \,|\, x \in \mathbb{Z}_p\}$. $\square$

Let us consider Example 4.3 and the automorphism σ_1 of $\mathbb{Z}_3 \times \mathbb{Z}_3$ defined by the matrix $M_1 = \left(\begin{smallmatrix} 1 & -1 \\ 0 & 1 \end{smallmatrix}\right)$. The automorphism action of σ_1 on the factorization α yields to factorization: $\sigma_1(\alpha) = [\sigma_1(B_1), \sigma_1(B_2)]$, where

$$\sigma_1(B_1) = \{(0,0), (0,1), (0,2)\}, \quad \sigma_1(B_2) = \{(0,0), (1,0), (2,2)\}.$$

We obtained a new factorization where one block is the vertical line $g : x = 0$ and the other block is the graph of the function $f : \left(\begin{smallmatrix} 0 & 1 & 2 \\ 0 & 0 & 2 \end{smallmatrix}\right)$.

In the following theorem we generalize this approach.

Theorem 4.3. *Let G be a group of type (p, p) and $\alpha = [B_1, B_2]$ a normalized factorization of G. Then, there exists $\sigma \in SL(2, p)$ such that one block of $\sigma(\alpha)$ is the vertical line and the other block is the graph of a normalized function.*

Proof. Without loss of generality, we can assume that the block B_1 is a line ℓ. Suppose that $\ell : x = 0$. We prove that in this case, B_2 must be a graph of a function. If B_2 is not graph of a function then there exist $x, y_1, y_2 \in \mathbb{Z}_p$, $y_1 \neq y_2$ such that (x, y_1) and (x, y_2) are in B_2. Then we have

$$(0, y_2 - y_1) + (x, y_2) = (0, 0) + (x, y_1)$$

what contradicts the fact that α is a factorization.

Consider the case when $\ell : y = 0$. By taking automorphism action of

$$\sigma = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

on the factorization α we obtain a new factorization where the first block $\sigma(B_1)$ is the line $x = 0$. According to the argument given above, it follows that $\sigma(B_2)$ must be the graph of a normalized function.

Finally, let us suppose that $\ell : y = mx$, $m \neq 0$. Then, we can define

$$\sigma = \begin{pmatrix} m & -1 \\ 0 & 1/m \end{pmatrix}.$$

It is clear that $\sigma \in SL(2, p)$ and $\sigma(B_1)$ is the line $x = 0$. Hence, $\sigma(B_2)$ must be the graph of a normalized function. $\square$

Theorem 4.3 characterizes the factorizations of the group $\mathbb{Z}_p \times \mathbb{Z}_p$ in a geometric fashion since it shows that every normalized factorization of $\mathbb{Z}_p \times \mathbb{Z}_p$ is a rotation of a factorization $\alpha = [B_1, B_2]$ where B_1 corresponds to the vertical line $x = 0$ and B_2 is the graph of a function from $\mathbb{Z}_p$ to $\mathbb{Z}_p$. Considering two factorizations $\alpha = [B_1, B_2]$ and $\alpha' = [B_1', B_2']$ of $\mathbb{Z}_p \times \mathbb{Z}_p$ to be equal if $\{B_1, B_2\} = \{B_1', B_2'\}$, it is not hard to see that the number of normalized factorizations of $\mathbb{Z}_p \times \mathbb{Z}_p$ is

$$(p+1)p^{p-1} - \binom{p+1}{2} = \frac{p(p+1)}{2}(2p^{p-2} - 1).$$

4.2. *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 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 4.5. 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.

Theorem 4.4. *Let p be a prime number and $c_p, c_{p-1}, \ldots, c_1$ integers. Let*

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

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, 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 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 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. $\square$

Definition 4.6. 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 its implication to factorization of abelian groups. Namely, it provides a condition under which the sum of two multisets of integer numbers, where one of them has prime number size p, is uniformly distributed among the residue classes modulo p.

Lemma 4.7. *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, a 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 $1 \le i \le p$. Note that

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

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

$$\begin{array}{rcccc} m_1 = & b_1 c_p & + b_2 c_{p-1} & + \cdots + & b_p c_1 \\ m_2 = & b_1 c_1 & + \quad b_2 c_p & + \cdots + & b_p c_2 \\ \vdots & \vdots & \vdots & & \vdots \\ m_p = & b_1 c_{p-1} & + b_2 c_{p-2} & + \cdots + & b_p c_p. \end{array}$$

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

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

If $C = \operatorname{circ}(c_p, c_{p-1}, \ldots, c_1)$, $b = (b_1, b_2, \ldots, b_p)^t$ and $d = (n, n, \ldots, n)^t$, 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 4.4, 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 very special case of the [7, Theorem 1], presented proof is based on new method, using circulant matrices and cyclotomic polynomials.

Lemma 4.8. *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

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

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 4.7, U must contain all residue classes modulo p. Therefore, B_1 is a complete system of residue classes modulo p. □

Corollary 4.2. *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 $B_1 = \{(a, f(a)) \mid 0 \leq a \leq p - 1\}$ and

$B_2 = \{(g(b), b) \,|\, 0 \le b \le q-1\}$. Consequently, using Theorem 3.1 we have the following result.

Corollary 4.3. *$\alpha = [B_1, B_2]$ is a factorization of $\mathbb{Z}_p \times \mathbb{Z}_q$ if and only if*

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

p and q different primes and f, g are free mappings.

Clearly, every factorization can be easily normalized, simply by translation for 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 $B_1 = \{(a, 0)) \,|\, 0 \le a \le p-1\}$. It means that $f(a) = 0$ for every $a \in \mathbb{Z}_p$. It 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 them is zero mapping. Similarly as in the case of $\mathbb{Z}_p \times \mathbb{Z}_p$, 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 total number of normalized factorizations of $\mathbb{Z}_p \times \mathbb{Z}_q$ is equal to $p^{q-1} + q^{p-1} - 1$.

Example 4.9. Consider the mappings $f : \mathbb{Z}_3 \to \mathbb{Z}_4$, $g : \mathbb{Z}_4 \to \mathbb{Z}_3$, defined as

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

It is not hard to see that f, g are free. Therefore, it is possible to factorize $\mathbb{Z}_3 \times \mathbb{Z}_4$ in the way shown in Theorem 3.1. 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 mappings $f : \mathbb{Z}_p \to \mathbb{Z}_q$, $g : \mathbb{Z}_q \to \mathbb{Z}_p$.

Theorem 4.5. *Let $f : \mathbb{Z}_p \to \mathbb{Z}_q$ and $g : \mathbb{Z}_q \to \mathbb{Z}_p$ be mappings such that $|\mathrm{Im}(f)| > 1$, $|\mathrm{Im}(g)| > 1$, $f(0) = 0$, $g(0) = 0$. Then f and g are chained whenever p and q are different primes.*

Proof. Let us suppose that f and g are free. By Theorem 3.1, $\alpha = [B_1, B_2]$ is a factorization of $\mathbb{Z}_p \times \mathbb{Z}_q$ where

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

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 and g must be chained. □

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

$$\begin{aligned} f(i_1) - f(i_2) &\equiv j_1 - j_2 \pmod{q} \\ g(j_1) - f(j_2) &\equiv i_1 - i_2 \pmod{p} \end{aligned}$$

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. The following example shows that the assumption for p and q to be different primes cannot be dropped.

Example 4.10. Consider mappings $f : \mathbb{Z}_3 \to \mathbb{Z}_3$, $g : \mathbb{Z}_3 \to \mathbb{Z}_3$, defined as

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

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

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

5. Conclusions

In this paper we studied group factorizations of G using free mappings, where $G \cong A \times B$. Lemma 3.2 provides an effective way for constructing pairs of free mappings. Consequently, using Theorem 3.1, new factorizations of G can be constructed. It should be emphasized that there are no further restrictions on groups A and B except that they have to be finite. It could be interesting exploring which conditions infinite groups A and B should satisfy to have factorizations using free mappings.

A special attention was given to the finite, abelian case. In particular, we were able to characterize all factorizations of $\mathbb{Z}_p \times \mathbb{Z}_p$ and $\mathbb{Z}_p \times \mathbb{Z}_q$ using free mappings. We showed the use of circulant matrices for studying group factorizations and the potential significance of this approach could be an interesting direction for the further research.

Also, it has been shown an interesting number theoretic consequence of Rédei's Theorem 2.2 on the pair of mappings $f : \mathbb{Z}_p \to \mathbb{Z}_q$, $g : \mathbb{Z}_q \to \mathbb{Z}_p$, when neither f nor g is a constant mapping. The problem we address for the further research is exploring some other methods for constructing free mappings between groups A and B.

As we already stated, group factorizations have relation to other branches of mathematics, like coding theory and cryptography. Finally, it would be worth examining what role the concept of free mappings has in the related scientific areas.

Acknowledgments

The authors would like to thank Spyros S. Magliveras and Gábor Korchmáros for their valuable comments and suggestions.

References

[1] N. Božović and Ž. Mijajlović, *Uvod u Teoriju Grupa* (Naučna knjiga, Beograd, 1990).
[2] P. J. Davis, *Circulant Matrices* (John Wiley and Sons, 1979).

[3] M. W. Liebeck, C. E. Praeger and J. Saxl, The maximal factorizations of the finite simple groups and their automorphism groups, *Memoirs of the AMS* **86**(432) (1990).
[4] S. S. Magliveras, A cryptosystem from logarithmic signatures over finite groups, *Proc. 29th Midwest Symposium on Circuits and Systems* (Elsevier, 1986), pp. 972–975.
[5] S. S. Magliveras and N. D. Memon, Algebraic properties of cryptosystem PGM, *J. Cryptology* **5** (1992) 167–184.
[6] S. Szabó, *Topics in Factorization of Abelian Groups* (Birkhäuser, 2004), pp. 20–26.
[7] A. D. Sands, On the factorization of finite groups, *J. London Math. Soc.* **s2–7** (1974) 627–631.