ALGEBRAIC AND COMBINATORIAL ASPECTS OF GROUP FACTORIZATIONS

by

Vladimir Božović

A Dissertation Submitted to the Faculty of
The Charles E. Schmidt College of Science
in Partial Fulfillment of the Requirements for the Degree of
Doctor of Philosophy

Florida Atlantic University
Boca Raton, Florida
December 2008

ALGEBRAIC AND COMBINATORIAL ASPECTS OF GROUP FACTORIZATIONS

by

Vladimir Božović

This dissertation was prepared under the direction of the candidate's dissertation advisor, Dr. Spyros S. Magliveras, Department of Mathematical Sciences, and it has been approved by the members of his supervisory committee. It was submitted to the faculty of the Charles E. Schmidt College of Science and was accepted in partial fulfillment of the requirements for the degree of Doctor of Philosophy.

SUPERVISORY COMITTEE:

Spyros S. Magliveras, Ph.D.
Dissertation Advisor

Fred Richman, Ph.D.

Lee Klingler, Ph.D.

Wan-DiWei, Ph.D.

Spyros S. Magliveras, Ph.D.
Chair, Department of Mathematical Sciences

Gary W. Perry, Ph.D.
Dean, The Charles E. Scmidt College of Science

Barry T. Rosson, Ph.D.
Dean, Graduate College

November 4, 2008
Date

Acknowledgements

First of all, I would like to express my deepest gratitude to all members of my dissertation committee, Professor Spyros S. Magliveras, Professor Wan-Di Wei, Professor Lee Klingler and Professor Fred Richman. I appreciate their time, interest, and valuable comments concerning my thesis.

For the last four years, I have had the opportunity and the privilege to work with Dr. Magliveras. Under his guidance I developed a strong tendency towards scientific research. It was he who introduced me to many amazing subjects in mathematics that I had not even seen before. I sincerely thank him for giving me the opportunity to see that world and feel the joy of being there.

I would also want to use this opportunity to thank many faculty members and my colleagues for their friendly but valuable discussions.

Some of the most valuable suggestions for this research came from Professor Aaron Meyerowitz. He has given me ideas and suggestions that enlighten my understanding of this research and gave me a better perspective on my own work. I thank him for his valuable comments and suggestions.

I owe special thanks to Professors Dragan Radulović and Heinrich Niederhausen for their tremendous, continuous help and support in many ways, from the very first day I came at FAU.

Most importantly, I am grateful to my parents and family for giving me their love and constant support for my academic journey. Their guidance have helped me sail through difficult chapters of my life. I dedicate this dissertation to them.

Abstract

Author:	Vladimir Božović
Title:	Algebraic and Combinatorial Aspects of Group Factorizations
Institution:	Florida Atlantic University
Dissertation Advisor:	Dr. Spyros S. Magliveras
Degree:	Doctor of Philosophy
Year:	2008

The aim of this work is to investigate some algebraic and combinatorial aspects of group factorizations. The main contribution of this dissertation is a set of new results regarding factorization of groups, with emphasis on the nonabelian case. We introduce a novel technique for factorization of groups, the so-called *free mappings*, a powerful tool for factorization of a wide class of abelian and non-abelian groups. By applying a certain group action on the blocks of a factorization, a number of combinatorial and computational problems were noted and studied. In particular, we analyze the case of the group $\mathrm{Aut}(\mathbb{Z}_n)$ acting on blocks of factorization of $\mathbb{Z}_n$. We present new theoretical facts that reveal the numerical structure of the stabilizer of a set in $\mathbb{Z}_n$, under the action of $\mathrm{Aut}(\mathbb{Z}_n)$. New algorithms for finding the stabilizer of a set and checking whether two sets belong to the same orbit are proposed.

Contents

Chapter 1

Introduction

In mathematics, the term "*factorization*" often refers to a decomposition of integers into a product of primes. Factorization of integers is assumed to be a difficult problem, since no efficient algorithm has been found to date. The complexity of factorization is the security basis for many public-key cryptosystems. The most prominent representative of this class is certainly the RSA public-key cryptosystem, which is used in many modern security protocols.

More generally, *factorization* represents the decomposition of an object (e.g. a number, a polynomial, or a matrix) into a product of other objects, called *factors*. The aim of factoring is usually to reduce something to its "basic building blocks", such as numbers to prime numbers, or polynomials to irreducible polynomials. However, in the case of more complex algebraic objects, it may not be clear what the actual basic building blocks are. While this is certainly true for *groups*, there exists a notion of *group factorization* in the literature.

Depending on whether a group G is abelian or non-abelian, two different approaches to defining *group factorization* have been proposed in the past. When G is abelian, a *factorization* is considered to be a collection of subsets $\alpha = [B_1, \ldots, B_k]$ such that that every element $g \in G$ has a unique representation $g = s_1 s_2 \ldots s_k$, where $s_i \in B_i$

for $1 \leq i \leq k$. The subsets B_i of G, $1 \leq i \leq k$, are called the *blocks* of the factorization. When G is non-abelian, the term *factorization* has frequently been used for the case where the blocks are subgroups of G, even without insisting on uniqueness of the representation of elements. However, in [10] one finds the notion of a *logarithmic signature* for an arbitrary group G, that completely agrees with the meaning of factorization in the abelian case. In this thesis, we use a unified definition of *group factorization* for both the abelian and non-abelian 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 non-abelian groups where the blocks are considered more generally as sets, rather than subgroups (for example [10], [11], [17], [18]). On the other hand, much work has been done when the blocks are subgroups (see for instance [9]).

In the abelian case, another term closely related to factorization is *tiling*. This indicates the connection of factorization to combinatorics and geometry. Indeed, at the beginning of the twentieth century, Hermann Minkowski gave the following conjecture [12]:

Conjecture 1.1 (Minkowski's Conjecture)**.** *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 [6]. 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 to abelian groups. In general, factorization questions are relevant to the theory of numbers, tilings, packings and covering problems.

On the other hand, group factorization is a topic that besides its theoretical

beauty has practical uses in graph theory, coding theory, number theory and modern cryptography. Group factorization is the main tool for cryptosystems such as PGM [11] and MST1 [16]. As a further application, group factorizations are used for constructing graphs of large girth, i.e. graphs that do not contain cycles of short length. It is known that bipartite graphs of large girth are important for LDPC codes. For instance, a construction for a cryptosystem based on such graphs is given in [20]. Therefore, finding new factorization techniques has a significant theoretical and practical impact.

The main substance of this thesis is group factorizations. While it may initially appear to the reader that Chapters 2 and 3 are completely independent with no obvious connection to group factorizations, these seemingly independent topics will in fact be put together in the context of group factorization theory in Chapter 4. The rest of this dissertation is organized as follows.

Chapter 2 starts with basic information about cyclic groups that is relevant to the presentation of the material that follows.

In Chapter 2 we mainly describe the action of the group of automorphisms of $\mathbb{Z}_n$, denoted by $\mathcal{I}(n)$, on the set of k-sets of $\mathbb{Z}_n$. Although elementary in nature, this topic has not yet been fully analyzed nor understood. A large class of enumerative and computational problems relate to this particular group action. For example, determining the number of orbits on the set of k-sets of $\mathbb{Z}_n$ is one such problem. Such enumerative problems are usually resolved by an application of Pólya's theory. Another problem that is of significant interest is to find an efficient way of determining the orbit of a particular subset $A \subseteq \mathbb{Z}_n$ under the aforementioned group action. In solving this problem, it is natural to start with finding the stabilizer of the subset A,

denoted by $\mathrm{Stab}(A, \mathcal{I}(n))$. Clearly,

$$\mathbb{Z}_n = \bigcup_{d|n} \Omega_d$$

where Ω_d are the elements of $(\mathbb{Z}_n, +)$ of additive order d. Hence, if $A \subseteq \mathbb{Z}_n$, then

$$A = \bigcup_{d \in \mathcal{D}_A} A \cap \Omega_d.$$

where $\mathcal{D}_A = \{d \mid A \cap \Omega_d \neq \emptyset,\ d \mid n\}$. Thus,

$$\mathrm{Stab}(A, \mathcal{I}(n)) = \bigcap_{d \in \mathcal{D}_A} \mathrm{Stab}(A \cap \Omega_d, \mathcal{I}(n)).$$

Therefore, it is important to find $\mathrm{Stab}(A \cap \Omega_d, \mathcal{I}(n))$ and understand its content. The key fact is the relation given in Lemma 2.15 which casts light on the numerical structure of the stabilizer of a k-set in $\mathbb{Z}_n$. Let $V = \mathrm{Stab}(A \cap \Omega_d, \mathcal{I}(n))$. Let A_d be the set such that $A \cap \Omega_d = \frac{n}{d} A_d$ and let $S = \mathrm{Stab}(A_d, \mathcal{I}(d))$. We prove that

$$V = \bigcup_{t \in S} \mathcal{I}_d^t(n), \tag{1.0.1}$$

where

$$\mathcal{I}_k^r(n) = \{x \in \mathcal{I}(n) |\ x \equiv r \pmod{k}\}.$$

We present an analysis of the $\mathcal{I}_k^r(n)$ sets in an algebraic and number theoretical sense. Using the result 1.0.1 we are able to give an algorithm, **Stab**(A, n), for efficiently determining the stabilizer of a set A under the described action of the group $\mathcal{I}(n)$. Also, we describe an algorithm, **IsInOrbit**(A, B, n), that checks whether two sets A and B are in the same orbit or not.

In Chapter 3 we deal with a problem similar to that of Chapter 2. Namely, we consider again the same group $\mathcal{I}(n)$ except that now the underlying set in the group action is the set of all k-complete sets. We define set $A \subseteq \mathbb{Z}_n$ to be a *k-complete* if it contains every residue class modulo k exactly once. As part of that problem, we first explain the connection between the canonical permutation representation of the group $\mathcal{I}(mn)$ and the canonical permutation representations of the groups $\mathcal{I}(m)$ and $\mathcal{I}(n)$, where m and n are relatively prime numbers. Here, by the canonical permutation representation of the group $\mathcal{I}(s)$ on $\mathbb{Z}_s$, we mean

$$a \to \pi_a,\ a \in \mathcal{I}(s)$$

where π_a is the mapping

$$\pi_a(x) = ax,\quad x \in \{0, 1, \ldots, s-1\}.$$

The second important question we deal with is finding the number of orbits of n-complete sets in $\mathbb{Z}_{mn}$, fixed by the element $g \in \mathcal{I}(mn)$, where m and n are relatively prime. The answer to this problem is given by Lemma 3.3.

The subject of Chapter 4 is factorization of groups. In Sections 4.1 and 4.2 we give an overview of some important, well known results in the factorization of abelian groups accompanied by some new results. Many known results related to abelian groups are generalized, so they could possibly be applied in the case of non-abelian groups. Since most of them are used on the way to proving Rédei's theorem, one can expect that those generalized results could lead to non-abelian variations of that famous theorem. In Section 4.4 we prove two useful results, given in Lemma 4.18 and Theorem 4.7, by which it is possible to determine *good* candidates for blocks

of a factorization. In Section 4.5 we introduce a novel concept, the so-called *free mappings*, a powerful factorization tool for members of a wide class of abelian and non-abelian groups. 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 form a *clip* for f and g if the following two conditions hold:

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

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

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 said to be *chained* if there exists a strong clip for f and g, otherwise we say that they are *free*. Originally, free mappings were considered in the factorization of direct products [2], but by using Lemma 4.20, it is possible to factor a much wider class of groups, among which are semidirect products. In Section 4.6 we apply free mappings to the factorization of abelian groups. In particular, we treat the cases $\mathbb{Z}_p \times \mathbb{Z}_p$ and $\mathbb{Z}_p \times \mathbb{Z}_q$, where p and q are primes. For example, we show that every factorization of $\mathbb{Z}_p \times \mathbb{Z}_q$ induces one pair of free mappings and vice versa. Finally, Section 4.7 connects the previous chapters with Chapter 4. Namely, we prove that in a factorization of $\mathbb{Z}_{mn}$ into two blocks $[B_1, B_2]$ of size m and n respectively, B_1 must be an m-complete set and B_2 must be an n-complete set when $\gcd(m, n) = 1$. Given the factorization $[B_1, B_2]$ of $\mathbb{Z}_{mn}$ and $t, s \in \mathbb{Z}_{mn}$ such that $\gcd(t, mn) = 1$, $\gcd(s, mn) = 1$, then $[tB_1, sB_2]$ is also a factorization of $\mathbb{Z}_{mn}$. Thus, it suffices to have just the representatives of orbits of $m-$ and n-complete sets for describing all factorizations of $\mathbb{Z}_{mn}$.

Chapter 2

Orbits of k-sets

2.1 Cyclic Groups

In this section, we give the basic definitions and theorems about cyclic groups. For the proofs, we recommend standard textbooks such as [5] or [22].

Definition 2.1. *A group G is called cyclic if there exists an element a in G such that $G = \langle a \rangle = \{a^i | \ i \in \mathbb{Z}\}$. When $|G| = n$, for a positive integer n, we say that the order of a, denoted by* $\mathrm{ord}(a)$*, is equal to n.*

Lemma 2.1. *Let G be a cyclic group. Then, $G \cong \mathbb{Z}$ if G is infinite, and $G \cong \mathbb{Z}_n$ if G is finite of order n.*

Corollary 2.1. *All finite cyclic groups of the same order are isomorphic. All infinite cyclic groups are isomorphic.*

Considering the previous corollary, by a finite cyclic group of order n, we will assume the additive group $\mathbb{Z}_n$.

Theorem 2.1. *Every subgroup of a cyclic group G is cyclic. For each divisor m of n, where n is the order of the finite cyclic group G, there is exactly one subgroup H such that $|H| = m$.*

Corollary 2.2. *In a finite cyclic group, two elements generate the same subgroup if and only if the elements have the same order.*

Lemma 2.2. *Let $G = \langle a \rangle$ be a finite cyclic group of size n. Then $\langle a^k \rangle = \langle a^{\gcd(k,n)} \rangle$ for any integer number $k \in \mathbb{Z}$. Consequently,*

$$\operatorname{ord}(a^k) = \frac{n}{\gcd(k,n)}.$$

Lemma 2.3. *Let $G = \langle a \rangle$ be a cyclic group where $|G| = n$, and suppose that $d \mid n$. Then $\langle a^{\frac{n}{d}} \rangle = \langle a^{k\frac{n}{d}} \rangle$ if and only if $\gcd(k,d) = 1$.*

Theorem 2.2. *Let G be a finite cyclic group of order n, $G = \langle a \rangle$. The group of automorphisms Aut(G) of G is isomorphic to the group of integers in $\{0, 1, \ldots, n-1\}$ relatively prime to n,*

$$\mathcal{I}(n) = \{i \mid 0 \leq i < n,\ \gcd(i,n) = 1\},$$

where the operation on $\mathcal{I}(n)$ is multiplication modulo n.

2.2 The action of $\mathcal{I}(n)$ on the k-sets of $\mathbb{Z}_n$

According to Theorem 2.2, there is an isomorphism between groups $\mathrm{Aut}(\mathbb{Z}_n)$ and $\mathcal{I}(n)$, the automorphism group of $\mathbb{Z}_n$ and the multiplicative group of residue classes that are coprime to n. In the sequel, we will denote by $\mathcal{I}(n)$ both groups and it will be clear from the context which one of those two we have specifically in mind. We consider the action of the group $\mathcal{I}(n)$ on the set of elements of $\mathbb{Z}_n$, given by

$$(x,t) \to tx \quad (t \in \mathcal{I}(n),\ x \in \mathbb{Z}_n).$$

There is a natural way to induce this action on the set of subsets of $\mathbb{Z}_n$ of size k, denoted by $\mathcal{O}_k$. Furthermore, by a *k-set* we will assume a set of size k. In order to answer some enumerative questions regarding the above action, we need to determine the *cycle index* of $\mathcal{I}(n)$ acting on $\mathbb{Z}_n$. We first find the cycle index of the permutation group $\mathcal{I}(p^m)$ acting on $\mathbb{Z}_{p^m}$, where p is a prime, and then use a technique described in [7] in order to find the cycle index of the product of permutation groups. Consequently, we obtain the cycle index of $\mathcal{I}(n)$ acting on $\mathbb{Z}_n$.

Besides this combinatorial aspect of the described action, we are also interested in some computational questions, such as finding the stabilizer of a k-set $A \subseteq \mathbb{Z}_n$. Once the stabilizer is found, there is a straightforward way to determine the orbit that A belongs to. It turns out that the $\mathcal{I}_k^r(n)$ sets, introduced in Section 2.3, play an important role in finding the stabilizer of a set A. By Lemma 2.15, the stabilizer of a k-set can be obtained as the disjoint union of some $\mathcal{I}_k^r(n)$ sets. This lemma is at the heart of the proposed algorithms for finding the stabilizer of a k-set and checking whether two k-sets belong to the same orbit or not. In what follows, we will let $\mathbb{N}$ denote the set of positive integers, which is also referred to as the set of *natural numbers*.

2.3 The notion of $\mathcal{I}_k^r(n)$ sets

In this section, we introduce the notion of an $\mathcal{I}_k^r(n)$ sets and analyze it from an algebraic and number-theoretical point of view.

Definition 2.2. *Let r, k be natural numbers such that $\gcd(r,k) = 1$, $r < k$ and let k be a divisor of the natural number n. We define*

$$\mathcal{I}_k^r(n) = \{x \in \mathcal{I}(n) |\ x \equiv r\ (mod\ k)\}$$

Firstly, we prove that no $\mathcal{I}_k^r(n)$ set is empty.

Lemma 2.4. *Let r, k, ℓ, n be natural numbers such that $\gcd(r,k) = 1$, $r < k$ and $n = k\ell$. Then the $\mathcal{I}_k^r(n)$ set is nonempty.*

Proof. We prove that for given r, k and n where $\gcd(r,k) = 1$, there exists t such that

$$\gcd(r + kt, n) = 1.$$

Let $p_i^{v_i}$ be a general prime power divisor of n. Then, there exists t_i such that

$$\gcd(r + kt_i, p_i^{v_i}) = 1.$$

Namely, if $p_i \mid k$, then $p_i \nmid r$ and $t_i = 0$ suffices. If $p_i \nmid k$, then any number t_i such that

$$t_i \not\equiv -r/k \pmod{p_i}$$

will work. By the Chinese Reminder Theorem, there exists t such that

$$t \equiv t_i \pmod{p_i}$$

and $\gcd(r + kt, n) = 1$. We need to prove that there exists $x \in \mathcal{I}(n)$ such that $x \equiv r \ (mod\ k)$. Let $x \equiv r + kt \pmod{n}$. Since $k \mid n$ then $x \equiv r \pmod{k}$. Also, it is easy to see that $\gcd(x, n) = 1$ and therefore $x \in \mathcal{I}(n)$. □

If k divides n, then there is natural homomorphism from $\mathbb{Z}_n$ to $\mathbb{Z}_k$ that is onto. This mapping induces homomorphism between corresponding automorphism groups $\mathcal{I}(n)$ and $\mathcal{I}(k)$. So Lemma 2.4 says that this, induced homomorphism from $\mathcal{I}(n)$ to $\mathcal{I}(k)$ is onto. The set $\mathcal{I}_k^1(n)$ is the kernel of this homomorphism and $\mathcal{I}_k^r(n)$ are the cosets of $\mathcal{I}_k^1(n)$ in $\mathcal{I}(n)$. From this observation, we have the following claim.

Lemma 2.5. *Let r, k, n be natural numbers such that $gcd(r, k) = 1$, $k \mid n$ and $r < k$. It follows that*

$$|\mathcal{I}_k^r(n)| = |\mathcal{I}_k^1(n)| = \frac{\phi(n)}{\phi(k)}.$$

Proof. Homomorphism from $\mathcal{I}(n)$ to $\mathcal{I}(k)$ is onto and $\mathcal{I}_k^1(n)$ is its kernel. Therefore

$$|\mathcal{I}_k^1(n)| = \frac{\phi(n)}{\phi(k)}.$$

Since $\mathcal{I}_k^r(n)$ are the cosets of $\mathcal{I}_k^1(n)$ in $\mathcal{I}(n)$, the claim is proven. □

Lemma 2.6. *Let k and ℓ be relatively prime natural numbers and $k > 1$. Then, it holds*

$$\mathcal{I}_k^1(k\ell) \cong \mathcal{I}(\ell).$$

Proof. Let $\mathcal{A}$ be a mapping from $\mathcal{I}_k^1(k\ell)$ to $\mathcal{I}(\ell)$ defined by

$$\mathcal{A}(x) = x \pmod{\ell}.$$

First, we show that $\mathrm{Im}(\mathcal{A}) \subseteq \mathcal{I}(\ell)$. Let $x \in \mathcal{I}_k^1(k\ell)$. Then, $x = a\ell + b$, $0 \leq b \leq \ell$. Since $x \in \mathcal{I}_k^1(k\ell)$, then by the definition of that set, it follows that $x \in \mathcal{I}(k\ell)$. Therefore $\gcd(x, \ell) = 1$ and consequently $\gcd(b, \ell) = 1$. Thus, $b \in \mathcal{I}(\ell)$, so we have $\mathcal{A}(x) \in \mathcal{I}(\ell)$.

$\mathcal{A}$ is evidently a homomorphism, according to the properties of modulo operation. $\mathcal{A}$ is one to one. Let $x, y \in \mathcal{I}_k^1(k\ell)$ and $\mathcal{A}(x) = \mathcal{A}(y)$. From the definition of $\mathcal{I}_k^1(k\ell)$, we have $x \equiv 1 \pmod{k}$ and $y \equiv 1 \pmod{k}$, so $x \equiv y \pmod{k}$. From $\mathcal{A}(x) = \mathcal{A}(y)$ it follows $x \equiv y \pmod{\ell}$. Since k and ℓ are relatively prime, then $x \equiv y \pmod{k\ell}$, so $\mathcal{A}$ is one to one.

$\mathcal{A}$ is onto. Let $z \in \mathcal{I}(\ell)$. We have to find $x \in \mathcal{I}_k^1(k\ell)$ such that $\mathcal{A}(x) = \ell$, or in other words $x \equiv z \pmod{\ell}$. That x must be of the form $1 + kt$, so we should find such a t for which it holds $x \equiv z \pmod{\ell}$. From $\gcd(k, \ell) = 1$, there exist $m, n \in \mathbb{Z}$ such that $mk + n\ell = 1$. Let us define $t = (z-1)m$, i.e. $x = 1 + (z-1)mk$. Clearly, $x \equiv 1 \pmod{k}$. Note that $x = 1 + (z-1)(1 - n\ell)$, that is $x = z + n\ell(1-z)$, so $x \equiv z \pmod{\ell}$. Now, we need to prove that $\gcd(x, \ell) = 1$. Since $z \in \mathcal{I}(\ell)$ than $\gcd(z, \ell) = 1$, but since $x \equiv z \pmod{\ell}$, we conclude that $\gcd(x, \ell) = 1$. Therefore, $\gcd(x, k\ell) = 1$. At the end, we need to provide that $x < k\ell$. If $x = 1 + (z-1)mk$ is not less than $k\ell$ then we should take $x = 1 + (z-1)mk \pmod{k\ell}$ and all previously given arguments hold. □

2.4 Group actions

Let G be a group and Ω be a nonempty set. Suppose that for each $\alpha \in \Omega$ and each $x \in G$ we have defined an element of Ω, denoted by αx. In other words,

$$(\alpha, x) \to \alpha x$$

is a function of $\Omega \times G$ into Ω. Then we say that this defines an *action* of G on Ω, or G *acts* on Ω if we have the following:

1. $\alpha e = \alpha$ for all $\alpha \in \Omega$, where e denotes the identity element of G;

2. $(\alpha x)y = \alpha(xy)$ for all $\alpha \in \Omega$ and all $x, y \in G$.

When a group G acts on a set Ω, a point α is moved by elements of G to various other points. The set of these images is called the *orbit* of α under G, and we denote it by

$$\mathrm{Orb}(\alpha, G) = \{\alpha x \mid x \in G\}$$

A kind of dual role is played by the set of elements in G which fix a specified point α. This is called the *stabilizer* of α in G and is denoted

$$\mathrm{Stab}(\alpha, G) = \{x \in G \mid \alpha x = \alpha\}.$$

The important properties of these objects are summarized in the following theorem.

Theorem 2.3. *Suppose that G is a group acting on a set Ω and that $x, y \in G$ and $\alpha, \beta \in \Omega$. Then,*

(a) Two orbits $\mathrm{Orb}(\alpha, G)$ and $\mathrm{Orb}(\beta, G)$ are either equal (as sets) or disjoint, so that the set of all orbits is a partition of Ω into a mutually disjoint subsets.

(b) The stabilizer $\mathrm{Stab}(\alpha, G)$ is a subgroup of G and

$$\mathrm{Stab}(\beta, G) = x^{-1}\,\mathrm{Stab}(\alpha, G)x$$

whenever $\beta = \alpha x$. Moreover

$$\alpha x = \alpha y \Leftrightarrow \mathrm{Stab}(\alpha, G)x = \mathrm{Stab}(\alpha, G)y.$$

(c) $|\,\mathrm{Orb}(\alpha, G)| = |G : \mathrm{Stab}(\alpha, G)|$.

In particular, if G is finite then $|\,\mathrm{Orb}(\alpha, G)||\,\mathrm{Stab}(\alpha, G)| = |G|$.

Proof. If $\delta \in \mathrm{Orb}(\alpha, G)$ then $\delta = \alpha u$ for some $u \in G$. Since ux runs over the elements of G as x runs over G,

$$\mathrm{Orb}(\delta, G) = \{\delta x \mid x \in G\} = \mathrm{Orb}(\alpha, G)$$

Hence, if $\mathrm{Orb}(\alpha, G)$ and $\mathrm{Orb}(\beta, G)$ have any element δ in common, then $\mathrm{Orb}(\alpha, G) =$

$\mathrm{Orb}(\delta, G) = \mathrm{Orb}(\beta, G)$. Since every $\alpha \in \Omega$ lies in at least one orbit, namely $\mathrm{Orb}(\alpha, G)$, this proves *(a)*.

Clearly $e \in \mathrm{Stab}(\alpha, G)$, and whenever $x, y \in \mathrm{Stab}(\alpha, G)$ then $xy^{-1} \in \mathrm{Stab}(\alpha, G)$. Thus $\mathrm{Stab}(\alpha, G)$ is a subgroup. If $\beta = \alpha x$ we also have

$$y \in \mathrm{Stab}(\beta, G) \Leftrightarrow \alpha(xy) = \alpha x \Leftrightarrow xyx^{-1} \in \mathrm{Stab}(\alpha, G)$$

and so $x^{-1} \mathrm{Stab}(\alpha, G)x = \mathrm{Stab}(\beta, G)$. Finally,

$$\alpha x = \alpha y \Leftrightarrow \alpha(xy^{-1}) = \alpha \Leftrightarrow xy^{-1} \in \mathrm{Stab}(\alpha, G)$$

This is equivalent to

$$\mathrm{Stab}(\alpha, G)x = \mathrm{Stab}(\alpha, G)y$$

and *(b)* is proved. Now, *(c)* follows immediately since *b* shows that distinct points in $\mathrm{Stab}(\alpha, G)$ are in bijective correspondence with right cosets of $\mathrm{Stab}(\alpha, G)$ in G, and for finite groups $|G : \mathrm{Stab}(\alpha, G)| = |G|/|\mathrm{Stab}(\alpha, G)|$. □

Definition 2.3. *A group acting on a set Ω is said to be transitive on Ω if it has only one orbit.*

Clearly, G is transitive if for every pair of points $\alpha, \beta \in \Omega$ there exists $x \in G$ such that $\alpha x = \beta$. Suppose that the group G acts on a set Ω and let T be a subset of G. Then we define the set of *fixed* points of T by

$$\mathrm{Fix}(T) := \{\alpha \in \Omega \mid \alpha x = \alpha \ \ for\ all\ x \in T\}$$

There is a simple relationship between the number of orbits of a finite group acting on a finite set and the number of fixed points of its elements. Although it is often referred

inaccurately as the Burnside Lemma, it is actually due to Cauchy and Frobenius.

Theorem 2.4. *Let G be a finite group acting on a finite set Ω. Then G has s orbits on Ω where*

$$s|G| = \sum_{x \in G} |\operatorname{Fix}(x)|.$$

Proof. Consider the set $\mathcal{F} = \{(\alpha, x) \in \Omega \times G \mid \alpha x = \alpha\}$. We shall count the number of elements of $\mathcal{F}$ in two ways. First, suppose that the orbits of G are $\Omega_1, \ldots, \Omega_s$. Then using the orbit-stabilizer property, we have

$$|\mathcal{F}| = \sum_{i=1}^{s} \sum_{\alpha \in \Omega_i} |\operatorname{Stab}(\alpha, G)| = \sum_{i=1}^{s} \sum_{\alpha \in \Omega_i} \frac{|G|}{|\Omega_i|} = \sum_{i=1}^{s} |G| = s|G|$$

Second,

$$|\mathcal{F}| = \sum_{x \in G} |\operatorname{Fix}(x)|.$$

The result follows. □

Further, $\mathbb{Z}_n$ denotes additive group of integers modulo n. By Theorem 2.2, the automorphisms of $\mathbb{Z}_n$ are mappings $\pi_t : \mathbb{Z}_n \to \mathbb{Z}_n$ of the form

$$\pi_t(x) = tx, \quad (x \in \mathbb{Z}_n)$$

where $\gcd(t, n) = 1$. Recall that we denote the automorphism group of $\mathbb{Z}_n$ by $\mathcal{I}(n)$.

Consider the following natural action of the group $\mathcal{I}(n)$ on the additive cyclic group $\mathbb{Z}_n$ by multiplication, $\mathbb{Z}_n \times \mathcal{I}(n) \to \mathbb{Z}_n$,

$$(x, t) \to tx \quad (t \in \mathcal{I}(n),\ x \in \mathbb{Z}_n).$$

Naturally, we can extend this action to k-sets in $\mathbb{Z}_n$. Let $\mathcal{O}_k$ be the collection of k-sets of $\mathbb{Z}_n$. Given a set $A = \{a_1, a_2, \ldots, a_k\}$, we define multiplication of the set A by an element $t \in \mathbb{Z}_n$ in the natural way

$$tA = \{ta_1, ta_2, \ldots, ta_k\}.$$

We consider the following type of group action $\mathcal{O}_k \times \mathcal{I}(n) \to \mathcal{O}_k$ defined as

$$(A, t) \to tA \ \ (t \in \mathcal{I}(n),\ A \in \mathcal{O}_k).$$

If not specified otherwise, the term *action* will be further reserved for the one described above. By Ω_d we denote the set of elements of additive order d in the $\mathbb{Z}_n$. Obviously,

$$\mathbb{Z}_n = \bigcup_{d|n} \Omega_d$$

and $|\Omega_d| = \phi(d)$, where ϕ is Euler's phi function.

2.4.1 Cycle index of $\mathcal{I}(n)$ and orbits of k-sets of $\mathbb{Z}_n$

There are a number of interesting enumerative problems regarding the action of $\mathcal{I}(n)$ on $\mathcal{O}_k$ that can mostly be answered by application of Pólya's theory. There is a significant literature on Pólya's counting theory. For instance, see [14, 3, 4]. Frequently, the main combinatorial problem about a permutation group acting on a set is to determine its *cycle index*. Firstly, we give several basic definitions.

Definition 2.4 (Type of a Permutation)**.** *Let M be a set with $|M| = m$. A permutation $\pi \in S_M$ is of type $(\lambda_1, \lambda_2, \ldots, \lambda_m)$, iff the decomposition of π as the product of disjoint cycles has exactly λ_i cycles of length i, for $i = 1, \ldots, m$. Hence, by $\lambda_i(\pi)$ we mean*

the number of cycles of length i in this decomposition. We write

$$\text{ctype}(\pi) = 1^{\lambda_1} 2^{\lambda_2} \cdots m^{\lambda_m},$$

or

$$\text{ctype}(\pi) = \prod_{i=1}^{m} i^{\lambda_i}.$$

where we adopt a formal product notation.

Definition 2.5 (Cycle Index)**.** *Let P be a set of $|P| = n$ elements and let Γ be a subgroup of S_P. The cycle index of Γ is a polynomial in n indeterminates $x_1, \ldots, x_n$, defined as:*

$$\mathcal{Z}_{(\Gamma,\, P)}(x_1, \ldots, x_n) := \frac{1}{|\Gamma|} \sum_{\gamma \in \Gamma} \prod_{i=1}^{n} x_i^{\lambda_i(\gamma)}.$$

We determine cycle index of the group $\mathcal{I}(n)$ acting on $\mathbb{Z}_n$ and calculate the number of orbits of k-sets of $\mathbb{Z}_n$. The following famous theorem of Pólya [13] was published in 1937.

Theorem 2.5 (Pólya's Theorem)**.** *Let P and F be finite sets with $|P| = n$, and let $\Gamma \leq S_P$. Furthermore let R be a commutative ring over the rationals Q and let w be a mapping $w : F \to R$. Two mappings $f_1, f_2 \in F^P$ are called equivalent, iff there exists some $\gamma \in \Gamma$ such that $f_1 \circ \gamma = f_2$. The equivalence classes are called mapping patterns and are written as $[f]$. For every $f \in F^P$ we define the weight $W(f)$ as product weight*

$$W(f) := \prod_{p \in P} w(f(p)).$$

Any two equivalent f's have the same weight. Thus we may define W([f]) := W(f).

Then the sum of the weights of the patterns is

$$\sum_{[f]} W([f]) = \mathcal{Z}_{(\Gamma,\, P)} \left(\sum_{y \in F} w(y), \sum_{y \in F} w(y)^2, \ldots, \sum_{y \in F} w(y)^n \right).$$

There are extensions of Pólya's theorem to cases with a different definition of the weight function and equivalence classes [3]. We will need the following elementary lemma.

Lemma 2.7. *Let Ω_d be the set of elements of $\mathbb{Z}_n$ of order d. Then,*

$$\Omega_d = \frac{n}{d} \mathcal{I}(d)$$

Also, Ω_d is an orbit under the action of the group $\mathcal{I}(n)$ on $\mathbb{Z}_n$.

Proof. From Lemma 2.3, it is clear that $\Omega_d = \frac{n}{d}\mathcal{I}(d)$. Let x and y be elements of order d. Then $x = (n/d)k_1$ and $y = (n/d)k_2$ where $k_1, k_2 \in \mathcal{I}(d)$. Therefore, there exists $k \in \mathcal{I}(d)$ such that $k_1 = kk_2$. On the other hand, Lemma 2.4 asserts the existence of an element $h \in \mathcal{I}(n)$ such that $h \equiv k \pmod{d}$. Clearly $k_1 \equiv hk_2 \pmod{d}$. By multiplying both sides by (n/d) we have $x = hy \pmod{n}$. Thus, $\mathcal{I}(n)$ is transitive on the set of elements of (additive) order d. □

Note that mappings from $\mathcal{I}(n)$ fix the sets Ω_d for each $d \mid n$. In the following lemma, we prove that the group $\mathcal{I}(2^m)$ is generated by π_3 and π_{-1}.

Lemma 2.8. *The order of the element 3 is 2^{m-2} modulo 2^m if $m \geq 3$. The elements from Ω_{2^m} are represented by*

$$(-1)^a 3^b \pmod{2^m} \text{ where } a \in \{0,1\} \text{ and } b \in \{0,1,\ldots,2^{m-3}\}.$$

Proof. We note that

$$\begin{aligned} 3^2 &= 1+8, \\ 3^4 &= 1+16+32t, \text{ and} \\ 3^8 &= 1+32+64u \end{aligned}$$

for integers t and u. By induction, 3 is of order 2^{m-2} modulo 2^m, if $m \geq 3$. For the second part, it is enough to show that

$$(-1)3^{b_1} \not\equiv 3^{b_2} \pmod{2^k}, \text{ for } b_1, b_2 \in \{0, 1, \ldots, 2^{k-3}\}.$$

If not so, we would have

$$8 \mid 3^b + 1$$

where $b = |b_1 - b_2|$. This is not possible since $3^b + 1 \equiv 2 \text{ or } 4 \pmod{8}$. □

Lemma 2.9. *Let f_j, g_j be the mappings from $\mathcal{I}(2^m)$ to $\mathcal{I}(2^m)$, $m \geq 3$ defined by*

$$f_j(x) := 3^j x \text{ and } g_j(x) := -3^j x,$$

for $j \geq 1$. Let s_j be the order of $f_j \in \mathcal{I}(2^m)$. Then

$$\text{ctype}(f_j) = (s_j^{u_j})$$

where $u_j = 2^{m-1}/s_j$. Note that $\text{ctype}(g_j) = \text{ctype}(f_j)$.

Proof. Consider the mapping $f_j \in \mathcal{I}(2^m)$. Let $x_0 \in \mathcal{I}(2^m)$ be an arbitrary element. Since $f_j^s(x_0) \equiv x_0 \pmod{2^m}$ if and only if $s \equiv 0 \pmod{s_j}$, then it is clear that every cycle must contain exactly s_j elements. Since the order of g_j is equal to order f_j, the

conclusion $\text{ctype}(g_j) = \text{ctype}(f_j)$ follows easily. □

The following lemma explains how the number of orbits of the permutation group $\mathcal{I}(n)$ acting on $\mathcal{O}_k$ can be determined once the cycle index of $\mathcal{I}(n)$ acting on $\mathbb{Z}_n$ is determined.

Lemma 2.10. *The number of orbits of the action of $\mathcal{I}(n)$ on the $\mathcal{O}_k$ is equal to the coefficient of x^k in*

$$\mathcal{Z}_{(\mathcal{I}(n),\,\mathbb{Z}_n)}(1+x, 1+x^2, \ldots, 1+x^n).$$

Proof. We apply Pólya's theorem 2.5. Let $F = \{\text{in}, \text{out}\}$ and $P = \{0, 1, \ldots, n-1\}$. This means that the functions $f \in F^P$ are actually the characteristic functions of subsets in $\mathbb{Z}_n$. Let us define $w(\text{in}) = x$ and $w(\text{out}) = 1$. Then, the weight of characteristic function f of a k-set is

$$W(f) = x^k$$

Thus, the number of orbits of k-sets under the given group action is the coefficient of x^k in

$$\mathcal{Z}_{(\mathcal{I}(n),\,\mathbb{Z}_n)}(1+x, 1+x^2, \ldots, 1+x^n).$$

□

Therefore, we need to determine the cycle index of $\mathcal{I}(n)$ acting on $\mathbb{Z}_n$. We start with some basic cases. The following lemma considers the cycle index of the group $\mathcal{I}(2^m)$. This is a special case since $\mathcal{I}(2^m)$ for $m \geq 3$ is not a cyclic group, unlike the groups $\mathcal{I}(p^m)$, where p is an odd prime number [22]. Note that the sets of integers in $\mathcal{I}(2^m)$ and Ω_{2^m} in $\mathbb{Z}_{2^m}$ are equal.

Lemma 2.11. *The cycle index* $\mathcal{Z} = \mathcal{Z}_{(\mathcal{I}(2^m),\,\mathbb{Z}_{2^m})}(x_1, x_2, \ldots, x_{2^m})$ *of the permutation group* $\mathcal{I}(2^m)$ *acting on* $\mathbb{Z}_{2^m}$ *is*

$$\begin{aligned}
\mathcal{Z} &\equiv x_1^2 \ \textit{if } m = 1, \\
\mathcal{Z} &\equiv \frac{1}{2}(x_1^4 + x_1^2 x_2) \ \textit{if } m = 2, \textit{ and} \\
\mathcal{Z} &\equiv \frac{1}{4}(x_1^8 + 2x_1^2 x_2^3 + x_1^4 x_2^2) \ \textit{if } m = 3, \textit{ and} \\
\mathcal{Z} &\equiv \frac{1}{2^{m-1}}(P + Q) \ \textit{if } m \geq 4, \textit{ where} \\
P &\equiv x_1^{2^m} + 2^{m-3} x_2 \prod_{i=0}^{m-2} x_{2^i}^2 + \sum_{i=0}^{m-4} 2^i x_1^{2^{m-2-i}} \prod_{s=0}^{i+1} x_{2^s}^{2^{m-2-i}}, \\
Q &\equiv x_1^2 x_2^{2^m-2} + 2^{m-3} x_1^2 \prod_{i=0}^{m-2} x_{2^i}^2 + \sum_{i=0}^{m-4} 2^i x_1^2 x_2^{2^{m-1-i}-1} \prod_{s=1}^{i} x_{2^{s+1}}^{2^{m-2-i}}.
\end{aligned}$$

Proof. The first three cases are trivial. In order to determine the cycle type of elements of $\mathcal{I}(2^m)$, for $m \geq 3$ we begin with one simple observation. Let us see the cycle type of permutation π_3 in $\mathbb{Z}_{2^3}$. Obviously,

$$\text{ctype}(\pi_3) = (2^3 1^2).$$

Note that order of π_3 in $\mathcal{I}(2^3)$ is 2. There are exactly two elements in $\mathcal{I}(2^4)$ congruent to 3 modulo 2^3. Both of these, 3 and 11, have the same order 4 in $\mathcal{I}(2^4)$. It is not hard to see that π_3 and π_{11} must act identically on the cyclic subgroup $H \leq \mathbb{Z}_{2^4}$ of order 8,

$$H = 2\{0, 1, 2, 3, 4, 5, 6, 7\}$$

just as π_3 is acting on $\mathbb{Z}_{2^3}$. Therefore, it is only necessary to determine how π_3 and π_{11} act on $\mathcal{I}(2^4)$. According to Lemma 2.9, they split $\mathcal{I}(2^4)$ into 2 orbits. Therefore,

$$\text{ctype}(\pi_3) = \text{ctype}(\pi_{11}) = (4^2 2^3 1^2).$$

Similarly, when we consider $\mathbb{Z}_{2^5}$ we see that

$$\text{ctype}(\pi_3) = \text{ctype}(\pi_{11}) = \text{ctype}(\pi_{19}) = \text{ctype}(\pi_{27}) = (8^2 4^2 2^3 1^2).$$

Using the same approach one can inductively determine the cycle types of all elements in $\mathcal{I}(2^m)$. Namely, for every element x of $\mathcal{I}(2^k)$, there are exactly two elements x_1 and x_2 from $\mathcal{I}(2^{k+1})$ such that

$$x_1 \equiv x \pmod{2^k} \quad \text{and} \quad x_2 \equiv x \pmod{2^k}.$$

The cycle type of x_1 and x_2 on the set of elements that belong to the cyclic subgroup of $\mathbb{Z}_{2^{k+1}}$ of order 2^k is the same as x has on $\mathcal{I}(2^k)$ and the cycle type on $\mathcal{I}(2^{k+1})$ is determined by Lemma 2.9. It is not hard to see that $\text{ord}(x_1) = \text{ord}(x_2)$, considering $x_1, x_2 \in \mathcal{I}(2^{k+1})$ is twice $\text{ord}(x)$, considering $x \in \mathcal{I}(2^k)$, when $x \not\equiv \pm 1 \pmod{2^k}$. When $x = 1$ then we have $\text{ctype}(x_1) = (1^{2^{k+1}})$ and $\text{ctype}(x_2) = (1^{2^k} 2^{2^{k-1}})$. Similarly, when $x \equiv -1 \pmod{2^k}$, then $\text{ctype}(x_1) = \text{ctype}(x_2) = (1^2 2^{2^k-1})$.

Hence, for elements of $\mathcal{I}(2^m)$ that correspond to $3^b \pmod{2^m}$ we have the following polynomial

$$P \equiv x_1^{2^m} + 2^{m-3} x_2 \prod_{i=0}^{m-2} x_{2^i}^2 + \sum_{i=0}^{m-4} 2^i x_1^{2^{m-2-i}} \prod_{s=0}^{i+1} x_{2^s}^{2^{m-2-i}}$$

This can be easily proved by induction. For those elements from $\mathcal{I}(2^m)$ that are congruent to $-3^b \pmod{2^m}$, the corresponding polynomial is

$$Q \equiv x_1^2 x_2^{2^m-2} + 2^{m-3} x_1^2 \prod_{i=0}^{m-2} x_{2^i}^2 + \sum_{i=0}^{m-4} 2^i x_1^2 x_2^{2^{m-1-i}-1} \prod_{s=1}^{i} x_{2^{s+1}}^{2^{m-2-i}}.$$

Thus, the cycle index of $\mathcal{I}(2^m)$ acting on $\mathbb{Z}_{2^m}$ is the sum of those two polynomials

divided by the order of $\mathcal{I}(2^m)$, that is

$$\mathcal{Z}_{(\mathcal{I}(2^m),\,\mathbb{Z}_{2^m})}(x_1, x_2, \ldots, x_{2^m}) \equiv \frac{1}{2^{m-1}}(P + Q)$$

□

The following lemma considers the case of $\mathcal{I}(p^m)$, where p is an odd prime number. As it has been already noted, this group is cyclic and therefore it is much easier to find its cycle index.

Lemma 2.12. *Let p be an odd prime. The cycle type of the permutation group $\mathcal{I}(p^m)$ acting on $\mathbb{Z}_{p^m}$ is*

$$\mathcal{Z}_{(\mathcal{I}(p^m),\,\mathbb{Z}_{p^m})}(x_1, x_2, \ldots, x_{p^m}) = \frac{1}{r}\sum_{k=1}^{r} x_1 \prod_{i=1}^{m} x_{u(i,k)}^{v(i,k)},$$

where $r = p^{m-1}(p-1)$, $v(i,k) = \gcd(k, p^{i-1}(p-1))$ and

$$u(i,k) = \frac{p^{i-1}(p-1)}{v(i,k)}.$$

Proof. It is well known that in the case of odd prime p, the automorphism group $\mathcal{I}(p^m)$ is cyclic [22]. Let β be a generator of $\mathcal{I}(p^m)$. According to Lemma 2.7, $\mathcal{I}(p^m)$ is transitive on each set Ω_d, for $d \mid p^m$. Note that $|\Omega_{p^i}| = p^{i-1}(p-1)$ and $|\mathcal{I}(p^m)| = p^{m-1}(p-1)$. Now it is easy to see that

$$\mathrm{ctype}(\beta) = x_1 \prod_{i=1}^{m} x_{\phi(p^i)}^{1}.$$

Since every element in $\mathcal{I}(p^m)$ is a power of β, the rest of the conclusion follows trivially. □

2.4.2 Cycle index of the direct product of permutation groups

Since we found the cycle indexes of all groups $\mathcal{I}(p^m)$ when p is a prime number, there is a natural question whether there is a way to combine them together in order to obtain the cycle index of $\mathcal{I}(n)$, where n is the product of those prime power components. Hence, we need something like the cycle index of the direct product of permutation groups.

Let G_1, G_2 be permutation groups acting on sets X_1, X_2 respectively. Let $G = G_1 \times G_2$ be the direct product of groups and $X = X_1 \times X_2$ the cartesian product of corresponding sets. For an element $x = (x_1, x_2)$ of X and an element $g = (g_1, g_2)$ of G, we define the action of g on x by

$$(g, x) \mapsto (x_1 g_1, x_2 g_2),$$

Evidently, G is a permutation group on X. Let P and Q be polynomials

$$P(x_1, x_2, \ldots, x_u) = \sum a_{i_1 i_2 \ldots i_u} x_1^{i_1} x_2^{i_2} \ldots x_u^{i_u},$$

$$Q(x_1, x_2, \ldots, x_v) = \sum b_{j_1 j_2 \ldots j_v} x_1^{j_1} x_2^{j_2} \ldots x_v^{j_v}.$$

In [7] the following product operator was defined

$$P \circledast Q = \sum a_{i_1 i_2 \ldots i_u} b_{j_1 j_2 \ldots j_v} \prod_{\substack{1 \le l \le u \\ 1 \le m \le v}} (x_l^{i_1} \circledast x_m^{j_m}),$$

where

$$x_l^{i_1} \circledast x_m^{j_m} = x_{\mathrm{lcm}(l,m)}^{i_1 j_m \gcd(l,m)}.$$

We need the following lemma. For the proof, see [7] and [21].

Lemma 2.13. *The cycle index of the natural action of permutation group $G_1 \times G_2$ on $X_1 \times X_2$ induced by actions G_1 on X_1 and G_2 on X_2 can be expressed as:*

$$\mathcal{Z}_{(G_1 \times G_2,\, X_1 \times X_2)} = \mathcal{Z}_{(G_1,\, X_1)} \circledast \mathcal{Z}_{(G_2,\, X_2)}.$$

Let $n = \prod_{i=1}^{s} p_i^{\alpha_i}$. Applying the ring isomorphism

$$\mathbb{Z}_n \cong \bigoplus_{i=1}^{s} \mathbb{Z}_{p_i^{\alpha_i}},$$

it follows that

$$\mathcal{I}(n) \cong \bigoplus_{i=1}^{s} \mathcal{I}(p_i^{\alpha_i}).$$

Hence, according to Lemma 2.13, we have

$$\mathcal{Z}_{(\mathcal{I}(n),\, \mathbb{Z}_n)} = \mathcal{Z}_{(\mathcal{I}(p_1^{\alpha_1}),\, \mathbb{Z}_{p_1^{\alpha_1}})} \circledast \mathcal{Z}_{(\mathcal{I}(p_2^{\alpha_2}),\, \mathbb{Z}_{p_2^{\alpha_2}})} \circledast \cdots \circledast \mathcal{Z}_{(\mathcal{I}(p_s^{\alpha_s}),\, \mathbb{Z}_{p_s^{\alpha_s}})}.$$

Since cycle indices of prime power components are given in Lemma 2.11 and Lemma 2.12, the cycle index $\mathcal{Z}_{(\mathcal{I}(n),\, \mathbb{Z}_n)}$ can be calculated as above. Thus, in order to find the number of orbits in the action of $\mathcal{I}(n)$ on $\mathcal{O}_k$ we just need to apply Lemma 2.10.

2.4.3 Stabilizer of k-sets of $\mathbb{Z}_n$

Let $A \subseteq \mathbb{Z}_n$ be an arbitrary k-set. One problem we are interested in is a computational procedure for finding the stabilizer of A under the action of $\mathcal{I}(n)$ on k-sets. Clearly, we would like to have a more sophisticated approach than exhaustive search through all elements of the group $\mathcal{I}(n)$. Another problem we consider is to determine whether

two k-sets A and B belong to the same orbit. Let

$$\mathcal{D}_A = \{d \mid A \cap \Omega_d \neq \emptyset,\ d \mid n\}.$$

Let $\mathrm{Stab}(A, \mathcal{I}(n))$ denote the set of automorphisms from $\mathcal{I}(n)$ that fix A, that is

$$\mathrm{Stab}(A, I(n)) = \{h \in \mathcal{I}(n) \mid h(A) = A\}.$$

Suppose that $\mathcal{D}_A = \{d_1, d_2, \ldots, d_u\}$. Clearly, it follows that

$$A = \bigcup_{i=1}^{u} A \cap \Omega_{d_i},$$

where this union is disjoint. This implies

$$\mathrm{Stab}(A, \mathcal{I}(n)) = \bigcap_{i=1}^{u} \mathrm{Stab}(A \cap \Omega_{d_i}, \mathcal{I}(n)).$$

Since $\Omega_d = \frac{n}{d}\mathcal{I}(d)$ by Lemma 2.7, it makes sense to define a set A_d in the following way

$$A \cap \Omega_d = \frac{n}{d} A_d.$$

Note that A_d is a subset of multiplicative group $\mathcal{I}(d)$. The idea is to relate $\mathrm{Stab}(A_d, \mathcal{I}(d))$ and $\mathrm{Stab}(A \cap \Omega_d, \mathcal{I}(n))$.

Lemma 2.14. *Let $\mathcal{O}_m$ be the collection of all subsets of size m of a finite group G. Consider the group action $\mathcal{O}_m \times G \to \mathcal{O}_m$ defined as*

$$(Y, g) \to Yg, \quad (Y \in \mathcal{O}_m,\ g \in G).$$

Let $H = \mathrm{Stab}(U, G)$, for a particular $U \in \mathcal{O}_m$. Then, there exist $U_0 \subseteq U$ such that U

is a disjoint union of some left cosets of H

$$U = \bigcup_{u \in U_0} uH.$$

For any $w \in U$ *it holds that* $H \subseteq w^{-1}U$.

Proof. Note that $H = \mathrm{Stab}(U, G)$ is a subgroup group G. For arbitrary $u_1 \in U$, it is clear that $u_1 H \subseteq U$. If $u_1 H = U$ we are done, otherwise there exists $u_2 \in U \setminus u_1 H$ such that $u_2 H \cap u_1 H = \emptyset$. This process must be finite, so $U_0 = \{u_1, u_2, \ldots, u_k\}$ and then

$$U = \bigcup_{u \in U_0} uH.$$

Thus, U could be represented as the disjoint union of some of the left cosets of H. Suppose that $h \in H$ and $w \in U$ are arbitrary elements of H and U respectively. Then $wh \in U$ and therefore $h \in w^{-1}U$. Hence, $H \subseteq w^{-1}U$ for each $w \in U$. □

The following lemma closely describes the nature of elements, that are contained in the stabilizer $\mathrm{Stab}(A \cap \Omega_d, \mathcal{I}(n))$. Namely, it shows that the stabilizer is the disjoint union of some $\mathcal{I}_d^t(n)$ sets. This lemma is the heart of the algorithm for finding the stabilizer of a k-set that will be given later.

Lemma 2.15. *Let* $V = \mathrm{Stab}(A \cap \Omega_d, \mathcal{I}(n))$ *and* $S = \mathrm{Stab}(A_d, \mathcal{I}(d))$ *where* $d \in \mathcal{D}_A$. *Then it holds*

$$V = \bigcup_{t \in S} \mathcal{I}_d^t(n).$$

Proof. Let

$$A \cap \Omega_d = \frac{n}{d}\{w_1, w_2, \ldots, w_l\}.$$

Then,

$$A_d = \{w_1, w_2, \ldots, w_l\}.$$

Let $x \in V$ be an arbitrary element. Let $x \equiv t \ (mod\ d)$. As $x \in \mathcal{I}_d^t(n)$ by definition, it needs to be shown that $t \in S$. From

$$\frac{n}{d} w_i x \equiv \frac{n}{d} w_j \ (mod\ n)$$

it follows that $w_i x \equiv w_j \pmod{d}$. Hence, $w_i t \equiv w_j \pmod{d}$ and we see that t just permutes the elements of A_d, so $t \in S$. We have proved that

$$V \subseteq \bigcup_{t \in S} \mathcal{I}_d^t(n).$$

Let us prove the opposite inclusion. If $y \in \mathcal{I}_d^t(n),\ t \in S$ then $w_i y \equiv w_j \ (mod\ d)$. From this, it is clear that

$$\frac{n}{d} w_i y \equiv \frac{n}{d} w_j \ (mod\ n),$$

so $y \in V$ which concludes the proof. □

The following corollary relates sizes of $\mathrm{Stab}(A \cap \Omega_d, \mathcal{I}(n))$ and $\mathrm{Stab}(A_d, \mathcal{I}(d))$.

Corollary 2.3. *Let $V = \mathrm{Stab}(A \cap \Omega_d, \mathcal{I}(n))$ and $S = \mathrm{Stab}(A_d, \mathcal{I}(d))$, where $d \in \mathcal{D}_A$. Then,*

$$|V| = \frac{\phi(n)}{\phi(d)} |S|.$$

Proof. From Lemma 2.15 we have that

$$V = \bigcup_{t \in S} \mathcal{I}_d^t(n).$$

By Lemma 2.5 it follows that

$$|\mathcal{I}_d^t(n)| = \frac{\phi(n)}{\phi(d)}$$

for each $t \in S$. This concludes the proof. □

Example 2.1. *Let* $A = \{1, 3, 4, 5, 10, 25, 27, 40\}$ *considered as a subset of* $\mathbb{Z}_{60}$ *and* $d = 12$. *Thus, we have*

$$A \cap \Omega_{12} = \{5, 25\}.$$

Therefore, $A_{12} = \{1, 5\}$. *It is easy to see that* $\mathrm{Stab}(A_{12}, \mathcal{I}(12)) = \{1, 5\}$. *According to Lemma 2.15*

$$\mathrm{Stab}(\{5, 25\}, \mathcal{I}(60)) = \mathcal{I}_{12}^{1}(60) \cup \mathcal{I}_{12}^{5}(60) = \{1, 13, 37, 49\} \cup \{17, 29, 41, 53\}.$$

Now, we are ready to give an algorithm that finds $\mathrm{Stab}(A, \mathcal{I}(n))$. As we already saw,

$$\mathrm{Stab}(A, \mathcal{I}(n)) = \bigcap_{i=1}^{u} \mathrm{Stab}(A \cap \Omega_{d_i}, \mathcal{I}(n)).$$

Hence, $\mathrm{Stab}(A, \mathcal{I}(n)) \subseteq \mathrm{Stab}(A \cap \Omega_d, \mathcal{I}(n))$ for each $d \in \mathcal{D}_A$. Therefore, it is clear that we can fix a particular $d \in \mathcal{D}_A$ and then single out the elements that fix A from the $\mathrm{Stab}(A \cap \Omega_d, \mathcal{I}(n))$. Later, we will explain how to choose $d \in \mathcal{D}_A$ in order to find $\mathrm{Stab}(A, \mathcal{I}(n))$ most efficiently. According to Lemma 2.14, A_d is disjoint union of some cosets of $\mathrm{Stab}(A_d, \mathcal{I}(d))$. Suppose that

$$\mathrm{Stab}(A_d, \mathcal{I}(d)) = \{t_1, t_2, \ldots, t_r\}.$$

Then, by Lemma 2.7 we have that

$$\mathrm{Stab}(A \cap \Omega_d, \mathcal{I}(n)) = \bigcup_{i=1}^{r} \{x \in \mathcal{I}(n) \mid x \equiv t_i \ (mod\ d)\}.$$

Obviously, $\mathrm{Stab}(A \cap \Omega_d, \mathcal{I}(n))$ is not hard to generate once $\mathrm{Stab}(A_d, \mathcal{I}(d))$ is known.

We give a rough estimate of the computational cost of finding $\mathrm{Stab}(A, \mathcal{I}(n))$. Let $f(U)$ be a function that represents the computational cost of checking if a single

element fixes set U. It is not hard to see that $f(U) \leq c_1|U|^2$, for some real constant c_1.

According to Lemma 2.14, it holds that $\mathrm{Stab}(A_d, \mathcal{I}(d)) \subseteq w^{-1}A_d$ for any $w \in A_d$. Therefore $|\mathrm{Stab}(A_d, \mathcal{I}(d))| \leq |A_d|$. Obviously, $\mathrm{Stab}(A_d, \mathcal{I}(d))$ could be found by going through the elements of $w^{-1}A_d$ and simply checking if they fix A_d. This could be done in at most $|A_d|f(A_d)$ operations. After $\mathrm{Stab}(A \cap \Omega_d, \mathcal{I}(n))$ is generated, we need to check which of those elements fix A. This could be done in at most $|\mathrm{Stab}(A \cap \Omega_d, \mathcal{I}(n))|f(A)$ operations.

Note that, if $\mathrm{Stab}(A_d, \mathcal{I}(d))$ is given, the generation of $\mathrm{Stab}(A \cap \Omega_d, \mathcal{I}(n))$ costs less than $c_2|A_d|(n/d)$, for some real constant c_2, according to Lemma 2.15.

Since

$$|\mathrm{Stab}(A \cap \Omega_d, \mathcal{I}(n))| = \frac{\phi(n)}{\phi(d)}|\mathrm{Stab}(A_d, \mathcal{I}(d))| \leq \frac{\phi(n)}{\phi(d)}|A_d|$$

it is reasonable to choose $d \in \mathcal{D}_A$ for which

$$|A_d|^3 + \frac{\phi(n)}{\phi(d)}|A_d||A|^2 + |A_d|\frac{n}{d}$$

is the smallest, although this analysis could be more sophisticated if c_1, c_2 are included. Thus, we just need to find the set $\mathcal{D}_A$ and the sets A_d, for each $d \in \mathcal{D}_A$. Given a set A, the set $\mathcal{D}_A$ could be easily found simply by taking $\gcd(a, n)$ for each $a \in A$. Finally, A is partitioned into the collection of its subsets where each subset has the property that its elements have the same gcd with n. Here, we assume that $0 \notin A$, since everything fixes 0 so we can safely exclude it. If $A = \{0\}$ then clearly, $\mathrm{Stab}(A, \mathcal{I}(n)) = \mathcal{I}(n)$. We present pseudo-code for the algorithm consisting of two functions, the auxilliary function **Fix**(B,C,m) and the main function **Stab**(A,n). The function **Fix**(B,C,m) outputs all elements from the set B that fix set C in $\mathbb{Z}_m$. The function **Stab** uses two elementary functions **Min**(seq) and **Index**(t,seq) that

return the minimum of the input sequence and the index of an element t in the input sequence.

There is a straightforward procedure for finding the coset representatives (transversal) of $\mathrm{Stab}(A, \mathcal{I}(n))$ in $\mathcal{I}(n)$. Consequently, that transversal can be used for finding the orbit of A under $\mathcal{I}(n)$. As mentioned earlier, we are interested in the problem of determining whether two k-sets A and B belong to the same orbit. One inefficient way would be simply constructing the orbit of A and checking if B is inside. However, it is possible to do it more efficiently using a method similar to the one demonstrated for finding $\mathrm{Stab}(A, \mathcal{I}(n))$. First, it is clear that if A and B are in the same orbit, it must be $|A| = |B|$, $\mathcal{D}_A = \mathcal{D}_B = \mathcal{D}$ and $|A_d| = |B_d|$ for all $d \in \mathcal{D}$. These would be a necessary conditions and the first check for two sets to belong in the same orbit.

If any of those conditions are not satisfied, A and B are not in the same orbit. Let us suppose that all these conditions are indeed satisfied and let $d \in \mathcal{D}$ be fixed. If there exists $t \in \mathcal{I}(n)$, for which $tA = B$, then for $w' \in \mathcal{I}(d)$, such that $w \equiv t \ (mod\ d)$, it holds that $tA_d = B_d$. If $1 \in A_d$, then $t \in B_d$. Otherwise, $t \in a^{-1}B_d$ for any particular $a \in A_d$. Therefore, after d has been chosen, by going through $\mathcal{I}_d^t(n)$, $t \in a^{-1}B_d$ it is possible to check whether A and B are in the same orbit or not. Hence, it seems reasonable to take $d \in \mathcal{D}$ such that $|A_d|$ is the smallest. We present a pseudo-code of the function $\mathbf{IsInOrbit}(A, B, n)$. The function outputs *true* if two sets A and B are in the same orbit. Otherwise it outputs *false*.

Function `Fix`(B,C,m)

```
K := {};
for b ∈ B do
    S := {};
    for c ∈ C do
        pom := bc mod m;   S := S ∪ {pom};
    if S = C then
        K := K ∪ {b};
return K;
```

Function `Stab(`A`,`n`)`

$\mathcal{D}_A := [\,]$;

`/* Assume that set` $\mathcal{D}_A$ `has been created */`

for $d \in \mathcal{D}_A$ **do**
  $A[d] := \{\}$;

for $a \in A$ **do**
  $uu := \gcd(a, n)$; $d := n/uu$; $pom := a/uu$; $A[d] := A[d] \cup \{pom\}$;

`/* Sets` A_d `have been created */`

$opt := [\,]$;

for $d \in \mathcal{D}_A$ **do**
  $rr := |A[d]|^3 + \frac{\phi(n)}{\phi(d)}|A[d]||A|^2 + \frac{n}{d}|A[d]|$; $opt := [opt, rr]$;

ll:=**Index**(**Min**(opt),opt);

`/* Choosing` $d \in \mathcal{D}_A$ `such that` $|A_d|^3 + \frac{\phi(n)}{\phi(d)}|A_d||A|^2 + |A_d|\frac{n}{d}$ `is the smallest. The one that has been found is denoted by` d_0. `*/`

$d_0 := \mathcal{D}_A[ll],\ S := A[d_0]$;

if $1 \notin S$ **then**
  $S := S[1]^{-1}S$;

SF:=**Fix**(S,S,d_0);

`/* SF is actually` $\mathrm{Stab}(A_{d_0}, \mathcal{I}(d_0))$ `*/`

$U := \{\}$;

`/* The following lines are just implementation of Lemma 2.15 */`

for $el \in SF$ **do**
  for $j \in [1..\frac{n}{d_0}]$ **do**
    $pcm := (el + jd_0)\ mod\ n$;
    if $\gcd(pcm, n) = 1$ **then**
      $U := U \cup \{pcm\}$;

Stab:=**Fix**(U, A, n);

return Stab;

Function `IsInOrbit`(A,B,n)

if $|A| \neq |B|$ **then**
  return *false*;

if $\mathcal{D}_A \neq \mathcal{D}_B$ **then**
  return *false*
$D := [\mathcal{D}_A]$;

for $d \in D$ **do**
  $A[d] := B[d] := \{\}$;

for $a \in A$ **do**
  $uu := \gcd(a, n)$; $d := n/uu$; $pom := a/uu$; $A[d] := A[d] \cup \{pom\}$;

for $b \in B$ **do**
  $uu := \gcd(b, n)$; $d := n/uu$; $pom := b/uu$; $B[d] := B[d] \cup \{pom\}$;
$opt1 := [\,]$; $opt2 := [\,]$;

for $d \in D$ **do**
  $opt1 := [opt1, |A_d|]$; $opt2 := [opt2, |B_d|]$;

if $opt1 \neq opt2$ **then**
  return *false*;
$ll :=$ **Index**(**Min**($opt1$)); $d_o := D[ll]$; $S := A[d_o]$;

if $1 \notin S$ **then**
  $S := S[1]^{-1}B[d_o]$;

for $el \in S$ **do**

  for $j \in [1..\frac{n}{d_o}]$ **do**
    $w := (el + jd_o)\ mod\ n$;

    if $\gcd(w, n) = 1$ **then**

      if $wA = B$ **then**
        return *true*;

return *false*;

Chapter 3

Orbits of k-complete Sets

In this section, we introduce the notion of a *k-complete set*, that is, a set of nonnegative integers that contains exactly one number from each of the residue classes modulo k. The special importance of this type of sets will be emphasized later, regarding the group factorizations of $\mathbb{Z}_{mn}$, when m and n are relatively prime natural numbers. Since a k-complete set is a subset of size k, every result from the previous chapter regarding an arbitrary k-set, is applicable to a k-complete set as well.

First, we give some results regarding the representation of the group $\mathcal{I}(n)$ as a permutation group on n points. The correlation of permutation representations of groups $\mathcal{I}(m)$, $\mathcal{I}(n)$ with $\mathcal{I}(mn)$ when $\gcd(m,n) = 1$ will be considered as a particularly interesting case.

3.1 The orbit signature

One of the frequent computational problems is to store orbits of a particular group action in an efficient way. Since every orbit is completely determined by its representative, it would be enough to store only orbit representatives and the function that describes

the action of the group G on the set Ω. On the other hand, for an efficient reconstruction of a particular orbit, it could be useful to have information on its size in advance. Hence, we introduce the notion of *orbit signature* of a group G acting on a set Ω. Let $g \in G$ be an arbitrary element. Consider a mapping $\pi_g : \Omega \to \Omega$ defined by

$$\pi_g(\alpha) = g \cdot \alpha.$$

Basically, π_g describes the action of g on Ω. In particular, π_g is a bijection and thus a permutation on Ω. Hence, the cycles in the permutation representation of π_g are essentially the orbits of the group $H = \langle g \rangle$ acting on Ω.

Definition 3.1. *Let G be a group acting on a finite set Ω and let*

$$\Omega = \bigcup_{i=1}^{k} O_k$$

be the partition of Ω into the k orbits induced by that action. We define an orbit signature of G, or shortly $\mathrm{osig}(G)$ *as*

$$\mathrm{osig}(G) := [\alpha_1, r_1][\alpha_2, r_2] \cdots [\alpha_k, r_k],$$

where α_i is a representative of the orbit O_i and $r_i = |O_i|$, for $1 \leq i \leq k$.

Note that the choice of representatives of the orbits O_i in the previous definition is arbitrary. This means that in general there could be many ways to write the orbit signature of a particular group G. We now define $\mathrm{osig}(h)$ for $h \in G$.

Definition 3.2. *Let G be a group action on a finite set Ω and let $h \in G$ be an arbitrary element. Then*

$$\mathrm{osig}(h) := \mathrm{osig}(H)$$

where $H = \langle h \rangle$ and we assume the corresponding action of the group H on the set Ω.

We consider the natural permutation representation of $\mathcal{I}(n)$ on n points. For every $a \in \mathcal{I}(n)$, a permutation on n points is constructed by the mapping $\pi_a(x) = ax$ where $x \in \{0, 1, \ldots, n-1\}$. This gives a permutation representation

$$a \rightarrow \pi_a$$

where $a \in \mathcal{I}(n)$. The permutation π_a, given in *cycle* form is as follows:

$$(a_1, aa_1, \ldots, a^{r_1-1}a_1)(a_2, aa_2, \ldots, a^{r_2-1}a_2)\ldots(a_l, aa_l, \ldots, a^{r_l-1}a_l),$$

where $r_1 + r_2 + \ldots + r_l = n$. Since zero is always fixed, we will assume that $a_l = 0$ and therefore $r_l = 1$. Thus, the orbit signature of π_a is

$$\mathrm{osig}(a) = [a_1, r_1][a_2, r_2]\ldots[a_l, r_l],$$

or, for short

$$\mathrm{osig}(a) = \prod_{i=1}^{l}[a_i, r_i].$$

Note that we have just identified π_a with a here. In particular we call the components $[a_i, r_i]$ of the signature $\mathrm{osig}(a)$, the *factors of the orbit signature*. Let us define the length $|\,\mathrm{osig}(a)|$ of the orbit signature as

$$|\,\mathrm{osig}(a)| = r_1 + r_2 + \ldots + r_l.$$

In what follows, by an *orbit of* $a \in \mathcal{I}(n)$ we will always mean an orbit of the cyclic group $\langle a \rangle$ acting by multiplication on $\mathbb{Z}_n$.

Example 3.1. *Consider the element* $5 \in \mathcal{I}(18)$. *We have*

$$\pi_5 = (1,\ 5,\ 7,\ 17,\ 13,\ 11)(2,\ 10,\ 14,\ 16,\ 8,\ 4)(3,\ 15)(6,\ 12)(9)(0).$$

Hence,

$$\text{osig}(5) = [1,6][2,6][3,2][6,2][9,1][0,1].$$

3.2 Orbit signature of elements of $\mathcal{I}(mn)$ where $\gcd(m,n) = 1$

Consider an element $g \in \mathcal{I}(mn)$ such that

$$g \equiv a \pmod{m}, \quad g \equiv b \pmod{n}.$$

We explore how the orbit signature of an element $g \in \mathcal{I}(mn)$ depends on the orbit signatures of $a \in \mathcal{I}(m)$ and $b \in \mathcal{I}(n)$. In general, we are interested in obtaining the representation of π_g on mn points, given representations on m and n points where m and n are relatively prime.

Theorem 3.1. *Let* m *and* n *be two positive, relatively prime integers and let*

$$\text{osig}(a) = \prod_{i=1}^{l} [a_i, r_i], \quad \text{osig}(b) = \prod_{j=1}^{t} [b_j, h_j]$$

be the orbit signatures of the elements $a \in \mathcal{I}(m)$ *and* $b \in \mathcal{I}(n)$ *respectively. Then, for* $g \in \mathcal{I}(mn)$, *such that* $g \equiv a \pmod{m}$, $g \equiv b \pmod{n}$ *it follows that*

$$\text{osig}(g) = \prod_{i=1}^{l} \prod_{j=1}^{t} \prod_{s=0}^{u(i,j)} [w_{ijs}, q_{ij}]$$

where w_{ijs} is the element of $\mathbb{Z}_{mn}$ such that

$$w_{ijs} \equiv a_i a^s \pmod{m}$$

$$w_{ijs} \equiv b_j \pmod{n}$$

and $u_{ij} = \gcd(r_i, h_j) - 1$, $q_{ij} = \operatorname{lcm}(r_i, h_j)$.

Proof. Since m and n are relatively prime we have that :

$$\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n.$$

(for example see [1].) Therefore, each element x of $\mathbb{Z}_{mn}$ can be viewed as an ordered pair, an image of x in the isomorphism

$$x \to (x \bmod m,\ x \bmod n).$$

Moreover, since $\gcd(n, m) = 1$, $\mathcal{I}(mn) \cong \mathcal{I}(m) \times \mathcal{I}(n)$, and $g \in \mathcal{I}(mn)$ can be viewed as an ordered pair $(a, b) \in \mathcal{I}(m) \times \mathcal{I}(n)$. We prove that all elements of type w_{ijs} for different i, j, s, defined as in the statement of the theorem belong to different orbits. In the terms of the ordered pairs, it means that $(a_i a^s, b_j)$ for different i, j, s belong to different orbits. It is clear that the ordered pair $(a_{i_1} a^{s_1}, b_{j_1})$ can not be in the same orbit as $(a_{i_2} a^{s_2}, b_{j_2})$ if $i_1 \neq i_2$ or $j_1 \neq j_2$. Thus, the only remaining case is when two pairs are of the form $(a_i a^{s_1}, b_j)$ and $(a_i a^{s_2}, b_j)$ and $s_1 \neq s_2$. Suppose that $(a_i a^{s_1}, b_j)$ and $(a_i a^{s_2}, b_j)$ belongs to the same orbit. Here, we have $0 \leq s_1, s_2 < \gcd(r_i, h_j)$. Suppose that $x > 0$ and $s_1 > s_2$. Since

$$a_i a^{s_1 - s_2 + x} = a_i \pmod{m}, \quad b_j b^x = b_j \pmod{n}$$

then it follows that $s_1 - s_2 + x = r_i t_1$ and $x = h_j t_2$. From here, we have $s_1 - s_2 = r_i t_1 - h_j t_2$. However $r_i t_1 - h_j t_2 = \gcd(r_i, h_j)z$ and then $s_1 - s_2 = \gcd(r_i, h_j)z$ what is not possible.

It is clear that in the orbit $(a_i a^{s_2}, b_j)$ must be exactly $\operatorname{lcm}(r_i, h_j)$ elements. At the end, note that

$$|\operatorname{osig}(g)| = \sum_{i,j} \gcd(r_i, h_j) \operatorname{lcm}(r_i, h_j) = \sum_{i,j} r_i h_j = mn$$

and therefore the collection of orbits and their representatives is complete. □

The previous theorem apparently constitutes an algorithm for constructing the orbit signature of an element $g \in Z_{nm}$, given the orbit signatures of the constituents $a \in \mathbb{Z}_n$ and $b \in \mathbb{Z}_m$, $\gcd(m, n) = 1$, where

$$g \equiv a \pmod{m}, \quad g \equiv b \pmod{n}.$$

Corollary 3.1. *Considering all conditions and the notation from Theorem 3.1, the number of orbits of the group $\langle g \rangle$ acting on the set of elements of $\mathbb{Z}_{mn}$ is*

$$\sum_{i=1}^{l} \sum_{j=1}^{t} \gcd(r_i, h_j).$$

Proof. By Theorem 3.1, element g has the orbit signature

$$\operatorname{osig}(g) = \prod_{i=1}^{l} \prod_{j=1}^{t} \prod_{s=0}^{u(i,j)} [w_{ijs}, q_{ij}]$$

where $u_{ij} = \gcd(r_i, h_j) - 1$. Clearly, the number of orbits is

$$\sum_{i=1}^{l} \sum_{j=1}^{t} \gcd(r_i, h_j).$$

□

We say that that a $k-$complete set is *normalized* if it contains 0. Let $\mathcal{C}_m$ be the set of all $m-$complete, sets in the $\mathbb{Z}_{mn}$. Recall, a $m-$complete set $A = \{a_1, a_2, \ldots, a_m\}$, $a_i \in \mathbb{Z}_{mn}$ is a set such that $a_i \not\equiv a_j \pmod{m}$, for $i \neq j$.

For an $m-$complete set $A = \{a_1, a_2, \ldots, a_m\}$ and $g \in \mathcal{I}(mn)$, we consider a group action

$$(g, A) \to gA$$

In order to confirm that $gA \in \mathcal{C}_m$, for any $A \in \mathcal{C}_m$ and $g \in \mathcal{I}(mn)$, we need the following simple lemma.

Lemma 3.1. *Let $A = \{a_1, a_2, \ldots, a_m\}$ be an $m-$complete set and let k be a natural number such that $\gcd(k, m) = 1$. Then $kA = \{ka_1, ka_2, \ldots, ka_m\}$ is also an $m-$complete set.*

Proof. Since k has a multiplicative inverse, $ka_i - ka_j \equiv 0 \pmod{m}$ implies $a_i - a_j \equiv 0 \pmod{m}$. However, this is possible only if $i = j$. More generally, if $gcd(k, m) = 1$, then

$$\{ka_r + l \mid 1 \leq r \leq m\}$$

is a $m-$complete set for any $l \in \mathbb{Z}$. □

Note that the previous lemma holds also when instead of $m-$complete, we put a normalized $m-$complete set.

Our goal is to determine the number of orbits of the previous action. For that

purpose, the Cauchy-Frobenius theorem will be used. We need to find $|\operatorname{Fix}(g)|$ for each $g \in \mathcal{I}(mn)$, where

$$\operatorname{Fix}(g) = \{A \mid gA = A,\ A \in \mathcal{C}_m\}.$$

We begin by introducing the *orbit similarity*, a new notion that we will need later.

Definition 3.3. *Let G and H be groups acting on the sets Ω_1 and Ω_2 respectively. Let $\phi : \Omega_1 \to \Omega_2$ be a mapping. We say that an orbit $O_2 \subset \Omega_2$ is ϕ-similar to an orbit $O_1 \subset \Omega_1$ if it holds that*

$$|O_1| = |O_2| \text{ and } \phi(O_1) = O_2.$$

Lemma 3.2. *Let m and n be relatively prime natural numbers. Let $g \in \mathcal{I}(mn)$, $a \in \mathcal{I}(m)$, $b \in \mathcal{I}(n)$ so it holds that*

$$g \equiv a \pmod{m}, \quad g \equiv b \pmod{n},$$

and

$$\operatorname{osig}(a) = \prod_{i=1}^{l} [a_i, r_i], \quad \operatorname{osig}(b) = \prod_{j=1}^{t} [b_j, h_j].$$

Let $\phi(x) = x \bmod m$ be the mapping from $\mathbb{Z}_{mn}$ to $\mathbb{Z}_m$. Let $[a_f, r_f]$ be an arbitrary orbit of the group $H = \langle a \rangle$ in its permutation representation on m points. Then, the number of orbits of the group $G = \langle g \rangle$ acting on $\mathbb{Z}_{mn}$ that are ϕ-similar to $[a_f, r_f]$ is

$$\sum_{h_j | r_f} h_j \quad (1 \le j \le t).$$

Proof. By Theorem 3.1 we know that

$$\operatorname{osig}(g) = \prod_{i=1}^{l} \prod_{j=1}^{t} \prod_{s=0}^{u(i,j)} [w_{ijs}, q_{ij}]$$

where w_{ij} is an element of $\mathbb{Z}_{mn}$ such that

$$w_{ijs} \equiv a_i a^s \pmod{m}$$

$$w_{ijs} \equiv b_j \pmod{n}.$$

We show that $[w_{ijs}, q_{ij}]$ is ϕ-similar to $[a_f, r_f]$ if and only if $i = f$ and $q_{ij} = r_f$. Suppose that $[w_{ijs}, q_{ij}]$ is ϕ-similar to $[a_f, r_f]$. Since $\phi(w_{ijs}) = a_i a^s$, than it must be that $i = f$. The condition $q_{ij} = r_f$ follows directly from the definition of ϕ-similarity. Suppose that $i = f$ and $q_{ij} = r_f$. Considering that $a_f a^{r_f} = a_f a$, we have

$$\{a_f, a_f a, \ldots, a_f a^{r_f - 1}\} = \{a_f a^s, \ldots, a_f a^{r_f + s - 1}\}.$$

From here, we conclude that the orbit $[w_{fjs}, q_{fj}]$ is ϕ-similar to $[a_f, r_f]$ for each j such that $q_{fj} = r_f$. Now, it is easy to count the number of similar orbits to the $[a_f, r_f]$. It is apparent that $q_{fj} = \gcd(r_f, h_j) = r_f$ if and only if $h_j \mid r_f$. Therefore, for each j such that $h_j \mid r_f$, orbit $[w_{fjs}, q_{fj}]$ is ϕ-similar to $[a_f, r_f]$ for each s. Since $0 \leq s \leq h_j - 1$, there is exactly h_j such orbits. Hence, the claim has been proven. □

Considering the mapping ϕ defined as in Lemma 3.2, it is clear that ϕ-similar orbits $[w_{fjs}, q_{fj}]$ and $[a_f, r_f]$ contain the same residue classes modulo m. Therefore, $[w_{fjs}, q_{fj}]$ is a subset of an m-complete set in $\mathbb{Z}_{mn}$. From this simple observation, we have the following lemma.

Lemma 3.3. *Let m and n be relatively prime natural numbers. Let $g \in \mathcal{I}(mn)$,*

$a \in \mathcal{I}(m)$, $b \in \mathcal{I}(n)$ such that

$$g \equiv a \pmod{m} \quad g \equiv b \pmod{n}$$

and

$$\mathrm{osig}(a) = \prod_{i=1}^{l} [a_i, r_i], \quad \mathrm{osig}(b) = \prod_{j=1}^{t} [b_j, h_j].$$

Then, the number of m-complete sets in $\mathbb{Z}_{mn}$, fixed by the element g is

$$|\operatorname{Fix}(g)| = \prod_{i=1}^{l} \sum_{h_j | r_i} h_j \quad (1 \leq j \leq t).$$

Proof. Let $A \subset \mathbb{Z}_{mn}$ be an m-complete set, fixed by an element g. Then, $A\langle g \rangle = A$. Therefore, A must be the union of some orbits of g. In other words, A must be the union of some cycles of g in its permutation representation. However, we should consider just those orbits that are ϕ-similar orbits of a since just those orbits are blocks of an m-complete set. Here, we naturally assume that $\phi(x) = x \bmod m$. As we concluded in Lemma 3.2, the number of orbits of g similar to the particular orbit $[a_i, r_i]$ is

$$\sum_{h_j | r_i} h_j.$$

Therefore, the number of m-complete sets, fixed by an element g is simply the product of those numbers where $1 \leq i \leq l$. This concludes the proof. □

Example 3.2. *Let us consider the number of 5-complete sets, fixed by $3 \in \mathcal{I}(40)$. Considering that $\mathbb{Z}_{40} \cong \mathbb{Z}_5 \times \mathbb{Z}_8$, we have*

$$a \equiv (1,\ 3,\ 4,\ 2)(0), \quad b \equiv (1,\ 3)(2,\ 6)(5,\ 7)(4)(0)$$

and then

$$\operatorname{osig}(a) = [1,4][0,1], \quad \operatorname{osig}(b) = [1,2][2,2][5,2][4,1][0,1].$$

Following the notation of the previous lemma, we see that $r_1 = 4,\ r_2 = 1,\ h_1 = h_2 = h_3 = 2,\ h_4 = h_5 = 1$. *Using the given formula, we get*

$$\operatorname{Fix}(3) = (h_1 + h_2 + h_3 + h_4 + h_5)(h_4 + h_5) = (2+2+2+1+1)(1+1) = 16.$$

Thus, there should be sixteen 5*-complete sets in* $\mathbb{Z}_{40}$ *fixed by element* $3 \in \mathcal{I}_{40}$. *Indeed, by direct computation, we obtain all of them*

$$\{0,1,3,9,27\},\ \{0,2,6,14,18\},\ \{0,11,17,19,33\},\ \{0,8,16,24,32\},$$

$$\{0,7,21,23,29\},\ \{0,22,26,34,38\},\ \{0,13,31,37,39\},\ \{0,4,12,28,36\}$$

$$\{1,3,9,20,27\},\ \{2,6,14,18,20\},\ \{11,17,19,20,33\},\ \{8,16,20,24,32\}$$

$$\{7,20,21,23,29\},\ \{20,22,26,34,38\},\ \{13,20,31,37,39\},\ \{4,12,20,28,36\}.$$

Lemma 3.4. *Consider all conditions and notation from Lemma 3.3. The number of normalized* m*-complete sets fixed by an element* g *is equal to*

$$|\operatorname{Fix}(g)| = \prod_{i=1}^{l-1} \sum_{h_j | r_i} h_j \quad (1 \leq j \leq t).$$

Proof. Recall that $[a_l, r_l] = [0,1]$. Since we consider that a normalized m-complete set always contains zero, then we see that in this case $\alpha_l = 1$. Therefore, the number of normalized m-complete sets fixed by an element g is equal to the product given in the statement of the lemma. □

Example 3.3. *According to Example 3.2, we see that number of normalized* 5*-complete subsets of* $\mathbb{Z}_{40}$ *fixed by* $3 \in \mathcal{I}(40)$ *is* 8*,*

$$\{0,1,3,9,27\},\ \{0,2,6,14,18\},\ \{0,11,17,19,33\},\ \{0,8,16,24,32\},$$

$$\{0,7,21,23,29\},\ \{0,22,26,34,38\},\ \{0,13,31,37,39\},\ \{0,4,12,28,36\}$$

that corresponds to the result

$$h_1 + h_2 + h_3 + h_4 + h_5 = 8,$$

obtained by the formula in the previous lemma.

By applying Theorem 2.4 (Cauchy-Frobenius) we calculate the number of orbits of (normalized) m-complete sets. The number of orbits is

$$s = \frac{1}{\phi(mn)} \sum_{g \in \mathcal{I}(mn)} |\operatorname{Fix}(g)|$$

where $\operatorname{Fix}(g)$ are calculated as in Lemma 3.3 and Lemma 3.4 respectively.

Example 3.4. *Let us calculate the number of orbits of* 5*-complete sets in* $\mathbb{Z}_{40}$*. The number of* 5*-complete sets fixed by particular elements is given in the following sequence.* $|\operatorname{Fix}(1)| = 32768,\ |\operatorname{Fix}(3)| = 16,\ |\operatorname{Fix}(7)| = 16,\ |\operatorname{Fix}(9)| = 512,\ |\operatorname{Fix}(11)| = 32,\ |\operatorname{Fix}(13)| = 32,\ |\operatorname{Fix}(17)| = 64,\ |\operatorname{Fix}(19)| = 128,\ |\operatorname{Fix}(21)| = 1024,\ |\operatorname{Fix}(23)| = 16,\ |\operatorname{Fix}(27)| = 16,\ |\operatorname{Fix}(29)| = 256,\ |\operatorname{Fix}(31)| = 32,\ |\operatorname{Fix}(33)| = 64,\ |\operatorname{Fix}(37)| = 32,\ |\operatorname{Fix}(39)| = 128.$

Therefore, by the Cauchy-Frobenius formula, we have 2196 *orbits of* 5*-complete sets in* $\mathbb{Z}_{40}$*.*

Chapter 4

Group Factorizations

The main topic of this chapter is *group factorizations*. As it has been noted in the introduction, the main goal is to give a theoretical background and develop some tools for factorizations of non-abelian groups. In this context, we generalize a number of known results from the abelian case to the general case. We introduce the concept of *free mappings*, by which it is possible to construct nontrivial factorizations of a wide class of groups. Particularly, we show how free mappings can be applied in the factorization of $\mathbb{Z}_p \times \mathbb{Z}_p$ and $\mathbb{Z}_p \times \mathbb{Z}_q$, where p and q are different primes. At the end of this chapter, we give a connection between group factorizations of $\mathbb{Z}_{mn}$ and the group action of $\mathcal{I}(mn)$ on m and n-complete subsets of $\mathbb{Z}_{mn}$, if m and n are relatively prime numbers.

4.1 Preliminary results

Definition 4.1. *We say that a list of $k \geq 2$ subsets $\alpha = [B_1, B_2, \ldots, B_k]$ of a group G is a factorization of $C \subseteq G$ if $C = B_1 B_2 \ldots B_k$ and every $c \in C$ has a unique representation as a product $c = b_1 b_2 \ldots b_k$, $b_i \in B_i$, $1 \leq i \leq k$. 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 $(r_1, r_2, \ldots, r_k)$, 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, $1 \leq i \leq k$. The following theorem, although elementary in its nature turns out to be very useful for analyzing group factorizations.

Theorem 4.1. *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 $a_1 b_1 = a_2 b_2$ exactly if $a_2^{-1} a_1 = b_2 b_1^{-1}$. □

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

Lemma 4.1. *Let $\{e\} = G_0 \leq G_1 \leq \ldots \leq G_k = G$ be a chain of subgroups and let B_i be a complete set of right representatives of G_{i-1} in G_i, for $1 \leq i \leq k$. Then, $\alpha = [B_1, \ldots, B_k]$ is a factorization of G.*

Proof. Let $g \in G$ be an arbitrary element. There exists a unique $b_{k-1} \in B_{k-1}$ such that $g \in G_{k-1}b_{k-1}$. Then $gb_{k-1}^{-1} \in G_{k-1}$. Similarly, there exists a unique $b_{k-2} \in B_{k-2}$ such that $gb_{k-1}^{-1} \in G_{k-2}b_{k-2}$ and consequently $gb_{k-1}^{-1}b_{k-2}^{-1} \in G_{k-2}$. Continuing this process, we have the sequence $b_1, b_2, \ldots, b_s$, unique to chosen $g \in G$ such that $gb_{k-1}^{-1}b_{k-2}^{-1}\ldots b_1^{-1} \in G_0$. Therefore, $g = b_1 \ldots b_k$ and $b_i \in B_i$ for $1 \leq i \leq k$. Thus, α is a factorization of G. □

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

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

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 4.1. *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*

$$G \geq G_1 \geq G_2 \geq \ldots \geq G_n \geq \{e\}$$

Therefore, it is very easy to find a chain of subgroups and consequently a factorization, when G is a permutation group.

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 $\mathcal{R}(G)$. The solutions to this type of problems are in general more developed in the case when G is abelian.

4.1.1 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 $g = s_1 s_2 \ldots s_i s_{i+1} \ldots s_k$ is the factorization of g with respect to α, then the factorization of g with respect to β will be $g = s_1 s_2 \ldots s_{i-1} t s_{i+2} \ldots s_k$, where $t = s_i s_{i+1}$. 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 $C_i = g_i^{-1} B_i g_{i+1}$ for $1 \leq i \leq k$. 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 $g^{-1} = s_1 s_2 \ldots s_k$ be the factorization of g^{-1} with respect to α. Thus, $g = s_k^{-1} s_{k-1}^{-1} \ldots s_1^{-1}$ is the factorization of g with respect to β. As it has been shown in [19], 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 integers 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 $\phi^{-1}(g) = b_1 b_2 \ldots b_k$ be the unique factorization of $\phi^{-1}(g)$ with respect to α. By applying the automorphism ϕ to the both sides we have that $g = \phi(b_1)\phi(b_2)\ldots\phi(b_k)$. Suppose that $g = \phi(b'_1)\phi(b'_2)\ldots\phi(b'_k)$, where $b'_i \in B_i, \quad 1 \leq i \leq k$. 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 $b_i = b'_i, \quad 1 \leq i \leq k$ and accordingly $\phi(b_i) = \phi(b'_i), \quad 1 \leq i \leq k$.

4.2 Replacement of factors

Here we present some important results in the theory of group factorizations. Some of the proofs are omitted due to their complexity, so we refer the reader to references [19] and [6] for further reading. Also, a number of theorems are generalized from the abelian case to the general case.

If A and A' are subsets of the finite group G such that, for every subset B of G, if $\alpha = [A, B]$ is a factorization of G, then $\beta = [A', B]$ is also factorization of G, then we say that A is *replaceable* by A'.

The subset A of the finite group G is said to be *simulated* if there is a subgroup H of G such that $|A| = |H| \geq 3$ and $|A \cap H| + 1 \geq |A|$. Basically, a simulated subset is either a subgroup of more than two elements or differs from such a subgroup by one element. In this case, the group H is said to be the *corresponding* subgroup of the set A. It can be seen that $|A| \geq 3$ implies that there is a unique subgroup that can differ by one element from A.

A subset A is defined *left periodic* if there exits and element g of $G \setminus \{e\}$ with $gA = A$. We refer to such elements g as left periods of A. Similarly, we define *right periodic* subsets and right periods. If $g \in G$ is both a left and right period of a subset A, then we say that A is periodic and g is a period of A. The empty set and the identity element e are not considered to be periodic. To a nonempty subset A of a finite group G we assign the subset L such that

$$L = \bigcap_{a \in A} Aa^{-1}.$$

Lemma 4.2. *Let A be a nonempty subset of a finite group G. If for the subset L assigned to A it holds that $L \neq \{e\}$, then A is left periodic.*

Proof. Let $A = \{a_1, \ldots, a_n\}$. Since A is not empty, $e \in L$. Suppose that $g \in L \setminus \{e\}$. Such g does exist since L is larger than $\{e\}$. As A is not empty, there are elements $b_1, \ldots, b_n \in A$ such that

$$g = b_1 a_1^{-1} = \cdots = b_n a_n^{-1}.$$

Note that $b_1, \ldots, b_n$ are pairwise distinct elements of A. Since $b_1, \ldots, b_n$ are different elements they are all the elements of A. Consequently,

$$gA = \{ga_1, \ldots, ga_n\} = \{b_1 a_1^{-1} a_1, \ldots, b_n a_n^{-1} a_n\} = \{b_1, \ldots, b_n\} = A.$$

□

Note that the set of left periods of A is a subgroup of finite group G. Let K be a group of left periods of set A. Then, $Ka \subset A$ for every $a \in A$. Therefore,

$$A = \bigcup_{a \in A} Ka.$$

Lemma 4.3. *Let A be a simulated subset of finite group G and let H be the corresponding subgroup of A. If A is left periodic, then $A = H$.*

Proof. Suppose $A = (H \setminus \{h\}) \cup \{hd\}$, where $h \in H, d \in G$. Let g be a left period of A and suppose $\text{ord}(g) = r$. We may assume that r is prime since if g is a left period than any power of is again left period. The permutation defined by:

$$a \rightarrow ga,\ a \in A$$

consists of cycles of length r. No fixed points can exist because $ga = a$ would imply that $g = 1$.

Consider the cycle of g which contains hd. If $r \geq 3$, then there must be at least two further elements a and b in this cycle contained in H. So $g^t a = b$ for some $t,\ 0 \leq t \leq r-1$. Therefore $g \in H$. Similarly, $g^s a = hd$ for some $s,\ 0 \leq s \leq r-1$ and so $d \in H$. If $r = 2$, then since $|A| \geq 3$ the permutation must contain at least one additional cycle. As before, using the second cycle we can see that $g \in H$ and using the first cycle we have that $d \in H$. □

The following theorem is an important step for proving Hajós's Theorem that will be stated later.

Theorem 4.2. *If $\alpha = [A_1, \ldots, A_n]$ is a factorization of the finite abelian group G where the factors are simulated subsets of G, then at least one of the blocks A_i for $1 \leq i \leq n$ must be a subgroup of G.*

Lemma 4.4. *Let $\alpha = [A, B]$ be a factorization of a finite abelian group G. Suppose that $A = \{h_1, \ldots, h_{s-1}, h_s d\}$ is a simulated subset and $H = \{h_1, \ldots, h_{s-1}, h_s\}$ is the corresponding subgroup of G. Then $dB = B$ and*

$$G = \{h_1, \ldots, h_{i-1}, h_i d^j, h_{i+1}, \ldots, h_s\}B$$

is also a factorization of G. In particular A is replaceable by H and if $d \neq e$, then B is left periodic with left period d.

Proof. Suppose that $h_1 = e$. The fact that $G = AB$ is a factorization of G is equivalent to the condition that the subsets:

$$h_1B, \ldots, h_{s-1}B, h_sdB$$

form a partition of G. We claim that $G = HB$ is a factorization of G, that is, the subsets:

$$h_1B, \ldots, h_{s-1}B, h_sB$$

form a partition of G. To prove the claim, assume the contrary, namely that those sets do not form a partition of G, say

$$h_iB \cap h_sB \neq \emptyset$$

for some i, $1 \leq i \leq s-1$. If $i \neq 1$, then we have the contradiction

$$h_i^{-1}h_i \cap h_i^{-1}h_sB = h_1B \cap h_jB \neq \emptyset$$

where $2 \leq j \leq s-1$. If $i = 1$, then since $|H| = s \geq 3$ there is an $h_k \in H$ with $2 \leq k \leq s-1$. Now, we have the contradiction that

$$h_kh_1B \cap h_kh_sB = h_kB \cap h_jB \neq \emptyset$$

where $1 \leq j, k \leq s-1$, $j \neq k$.

Comparing the two partitions of G we get that $h_sdB = h_sB$ and so $dB = B$. It

follows that $d^jB = B$ for each integer j. This gives that the sets

$$h_1B, \ldots, h_{i-1}B, h_id^jB, h_{i+1}B, \ldots, h_sB$$

form a partition of G. □

Definition 4.2. *A subset B of the group G is called abelian if $b_1b_2 = b_2b_1$ for any $b_1, b_2 \in B$.*

Example 4.2. *Let $G = \langle g, h\rangle$ be the dihedral group D_{12}, where $\mathrm{ord}(g) = 12$, $\mathrm{ord}(h) = 2$. Let $V = \{e, g^5, g^6, g^{11}\}$ and $S = \{e, g^2, g^4, h, hg^2, hg^4\}$. By direct computation, we see that $[V, S]$ is a normalized factorization of D_{12}.*

As an illustration of the factorization where we have an abelian set, look at the set V in the previous Example 4.2. Moreover, notice that

$$[S, V],\ [V, S],\ [S^{-1}, V],\ [S, V^{-1}]$$

are factorizations of G as well.

Lemma 4.5. *Let $[A, B]$ be a factorization of the finite group G where A is an abelian subset of G. Then*

$$[A^{-1}, B],\ \ [B^{-1}, A]$$

are factorizations of the group G. Similarly, if B is an abelian subset of G, then

$$[A, B^{-1}],\ \ [B, A^{-1}]$$

are factorizations of the group G.

Proof. From the fact that $[A, B]$ is a factorization of G, by Theorem 4.1 it follows $A^{-1}A \cap BB^{-1} = \{e\}$. Since A is an abelian set then it holds $A^{-1}A = AA^{-1}$ and

then $AA^{-1} \cap BB^{-1} = \{e\}$. According to Theorem 4.1, we have that $[A^{-1}, B]$ is a factorization of G. Now, by taking inverse of $[A^{-1}, B]$ we have that $[B^{-1}, A]$ is a factorization of G. □

Example 4.3. *Let us consider non-transversal factorizations of the dihedral group* $D_6 = \langle g, h \rangle$, $\text{ord}(g) = 6, \text{ord}(h) = 2$, *of type* $[3, 4]$. *There are* 12 *of them.*

1. $A = \{e, hg^4, hg^2\}$, $B = \{e, h, hg^5, g^5\}$.
2. $A = \{e, hg^4, hg^2\}$, $B = \{e, h, hg^1, g^1\}$.
3. $A = \{e, h, hg^4\}$, $B = \{e, hg^3, g^1, hg^2\}$.
4. $A = \{e, h, hg^4\}$, $B = \{e, hg^1, hg^2, g^5\}$.
5. $A = \{e, hg^3, hg^1\}$, $B = \{e, h, hg^5, g^1\}$.
6. $A = \{e, hg^3, hg^1\}$, $B = \{e, hg^5, hg^4, g^5\}$.
7. $A = \{e, hg^1, hg^5\}$, $B = \{e, hg^3, hg^2, g^5\}$.
8. $A = \{e, hg^1, hg^5\}$, $B = \{e, hg^3, hg^4, g^1\}$.
9. $A = \{e, h, hg^2\}$, $B = \{e, hg^5, hg^4, g^1\}$.
10. $A = \{e, h, hg^2\}$, $B = \{e, hg^3, hg^4, g^5\}$.
11. $A = \{e, hg^3, hg^5\}$, $B = \{e, h, hg^1, g^5\}$.
12. $A = \{e, hg^3, hg^5\}$, $B = \{e, hg^1, g^1, hg^2\}$.

As one can see, none of the $A's$ *is an abelian set. However for each of these factorizations* $[A, B]$ *it holds that* $[A^{-1}, B]$ *is also a factorization. On the other hand, none of there has* $[A, B^{-1}]$ *as a factorization.*

In the case of an abelian group G, clearly every subset is abelian and therefore the following lemma is an easy consequence of the previous one.

Corollary 4.1. *Let $[A, B]$ be a factorization of a finite abelian group G. Then*

$$[A^{-1}, B], \ \ [B^{-1}, A], \ \ [A, B^{-1}], \ \ [B, A^{-1}]$$

are factorizations of the group G.

Definition 4.3. *Let $\alpha = [A_1, A_2, \ldots, A_k]$ be a factorization of a group G. Then, for every $g \in G$ we have a unique factorization $g = g_1 g_2 \cdots g_k$ where $g_i \in A_i$. For a fixed $i \in \{1, 2, \ldots, k\}$, the mapping*

$$g \to g_i, \ \ g \in G$$

we call the projection mapping onto block A_i and g_i is denoted by g_{A_i}.

Lemma 4.6. *Suppose that $\alpha = [A, B]$ and $\beta = [A, B^{-1}]$ are factorizations of a group G. Let $f_g : A \to A$, $h_t : A \to A$ be functions defined as*

$$f_g(a) = (ga)_A,$$

$$h_t(a) = (at)_A,$$

where g, t is an arbitrary element of the group G and $(ga)_A$, $(at)_A$ come from the factorization α, β respectively. Then f_g and h_t are one to one.

Proof. Suppose that $f_g(a_1) = f_g(a_2)$. We have

$$ga_1 = (ga_1)_A (ga_1)_B,$$

$$ga_2 = (ga_2)_A (ga_2)_B.$$

From $(ga_1)_A = (ga_2)_A$ it follows

$$ga_1(ga_1)_B^{-1} = (ga_1)_A = (ga_2)_A = ga_2(ga_2)_B^{-1},$$

from which follows that

$$a_1(ga_1)_B^{-1} = a_2(ga_2)_B^{-1}.$$

Since $[A, B^{-1}]$ is a factorization then it follows $a_1 = a_2$. The proof is similar for h_t. □

Lemma 4.7. *If $[A, B]$, $[A, B^{-1}]$ are factorizations of a finite group G, where A is an abelian set, and k is an integer relatively prime to $|A|$, then $[A^k, B]$ is a factorization of the group G.*

Proof. Let p be a prime which does not divide $n = |A|$. We claim that for each $g \in G$, the subset $\{(ga^p)_A \mid a \in A\}$ is equal to A, with respect to $[A, B]$ and $[A, B^{-1}]$. Let $a \in A$, and consider the number of solutions of the equation $(gx_1 \cdots x_p)_A = a$ with all $x_i \in A$. By Lemma 4.6 we may choose $x_1, \ldots, x_{p-1}$ arbitrarily, and solve for x_p uniquely. Thus, there are n^{p-1} solutions. If $x_1 = a_1, \ldots, x_p = a_p$ is a solution in which not all x_i are equal, then we obtain p distinct solutions from this one by cyclic permutation. This is possible to do since A is an abelian set. So the number of such solutions is a multiple of p. Since p does not divide n^{p-1}, there must be at least one solution with $x_i = a_1$, for $1 \leq i \leq p$. This gives that $(ga_1^p)_A = a$. Since A is finite, the claimed result follows, and a_1 is uniquely determined by g and a.

If $a_1^p = a_2^p$, then $(ga_1^p)_A = (ga_2^p)_A$, so we have that $a_1 = a_2$. Hence, $|A^p| = |A|$. Suppose that $a_1^p b_1 = a_2^p b_2$ where $a_i \in A$ and $b_i \in B$. Since A is an abelian set, then

by Lemma 4.5, $[B^{-1}, A]$ is a factorization of G. Therefore, we have that

$$a_1^p b_1 = a_2^p b_2 = b_0^{-1} a_0,$$

where $a_0 \in A$ and $b_0 \in B$. From here, it follows that

$$b_0 a_1^p = a_0 b_1^{-1} \text{ and } b_0 a_2^p = a_0 b_2^{-1}.$$

Hence, $(b_0 a_1^p)_A = (b_0 a_2^p)_A$ with the respect to $[A, B^{-1}]$ factorization, so that $a_1 = a_2$. Thus, $b_1 = b_2$. Therefore, $[A^p, B]$ is a factorization.

Now for any positive integer k relatively prime to $|A|$, we may apply this result successively to obtain $|A^k| = |A|$ and $[A^k, B]$ as a factorization. If k is a negative integer relatively prime to $|A|$, then we obtain the desired result by using the above result for $-k$ and starting with the factorization $[A^{-1}, B]$. □

Example 4.4. *Let us give an illustration of the previous lemma through a factorization of the dihedral group* $D_8 = \langle g, h \rangle$, *where* $\text{ord}(g) = 8$ *and* $\text{ord}(h) = 2$. *Consider the following factorization*

$$A = \{e, g^7, g^3, g^4\}, \quad B = \{e, hg^1, g^2, hg^3\}.$$

Clearly, A is an abelian set and it is easy to see that $[A, B^{-1}]$ *is also a factorization of* D_8. *By fixing k, say* $k = 3$, *according to the previous lemma,* $[A^k, B]$ *is also a factorization of* D_8. *Indeed,* $[A^3, B]$ *where* $A^3 = \{e, g^5, g, g^4\}$ *and* $B = \{e, hg^1, g^2, hg^3\}$ *is a factorization of* D_8.

As the direct consequence of the previous lemma, we have an interesting result in the abelian case.

Corollary 4.2. *Let $\alpha = [B_1, B_2]$ be a factorization of finite abelian group G and let t, q be integers such that $\gcd(t, |B_1|) = 1$ and $\gcd(q, |B_2|) = 1$. Then $\beta = [B_1^t, B_2^q]$ is also a factorization of G.*

Corollary 4.3. *If $[A, B]$, $[A, B^{-1}]$ are factorizations of the finite group G, and A is an abelian set, then the order of any nonidentity element from AA^{-1} and $A^{-1}A$ is not relatively prime to $|A|$.*

Proof. Suppose that $(a_1 a_2^{-1})^k = e$ for $a_1, a_2 \in A$ and k is relatively prime to $|A|$. Since A is an abelian subset, then $a_1^k = a_2^k$. Since $|A^k| = |A|$, then it must be $a_1 = a_2$. □

Let G be a group with the property that there exists a positive integer n such that, for every $g \in G$, $g^n = e$. The exponent of G, denoted $\exp(G)$, is the smallest positive integer m such that, for every $g \in G$, $g^m = e$. Thus, for every finite group G, $\exp(G)$ divides $|G|$.

Theorem 4.3. *Let a group G be the direct product of a subgroup H of order n and a subgroup K of exponent m, where n and m are relatively prime. If $[A, B]$, $[A, B^{-1}]$ are factorizations of G in which A is an abelian subset, $|A| = n$, then A may be replaced by the subgroup H to give a factorization $[H, B]$.*

Proof. By Lemma 4.7 we know that $[A^m, B]$ is a factorization. Since K has exponent m, we have that $K^m = \{e\}$, so $A^m \subseteq H$. Since $|H| = |A^m|$ it follows that $A^m = H$, so $[H, B]$ is a factorization. □

Theorem 4.4. *Let G be an abelian group of order nm, where n and m are relatively prime. If $[A, B]$ is a factorization of G with $|A| = n$ and $|B| = m$, then there exist subgroups H, K of G such that $[H, B]$ and $[A, K]$ are factorizations of G.*

Proof. Since n, m are relatively prime, G is the direct product of unique subgroups H, K of order n, m respectively. Since A, B are abelian sets, we may apply Theorem 4.3 in two ways to obtain the required factorizations $[H, B]$ and $[A, K]$. □

A subset A of a finite abelian group G is defined to be *cyclic* if there is an element a of G and an integer r such that the elements $e, a, a^2, \ldots, a^{r-1}$ are distinct and give all the elements of A. In order to avoid trivial cases we will assume that $a \neq e$ and $r \geq 2$.

The following lemma shows that under certain conditions, a block of a factorization could be replaced by the corresponding cyclic subset.

Lemma 4.8. *If $[A, B]$, $[A, B^{-1}]$ are factorizations of finite group G, A is an abelian set, $|A| = p$ a prime, then $[A', B]$ is a factorization of G, where $A' = \{e, a, a^2, \ldots, a^{p-1}\}$, $a \in A \setminus \{e\}$.*

Proof. By Lemma 4.7, $[A^t, B]$ is a factorization of G whenever $\gcd(p, t) = 1$. Let $A = \{e, a_1, a_2, \ldots, a_{p-1}\}$. It follows that the sets

$$eB,\ a_1^t B,\ a_2^t B, \ldots,\ a_{p-1}^t B$$

form a partition of G. Similarly, the fact that $[A', B]$ is a factorization is equivalent to the sets

$$eB,\ a_k^t B,\ a_k^2 B, \ldots,\ a_k^{p-1} B$$

forming a partition of G. Here $A' = \{e, a_k, a_k^2, \ldots, a_k^{p-1}\}$. Since G is finite it is enough to show that $a_k^i B \cap a_k^j B = \emptyset$ for each $i, j,\ 0 \leq i < j \leq p-1$. Suppose that $a_k^i B \cap a_k^j B \neq \emptyset$. Set $t = j - i$. Clearly, $1 \leq t \leq p-1$ and so t is prime to p. Now $eB \cap a_k^t B \neq \emptyset$ contradicts the fact that $[A^t, B]$ is a factorization of G. □

Example 4.5. *Consider the following illustration of the previous lemma. Let* $G = D_{12} = \langle g, h \rangle$, $\mathrm{ord}(g) = 12, \mathrm{ord}(h) = 2$ *be a dihedral group of order* 24. *It is easy to confirm that*

$$A = \{e, g^2, g^4\} \quad B = \{e, g, g^7, hg^1, hg^7, h, g^6, hg^6\}$$

is a factorization of the group G. *Clearly,* A *is an abelian set and one can show that* $[A, B^{-1}]$ *is also a factorization. According to the previous lemma, we have that* $[A', B]$ *is a factorization, where* $A' = \{e, g^4, g^8\}$. *This can be confirmed by direct computation.*

The next lemma proves Hajós theorem for abelian p-groups.

Lemma 4.9. *Let* G *be a finite abelian* p*-group and let* $\alpha = [A_1, \ldots, A_n]$ *be a factorization of* G, *where the* A_i *are cyclic subsets and* $|A_i| = p$ *for* $1 \leq i \leq n$. *Then at least one of the factors* A_i *is a subgroup of* G.

The following lemma is a good example of a block transformation using exponentiation. A block on which the transformation is applied must be a cyclic subset. Later, a more general result will be proven without this particular restriction.

Lemma 4.10. *Let* $[A, B]$ *be a normalized factorization of finite group* G, *let* p *be a prime and* t *an integer. If* A *is a cyclic subset*

$$A = \{e, a, a^2, \ldots, a^{p-1}\},$$

then $[A', B]$ *is a factorization of* G *where*

$$A' = \{e, a^t, a^{2t}, \ldots, a^{(p-1)t}\},$$

whenever t *is relatively prime to* p.

Proof. By the partition reformulation of the factorization, the sets

$$a^0B, a^1B, a^2B, \ldots, a^{p-1}B \tag{4.2.1}$$

form a partition of G. We want to prove that the sets

$$a^{0t}B, a^{1t}B, a^{2t}B, \ldots, a^{(p-1)t}B \tag{4.2.2}$$

also form a partition of G, that is $[A', B]$ is a factorization of G.

Multiply both sides of the factorization $[A, B]$ by a to get $aG = (aA)B$. As $aG = G$ and $aA = \{a^1, a^2, \ldots, a^p\}$, the sets

$$a^1B, a^2B, \ldots, a^{(p-1)}B, a^pB \tag{4.2.3}$$

form a partition of G. Since the sets 4.2.1 and 4.2.3 form a partition of G, we have that $a^pB = B$. We may say that the multiplication by a permutes the sets 4.2.1 cyclically. Thus if i and j are integers (positive or negative) and they are congruent modulo p, then $a^iB = a^jB$. As t is relatively prime to p, the collection of sets 4.2.2 is a permutation of those given by 4.2.1 and so $[A', B]$ is a factorization of G. □

Lemma 4.11. *Let p be a prime and let $q \geq 2$ be a positive integer not divisible by p. Let u and v be elements of the finite group G such that $uv = vu$. Let the order of u and v be p and q, respectively. Let $\alpha = [A, B]$ be a factorization of G, where*

$$A = \{e, uv, (uv)^2, \ldots, (uv)^{p-1}\}$$

is a cyclic subset. Then $\beta = [A', B]$ *is a factorization where*

$$A' = \{e, u, u^2, \ldots, u^{p-2}, u^{p-1}v\}$$

Note that A' *is a simulated subset if* $p \geq 3$.

Proof. Using Lemma 4.10 with $t = q$ replace A by $\langle u^q \rangle$. As $\langle u^q \rangle = \langle u \rangle$, A can be replaced by $A'' = \{e, u, u^2, \ldots, u^{p-1}\}$. Therefore,

$$u^0B, u^1B, u^2B, \ldots, u^{p-1}B \tag{4.2.4}$$

form a partition of G.

For a given i, $0 \leq i \leq p-2$ choose an integer t such that

$$(uv)^t = u^{p-1-i}v.$$

Since p and q are coprimes, the system of congruences

$$t \equiv p - 1 - i \pmod{p}$$

$$t \equiv 1 \pmod{q}$$

has a solution, and so such t exists. Clearly t is relatively prime to p. Thus, in the factorization α, A can be replaced by

$$C = \{e, (uv)^t, (uv)^{2t}, \ldots, (uv)^{(p-1)t}\}.$$

Note that $C = \{e, u^t v, u^{2t} v, \ldots, u^{(p-1)t} v\}$. Therefore, the sets

$$B, (uv)^t B, (uv)^{2t} B, \ldots, (uv)^{(p-1)t} B$$

form a partition of G. The only information we need from this partition is that B and $u^{p-1-i} vB$ are disjoint for each i, $0 \leq i \leq p-2$. We want to prove that the sets

$$B, uB, u^2 B, \ldots, u^{p-2} B, u^{p-1} vB$$

form a partition of G. Since the sets 4.2.4 form a partition of G it is enough to show that $u^{p-1} vB$ and $u^i B$ are disjoint for each $0 \leq i \leq p-2$. Suppose that they are not disjoint. Multiplying by u^{-i} we have the contradiction that $u^{p-1-i} vB$ and B are not disjoint. □

Lemma 4.12. *Let $[A, B]$ and $[A, B^{-1}]$ be factorizations of a finite group G, where A is an abelian set. Suppose that*

$$A = \{e, a_1 b_1, a_2 b_2, \ldots, a_{p-1} b_{p-1}\}$$

and a_1 and b_1 commute. Let $\mathrm{ord}(a_1) = p$, $\mathrm{ord}(b_1) = q$, where p is a prime and q is a positive integer such that $\gcd(p, q) = 1$. Then $[A', B]$ is a factorization of G, where

$$A' = \{e, a_1, a_1^2, \ldots, a_1^{p-2}, a_1^{p-1} b_1\}.$$

Proof. It is clear that $a_1 b_1 \neq e$. Thus, by Lemma 4.8, A can be replaced by C, where

$$C = \{e, a_1 b_1, (a_1 b_1)^2, \ldots, (a_1 b_1)^{p-2}, (a_1 b_1)^{p-1}\}.$$

If $q = 1$ then $b_1 = e$ and C is equal to A'. If $q \geq 2$ then by Lemma 4.11 the block C can be replaced by A', where

$$A' = \{e, a_1, a_1^2, \ldots, a_1^{p-2}, a_1^{p-1}b_1\}.$$

This concludes the proof. □

The following is the famous theorem of Hajós's, that was the answer to Minkowski's conjecture, finally given in 1942. Basically, Hajós transformed the original problem into an algebraic form which had a tremendous impact on the theory of factorizations of abelian groups.

Theorem 4.5. *[Hajós's Theorem] Let $[A_1, \ldots, A_n]$ be a normalized factorization of a finite abelian group G, where each A_i is a cyclic subset of G. Then at least one of the factors must be a subgroup of G.*

As we said Hajós's Theorem did inspire new questions and new work. Perhaps the most interesting is Rédei's generalization [15] in 1965 of Hajós's Theorem, where the factors are no longer required to be simulated or cyclic sets. However, there is a new type of restriction on the sizes of the blocks.

4.3 Rédei's Theorem

Rédei's Theorem has a substantial role in the theory of factorizations of finite abelian groups. It says that if $[B_1, \ldots, B_k]$ is a normalized factorization of finite abelian group G and all $|B_i|$, for $1 \leq i \leq k$ are prime numbers, then at least one of the blocks is a subgroup of G. We will prove this theorem in several steps.

First, we prove Rédei's Theorem for groups of type (p, p) where p is a prime. We will use concepts from finite geometries. Let X be a subset of an affine plane. We

say that X determines a direction if there are two points in X that span line in this direction. The affine plane we need is $[\mathbb{F}_p]^2$, where $\mathbb{F}_p$ is isomorphic to the finite field of of order p. First, we need one fact about finite fields.

Lemma 4.13. *Let $\mathbb{F}_q$ be a finite field, where q is a prime power. Then for any integer $n \geq 1$ it holds that*

$$S_n = \sum_{x \in \mathbb{F}_q} x^n = \begin{cases} 0 & \text{if } q-1 \nmid n \\ -1 & \text{if } q-1 \mid n \end{cases}$$

Proof. We use the fact that the multiplicative group of a finite field is cyclic [8]. Let $\mathbb{F}_q^*$ be the multiplicative group of the finite field $\mathbb{F}_q$ and let $\mathbb{F}_q^*$ be generated by $g \in \mathbb{F}_q^*$. Notice that we can omit the zero term in the sum S_n so if $q-1 \mid n$ then

$$S_n = \sum_{x \in \mathbb{F}_q^*} x^n = \sum_{x \in \mathbb{F}_q^*} 1 = q - 1 = -1.$$

On the other hand, if $q-1 \nmid n$ then $g^n \neq 1$, so

$$S_n = \sum_{i=0}^{q-2} (g^i)^n = \sum_{i=0}^{q-2} (g^n)^i = \frac{(g^n)^{q-1} - 1}{g^n - 1} = \frac{1-1}{g^n - 1} = 0.$$

□

Lemma 4.14. *If X is a subset of the affine plane $[\mathbb{F}_p]^2$ such that $|X| = p$ is a prime and X determines at most $(p+1)/2$ directions, then X is a straight line.*

Proof. Clearly, $[\mathbb{F}_p]^2$ determines $p+1$ directions. Since X determines at most $(p+1)/2$ directions, it follows that there is at least one direction that is not determined by X. Consequently, we can introduce a coordinate system in such a way that the direction of the second coordinate axis is not determined by X. Hence, X can be represented in the form

$$X = \{(k, b_k) \mid 0 \leq k \leq p-1\}.$$

It is convenient to represent the directions determined by X by the slopes of the corresponding straight lines. This is possible since none of the directions determined by X is parallel to the second coordinate axis. Set

$$U = \{\frac{b_k - b_m}{k - m} \mid 0 \leq k, m \leq p-1,\ k \neq m\}.$$

By the assumption of the lemma, $|U| \leq (p+1)/2$. Consider the polynomials

$$F_j(x) = \sum_{k=0}^{p-1} (b_k - kx)^j$$

in $\mathbb{F}_p$ for each j, $1 \leq j \leq (p+1)/2$. From Lemma 4.13 we have

$$\sum_{i=0}^{p-1} a_i^j = \begin{cases} 0 & \text{if } 0 \leq j \leq p-2, \\ \text{-1} & \text{if } j = p-1 \end{cases} \tag{4.3.1}$$

Hence, it follows that $\deg F_j(x) \leq j-1$. If $x \notin U$ then the elements are all distinct as k varies over $\mathbb{F}_p$. So, $x \notin U$ implies $F_j(x) = 0$. Since $\deg F_j(x) \leq j-1$ it follows that if $j - 1 < p - |U|$, then F_j is the zero polynomial. In particular F_j is the zero polynomial when $1 \leq j \leq (p+1)/2$. Using the fact that every function from $\mathbb{F}_p$ to $\mathbb{F}_p$ is a polynomial of degree less than equal to $p-1$, we can represent b_k in the form

$$b_k = c_0 + c_1 k + c_2 k^2 + \ldots + c_{p-1} k^{p-1}.$$

We will show that $c_m = 0$ for each m such that $1 \leq m \leq p-1$. This will show that X is a straight line. Divide $p-1$ by m with remainder. Then,

$$p - 1 = ma + b, \quad 0 \leq b \leq m-1.$$

Note that $1 \leq a$ and $a + b \leq (p-1)/2$ as $m \leq 2$. So $F_{a+b}(x)$ is the zero polynomial. Let us compute the coefficient of $(-x^b)$ in $F_{a+b}(x)$.

$$0 = \sum_{k=0}^{p-1} \binom{a+b}{b} b_k^a k^b = \binom{a+b}{b} \sum_{k=0}^{p-1} (c_m^a k^{am+b} + \sum_{j=b}^{p-2} d_j k^j).$$

Using 4.3.1 we get for this same coefficient

$$\binom{a+b}{b} c_m^a \sum_{k=0}^{p-1} k^{p-1} = -\binom{a+b}{b} c_m^a.$$

It follows that $c_m = 0$. This completes the proof. □

Lemma 4.15. *If $\alpha = [A, B]$ is a normalized factorization of a group G of type (p, p), such that $|A| = |B| = p$, then A or B is a subgroup of G.*

Proof. Let u, v be basis elements of G. The correspondence $u^i v^j \to (i, j)$ assigns the elements of G to the points of the affine plane $[\mathbb{F}_p]^2$. Subgroups of order p correspond to the straight lines passing through the point $(0, 0)$. The $p+1$ subgroups of order p of G correspond to the $p+1$ directions available on the plane. Suppose that the elements $a_1, a_2 \in G$ correspond to the points $p_1, p_2 \in [\mathbb{F}_p]^2$. Then the direction determined by the points p_1, p_2 correspond to the subgroup $\langle a_1 a_2^{-1} \rangle$ of G. For short, we will talk about the direction determined by a_1, a_2.

Next, we will show that if $G = AB$ is a factorization then the directions determined by the elements of A are distinct from the directions determined by the elements of B. Assume that there are $a_1, a_2 \in A$, $b_1, b_2 \in B$ such that $a_1 \neq a_2$, $b_1 \neq b_2$ and $\langle a_1 a_2^{-1} \rangle = \langle b_1 b_2^{-1} \rangle$. Multiply the factorization α by $a_2^{-1} b_2^{-1}$ to get the factorization $\beta = [A a_2^{-1}, B b_2^{-1}]$. By Lemma 4.8, $A a_2^{-1}$, $B b_2^{-1}$ can be replaced by $\langle a_1 a_2^{-1} \rangle$, $\langle b_1 b_2^{-1} \rangle$ respectively to get the factorization $\gamma = [\langle a_1 a_2^{-1} \rangle, \langle b_1 b_2^{-1} \rangle]$. But this is a contradiction as $\langle a_1 a_2^{-1} \rangle = \langle b_1 b_2^{-1} \rangle$. Since A and B determine distinct directions it follows that

either A or B determines at most $(p+1)/2$ directions. By the Lemma 4.14 it follows that A or B is a subgroup of G. This completes the proof. □

Lemma 4.16. *Let $\alpha = [A_1, A_2, \ldots, A_n]$ be a normalized factorization of finite abelian p-group G where $|A_i| = p$ for $1 \leq i \leq n$. Then, at least one of the blocks is a subgroup of G.*

Proof. The $n = 1$ case is trivial. We may assume that $n \geq 2$. By Lemma 4.8, every factor A_i can be replaced by a cyclic subset. If A_i contains an element of order at least p^2, then A_i can be replaced by a non-subgroup cyclic subset. If each factor has an element of order at least p^2, then we construct a factorization of G consisting of non-subgroup cyclic subsets. By Lemma 4.9, this is not possible. So there is a factor, say A_1, all of whose non-identity elements have order p. We assume that $n \geq 2$ and start induction on n.

By Lemma 4.8 factor A_1 can be replaced by a subgroup H_1 in the factorization α. Considering the factor group G/H_1 we have factorization

$$G/H_1 = (A_2H_1)/H_1 \ldots (A_nH_1)/H_1.$$

By the induction hypothesis, there is a permutation $B_1, B_2, \ldots, B_n$ of the factors $H_1, A_2, \ldots, A_n$ such that

$$B_1, B_1B_2, \ldots, B_1B_2 \cdots B_n$$

is an ascending chain of subgroups of G and $B_1 = H_1$. For notational convenience we assume that $B_2 = A_2, \ldots, B_n = A_n$ since this is only a matter of permutation of the indexes of the factors in the factorization $G = A_1A_2 \ldots A_n$. Consider the subgroup $M = H_1A_2 \ldots A_{n-1}$. Clearly, each of the factors $H_1, A_2, \ldots, A_{n-1}$ is a subset of M. If $A_1 \subseteq M$, then $M = A_1A_2 \ldots A_{n-1}$ is a factorization of M. By the inductive

assumption at least one of the factors $A_1, \ldots, A_{n-1}$ is a subgroup of M and so is a subgroup of G.

For the remaining part of the proof, we may assume that $A_1 \nsubseteq M$. We have

$$A_1 = \{e, x, x^2 d_2, \ldots, x^{p-1} d_{p-1}\}$$

and then $H_1 = \langle x \rangle$. Also, it is clear that $\{d_2, \ldots, d_{p-1}\} \nsubseteq M$. The factor A_n can be replaced by $A'_n = \{e, y, y^2, \ldots, y^{p-1}\}$, for each $y \in A_n \setminus \{e\}$. Since $G = MA'_n$ is a factorization of G, A'_n is a complete set of representatives modulo M. There are $u_2, \ldots, u_{p-1} \in A'_n$ such that

$$(x^2 d_2)^{-1} \in u_2 M, \ldots, (x^{p-1} d_{p-1})^{-1} \in u_{p-1} M,$$

that is

$$x^2 d_2 u_2, \ldots, x^{p-1} d_{p-1} u_{p-1} \in M.$$

Set

$$B = \{e, x, (x^2 d_2) u_2, \ldots, (x^{p-1} d_{p-1}) u_{p-1}\}.$$

Note that $B \subseteq M$ and $BA_2 \ldots A_{n-1}$ is a factorization of M. Indeed, the products coming from $BA_2 \ldots A_{n-1}$ are among the products coming from $A_1 A_2 \ldots A_{n-1} A'_n$. From the factorization $M = BA_2 \ldots A_{n-1}$ the inductive assumption gives that B is a subgroup of M. In fact $B = \langle x \rangle = H_1$. For each $i,\ 2 \leq i \leq p-1$, there is a $j,\ 0 \leq j \leq p-1$ such that $x^i d_i u_i = x^j$. It follows that $u_i = d_i^{-1} x^{j-i} \in A'_n$. From the fact that all elements of A_1 have order p, it follows that every d_i has order p. Therefore, every u_i, $2 \leq i \leq p-1$ has order p and hence $\mathrm{ord}(y) = p$. Since, y was any element from A_n different than e, it means that each element $A_n \setminus \{e\}$ has order p. Thus, $d_i \in \langle x, y \rangle$. Hence $A_1 \subseteq \langle x, y \rangle$. If $A_n \subseteq \langle x, y \rangle$, then $A_1 A_2$ is a factorization

of $\langle x, y\rangle$ and by Lemma 4.15 A_1 or A_2 is a subgroup. Therefore, we may assume tat $A_n \not\subseteq \langle x, y\rangle$. There is a $z \in A_n \setminus \{e\}$ such that $z \notin \langle x, y\rangle$. Replacing A_n by $A_n'' = \{e, z, z^2, \ldots, z^{p-1}\}$ we get that $d_2, \ldots, d_{p-1} \in \langle x, z\rangle$. Therefore,

$$d_2, \ldots, d_{p-1} \in \langle x, y\rangle \cap \langle x, z\rangle = \langle x\rangle$$

and so A_1 is a subgroup of G. □

Now, Rédei's Theorem can be proven in full generality.

Theorem 4.6. *Let $\alpha = [A_1, \ldots, A_n]$ be a normalized factorization of the finite abelian group G, where $|A_i| = p_i$ is a prime for each i, $1 \leq i \leq n$. Then, at least one of the factors $A_1, \ldots, A_n$ is a subgroup of G.*

Proof. The theorem holds for $n = 1$. We start an induction on n and assume that $n \geq 2$. If $|G|$ is a power of 2, then by Lemma 4.16 at least one of the factors is a subgroup of G. So we may assume that $|G|$ has a prime factor p with $p \geq 3$ and suppose that $A_1, \ldots, A_t$ are all factors among the $A_1, \ldots, A_n$ with cardinality p. Let $A_1 = \{e, a_1b_1, a_2b_2, \ldots, a_{p-1}b_{p-1}\}$ where a_i belongs to a p-Sylow subgroup of G and b_i to its complement.
By raising A_1 to the power s where $s = \text{lcm}(\text{ord}(b_1), \text{ord}(b_2), \ldots, \text{ord}(b_{p-1}))$ we obtain

$$A_1' = \{e, a_1^s, a_2^s, \ldots, a_{p-1}^s\}.$$

By Corollary 4.2, A_1 can be replaced by A_1'. Continuing this process there is a factorization $\beta = [A_1', \ldots, A_t', A_{t+1}, \ldots, A_n]$ of G such that A_i' contains only elements that have orders powers of p, or so called p-elements. Now $\gamma = [A_1', \ldots, A_t']$ is a factorization of the Sylow p-subgroup of G. By Lemma 4.16, at least one of the blocks of γ must be a subgroup of G. Let A_1' be the factor. If A_1 is a subgroup of G

there is nothing to prove. Considering that $\text{ord}(a_i) = \text{ord}(a_i^q)$ and the fact that A_1' is a group of order p, it follows that $\text{ord}(a_i) = p$ for i such that $1 \leq i \leq p-1$. As A_1 does not contain only p-elements, we suppose that $\text{ord}(b_1) = q$ and $p \nmid q$. Therefore, we see that A_1 satisfies the conditions of Lemma 4.12. So, there is a factorization $\eta = [A_1^*, A_2, \ldots, A_n]$ such that A_1^* is in the form

$$A_1^* = \{e, x, x^2, \ldots, x^{p-2}, x^{p-1}y\}$$

and $\text{ord}(x) = p$. Now, by Lemma 4.4 A_1^* can be replaced by

$$H_1 = \{e, x, x^2, \ldots, x^{p-2}, x^{p-1}\},$$

the corresponding subgroup. From this, considering the factor group G/H_1, we get the factorization

$$G/H_1 = (A_2H_1)/H_1 \cdots (A_nH_1)/H_1$$

of the factor group G/H_1.

Here $(A_iH_1)/H_1$ denotes the set of cosets $\{a_iH_1 \mid a_i \in A_i\}$. By the inductive assumption some factor $(A_iH_1)/H_1$ is a subgroup of G for some i, $2 \leq i \leq n$. We may assume that $i = 2$ because it is only matter of indexing the factors $A_1, \ldots, A_n$ in the factorization $G = A_1 \cdots A_n$. We may consider a suitable factor group again to get a new factorization. Continuing in this way we conclude that

$$H_1 \subset H_1A_2 \subset \cdots \subset H_1B_2 \cdots B_n$$

are subgroups of G. However, we may assume that the permutation is identical since this is the only a matter of indexing factors in $G = A_1 \cdots A_n$.

Let $M = H_1 A_2 \cdots A_{n-1}$. Note that

$$M = H_1 A_2 \cdots A_{n-1},\ G = MA_n$$

are factorizations of M and G respectively. Let $a \in A_n$. From the factorizations

$$G = A_1 A_2 \cdots A_n,$$

$$G = H_1 A_2 \cdots A_n,$$

$$G = MA_n$$

multiplying by a^{-1} we have the factorizations

$$G = A_1 A_2 \cdots A_{n-1}(a^{-1}A_n),$$

$$G = H_1 \cdots A_{n-1}(a^{-1}A_n),$$

$$G = M(a^{-1}A_n)$$

If $A_1 \subseteq M$ then $M = A_1 A_2 \cdots A_{n-1}$ is a factorization of M. By the inductive assumption, $A_i = H_i$ for some $i,\ 1 \leq i \leq n-1$.

If $A_1 \nsubseteq M$ then from the factorization $G = M(a^{-1}A_n)$ it follows that $a^{-1}A_n$ is a complete set of representative modulo M. Therefore, there exists an elements c_a of $a^{-1}A_n$ such that coset $c_a M$ contains the element $h_1^{-1}d_1^{-1}$, that is for which $h_1 d_1 c_a \in M$.

Let

$$C_a = (H_1 \setminus \{h_1\}) \cup \{h_1 d_1 c_a\}$$

$$= (A_1 \setminus \{a_1\}) \cup \{h_1 d_1 c_a\}.$$

We claim that $M = C_a A_2 \cdots A_{n-1}$ is a factorization of M. To prove the claim, note that $C_a \subseteq M$ and in addition products coming from $C_a A_2 \cdots A_{n-1}$ occur among the products coming from $A_1 A_2 \cdots A_{n-1}(a^{-1}A_n)$, and these latter are distinct since the product $A_1 \cdots A_{n-1}(a^{-1}A_n)$ is a factorization of G. To see this consider a product

$$x_1 x_2 \cdots x_{n-1},\ (x_1 \in C_a,\ x_2 \in A_2, \ldots,\ x_{n-1} \in A_{n-1})$$

If $x_1 \in A_1$, then

$$x_1 x_2 \cdots x_{n-1} \in A_1 A_2 \cdots A_{n-1}.$$

If $x_1 = h_1 d_1 c_a$, then as $h_1 d_1 \in A_1$ and $c_a \in (a^{-1}A_n)$. Using the factorization $M = C_a A_2 \cdots A_{n-1}$, the inductive assumption gives that one of the factors $C_a, A_2, \ldots, A_{n-1}$ is a subgroup of M since otherwise there is nothing to prove. In particular C_a is a periodic subset of M and so, by Lemma 4.3, $C_a = H_1$. Thus $h_1 d_1 c_a = h_1$, that is, $c_a = d_1^{-1}$ and so $d_1^{-1} \in a^{-1}A_n$. This gives

$$d_1^{-1} \in \bigcap_{a \in A_n} a^{-1}A_n.$$

The element d_1^{-1} is independent of the choice of a and $d_1^{-1} \neq e$. We can test the periodicity of A by its translates. By Lemma 4.2, A_n is periodic. By Lemma 4.3, A_n is a subgroup of G. This completes the proof. □

The following lemma shows that all factorizations of a finite abelian group G, when the sizes of the blocks are prime numbers, are transversal.

Lemma 4.17. *Let $\alpha = [B_1, B_2, \ldots, B_k]$ be a normalized factorization of the finite abelian group G such that $|B_i|$ is a prime for each i, $1 \leq i \leq k$. Then $\alpha \in \mathcal{T}(G)$.*

Proof. We give a proof by the consecutive use of Redei's Theorem. It is clear that the claim holds whenever the size of G is a prime number. Let $\alpha = [B_1, B_2, \ldots, B_k]$ be a factorization of G. According to Rédei's Theorem, there is at least one block that is a subgroup of G. Let it be B_1. It is not hard to see that $\beta = [C_2, \ldots, C_k]$ is a factorization of G/B_1, where $C_i = B_i B_1/B_1$. Since α is normalized, note that $B_i \cap B_j = \{e\}$. Therefore, it must be $|C_i| = |B_i|$ i.e. the sizes of the blocks in β are again prime numbers. Thus, at least one of the C_i must be a subgroup, say without loss of generality C_2. Since B_2B_1/B_1 is a subgroup of G/B_1, B_1B_2 is a subgroup of G. Continuing this process, we see that

$$\{e\} \leq B_1 \leq B_1B_2 \leq \ldots \leq B_1B_2 \ldots B_k = G$$

is an ascending chain of subgroups and hence α is a transversal factorization. □

There are examples of some groups, given in [11] for which all factorizations belong to $\mathcal{T}(G)$. For example, the factorizations of the dihedral group D_4 (of order 8) and of $Z_4 \times Z_2$ are all transversal, while there exist factorizations of the alternating group A_5 that are not transversal.

4.4 Non-full rank factorizations

In this section we study recursive decompositions of finite groups.

Definition 4.4. *A factorization $\alpha = [B_1, B_2]$ of a group G is called full-rank if $\langle B_1 \rangle = \langle B_2 \rangle = G$.*

We call the subsets B_1 and B_n the *ending* blocks of a factorization $[B_1, B_2, \ldots, B_n]$ of a group G.

Lemma 4.18. *A subset $V \subseteq G$ is an ending block of a factorization of G if and only if it is an ending block of a factorization of $\langle V \rangle$.*

Proof. Suppose that V is an ending block of $\langle V \rangle$. Since $\langle V \rangle$ is a subgroup of G, V is clearly an ending block of G. Let $[\langle V \rangle, A_1]$ be a factorization of G and let $[V, A_0]$ be a factorization of $\langle V \rangle$. Then, it is clear that $[V, A_0A_1]$ is a factorization of G.
Conversely, let $[V, A]$ be a factorization of G. Let $A_0 = A \cap \langle V \rangle$. Clearly, $VA_0 \subseteq \langle V \rangle$. Since $\langle V \rangle \subseteq VA$, then any $w \in \langle V \rangle$ can be written as $w = va$ from which follows that $a = v^{-1}w \in \langle V \rangle$ and therefore $a \in A_0$. We conclude that $\langle V \rangle \subseteq VA_0$ and therefore $[V, A_0]$ is a factorization of $\langle V \rangle$. □

The previous lemma can be helpful when we need to answer on question whether certain subset can be a block of a factorization. For example if $g \in G$ and $\mathrm{ord}(g) = m$, then any subset $A \subseteq \langle g \rangle$ such that $|A| = k$, where k does not divide m, can not be ending block of a factorization of G. Utilizing the transformations we have already discussed on factorizations we obtain different criteria for subsets to be ending blocks in factorizations of a group G. For example, we have

Corollary 4.4. *If $[B_1, \ldots, B_n]$ is a factorization of a group G then $B_1 \cdots B_i$ is an ending block of a factorization of $\langle B_1 \cup \ldots \cup B_i \rangle$ for $1 \leq i \leq n$. Similarly, $B_i \cdots B_n$ is an ending block of a factorization of $\langle B_i \cup \ldots \cup B_n \rangle$.*

Theorem 4.7. *Let V be a block of a factorization of group G with $\langle V \rangle \neq G$. Let $z = \frac{|G|}{|V|}$ and let $m = \frac{|G|}{|\langle V \rangle|}$. Let $C = \{c_1, \ldots, c_m\}$ be an arbitrary but fixed complete set of left coset representatives, so $C\langle V \rangle = G$. Then $[A, V]$ is a factorization of G if and*

only if A has the following form:

$$A = c_1A_1 \cup \ldots \cup c_mA_m,$$

where A_i are subsets of $\langle V\rangle$ such that $[A_i, V]$ is a factorization of $\langle V\rangle$.

Proof. Suppose that

$$A = c_1A_1 \cup \ldots \cup c_mA_m.$$

Then

$$AV = c_1A_1V \cup \ldots \cup c_mA_mV = c_1\langle V\rangle \cup \ldots \cup c_m\langle V\rangle = C\langle V\rangle = G.$$

To show that $[A, V]$ is a factorization of G, it remains only to observe that the second union is disjoint by the definition of set C. Note that the first union is also disjoint as it comes from replacing each member of the second by a proper subset.
Conversely, suppose that $[A, V]$ is a factorization of G and let $A_i = \langle V\rangle \cap c_i^{-1}A$ with C as above. Then $c_iA_i = c_i\langle V\rangle \cap A$ which has two consequences. Firstly,

$$A = c_1A_1 \cup \ldots \cup c_mA_m \tag{4.4.1}$$

and the union is disjoint. Also, it is easy to see that $A_i^{-1}A_i \subseteq A^{-1}A$ and therefore $A_i^{-1}A_i \cap VV^{-1} = \{e\}$. From $A_iV \subseteq \langle V\rangle$ it follows that $|A_i| \leq z/m$. On the other hand, from Equation 4.4.1 it follows that

$$z = |A| \leq \sum_{i=1}^{m} |A_i|$$

and therefore $|A_i| = z/m$, for $1 \leq i \leq m$. Hence, $[A_i, V]$ is a factorization of $\langle V\rangle$. □

4.5 Factorizations by free mappings

In this section, A and B will denote groups. We introduce the new notion of *free mappings*, a tool for factorizing groups in a certain class. Firstly, we will show how to utilize free mappings in order to obtain factorizations of the direct product $A \times B$. Later, we will show that a broader class of groups, among which is the semidirect product of groups, can be factorized by using free mappings if certain conditions are satisfied.

Definition 4.5. *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 $A \times B$, given a pair of free mappings f, g.

Theorem 4.8. *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 4.1, α is a factorization of $A \times B$. □

Let A and B be groups and H 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 4.19. *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 $b_2b_1^{-1} = e$, 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 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 4.6. *Consider the group*

$$G =< a, b, c \mid a^2 = b^3 = c^3 = e,\ b^a = b,\ c^a = c^{-1},\ bc = cb >$$

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 4.19 in order to find a pair of free mappings. We choose a subgroup H *of* $\mathcal{S}_3$, *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:*

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

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

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.*

We can generalize Theorem 4.8 in the following way.

Theorem 4.9. *Let A, B be subgroups of a finite group G such that $A \cap B = \{e\}$. Let $f : A \to B$ and $g : B \to A$ be a pair of free mappings such that*

$$f(a)g(b) = g(b)f(a)$$

for $a \in A$ and $b \in B$. Then, the product of sets $\bar{A}\bar{B}$, where $\bar{A} = \{af(a) \mid a \in A\}$ and $\bar{B} = \{g(b)b \mid b \in B\}$ is direct, i.e. $|\bar{A}\bar{B}| = |\bar{A}||\bar{B}|$.

Proof. Suppose that

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

where $a_1, a_2 \in A$ and $b_1, b_2 \in B$. Then, it follows

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

Using the fact that $A \cap B = \{e\}$, we have

$$a_1 g(b_1) = a_2 g(b_2) \text{ and } f(a_1) b_1 = f(a_1) b_1.$$

Then, since f, g is a pair of free mappings, it follows that

$$a_1 = a_2 \text{ and } b_1 = b_2,$$

which means that

$$a_1 f(a_1) = a_2 f(a_2) \text{ and } g(b_1) b_1 = g(b_2) b_2$$

and therefore $|\bar{A}\bar{B}| = |\bar{A}||\bar{B}|$. □

The following lemma, based on the previous theorem, gives a constructive way for

obtaining a pair of free mappings $f : A \to B$ and $g : B \to A$ such that

$$f(a)g(b) = g(b)f(a),$$

for $a \in A$ and $b \in B$. Here, A and B are subgroups of a finite group G and $A \cap B = \{e\}$.

Lemma 4.20. *Let A and B be subgroups of a finite group G. Let $H = A \cap C_G(B)$ and $f : A \to B$ and $g : B \to A$ be any two mappings such that $Im(g) \subseteq H$ and f is constant on cosets of H. Then f, g is a pair of free mappings and*

$$f(a)g(b) = g(b)f(a).$$

Moreover, if $A \cap B = \{e\}$ then the product of sets $\bar{A}\bar{B}$, where $\bar{A} = \{af(a) \mid a \in A\}$ and $\bar{B} = \{g(b)\, b \mid b \in B\}$ is direct.

Proof. The first part follows directly from Lemma 4.19 and the fact that $\mathrm{Im}(g) \subseteq A \cap C_G(B)$. The second part is a simple consequence of the previous theorem. □

It is clear that we could interchange A and B since everything is symmetric. The previous lemma gives us a way of constructing nontrivial factorizations of a finite group G, provided the following requirements hold:

a. $A \cap B = \{e\}$, where A and B are subgroups of G.

b. Either $H = A \cap C_G(B)$ or $S = B \cap C_G(A)$ is a nontrivial subgroup of G.

c. $|A||B| = |G|$.

Note that if G is the semidirect product of A and B then conditions *a.* and *c.* are immediately satisfied. Therefore, the technique described in the previous lemma could be applied in the case when G is a semidirect product. In the following example, we are going to illustrate the technique proposed in the lemma above.

Example 4.7. *Let* $G = D_{12} = \langle u, v \rangle$ *be a dihedral group of order* 24*, such that* $\mathrm{ord}(u) = 12$ *and* $\mathrm{ord}(v) = 2$*. Let*

$$A = \{e, u^3, u^6, u^9, vu, vu^4, vu^7, vu^{10}\}, \quad B = \{e, u^4, u^8\}.$$

Clearly, $A \cap B = \{e\}$ *and* $|G| = |A||B|$*. Then,* $H = A \cap C_G(B) = \{e, u^3, u^6, u^9\}$*. Let us construct* $f : A \to B$ *such that* f *is constant on cosets of* H *and* $g : B \to A$ *such that* $\mathrm{Im}(g) \subseteq H$*. So, let*

$$f : \begin{pmatrix} e & u^3 & u^6 & u^9 & vu & vu^4 & vu^7 & vu^{10} \\ e & e & e & e & u^4 & u^4 & u^4 & u^4 \end{pmatrix}$$

and $g(e) = e,\ g(u^4) = u^6,\ g(u^8) = u^3$*. Then,*

$$\bar{A} = \{af(a) \mid a \in A\} = \{e, u^3, u^6, u^9, vu^2, vu^5, vu^8, vu^{11}\}$$

and $\bar{B} = \{g(b)\, b \mid b \in B\} = \{e, u^{10}, u^{11}\}$*. It is easy to check that* $[\bar{A}, \bar{B}]$ *is actually a factorization of* G*.*

4.6 Free mappings in 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 4.8. At the end we show an interesting application of Rédei's theorem with a number theoretic implication.

Lemma 4.21. *Let $f : A \to B$ and $g : B \to A$ be two mappings between groups A and B. Let $\mathcal{R}_{f,g}$ be the relation, induced by those mappings on $A \times B$ and defined by*

$$(s,t)\mathcal{R}_{f,g}(u,w) \Leftrightarrow \begin{array}{l} f(s)f(u)^{-1} = tw^{-1}, \\ g(t)g(w)^{-1} = su^{-1}. \end{array}$$

Then, $\mathcal{R}_{f,g}$ 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

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

it follows that

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

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

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

$$f(u)f(z)^{-1} = wr^{-1}, \;\; g(w)g(r)^{-1} = uz^{-1}.$$

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

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

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

Note that in the case of abelian groups A and B, $(a_1,b_1)\mathcal{R}_{f,g}(a_2,b_2)$ if and only if (a_1,b_1), (a_2,b_2) is a clip of f and g.

Theorem 4.10. *Let $f : A \to B$ and $g : B \to A$ be mappings where A, B are 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 every equivalence class of $\mathcal{R}_{f,g}$ contains just one element.*

Proof. Suppose $(a_1,b_1)\mathcal{R}_{f,g}(a_2,b_2)$. Clearly $a1 \neq a_2$ if and only if $b_1 \neq b_2$. Hence, $(a_1,b_1),(a_2,b_2)$ is a strong clip for f and g.
Conversely, if f and g are free then $(a_1,b_1)\mathcal{R}_{f,g}(a_2,b_2)$ if and only if $a_1 = a_2$, $b_1 = b_2$. Therefore, each equivalence class of $\mathcal{R}_{f,g}$ contains just one element. □

4.6.1 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 on $\mathbb{Z}_p$, and let ℓ_1, ℓ_2 be the two distinct lines, passing through the origin, corresponding to f and g respectively.

Then,

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

where $a_1, a_2, b_1, b_2 \in \mathbb{Z}_p$. Clearly, the lines ℓ_1 and ℓ_2 i 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 non-zero elements and then there exist i $m_1, m_2 \in \mathbb{Z}_p$ such that

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

It is easy to check that the two mappings

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

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

Lemma 4.22. *Let f, g be the mappings defined as*

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

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

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

By Lemma 4.22, given a pair of non-parallel lines, through the origin, 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 4.6, either B_1 or B_2 is a subgroup of G, and then that block can be seen as a line through the origin in the affine plane $AG(2, p)$. Thus, we can state the following lemma.

Lemma 4.23. *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 4.8. *Let $G = \mathbb{Z}_3 \times \mathbb{Z}_3$ and*

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

Then, $\alpha = [B_1, B_2]$ is a factorization of G. Clearly, even though B_1 is a line, the factorization α is not of the type given by Theorem 4.8. 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 4.23, 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 4.22. The following lemma provides a characterization in the general case.

Lemma 4.24. *Let $A \subset \mathbb{Z}_p \times \mathbb{Z}_p$, where $|A| = p$. Let $g : \mathbb{Z}_p \to \mathbb{Z}_p$ be defined by $g(y) = my$, and $B = \{(my, y) \mid y \in \mathbb{Z}_p\}$. Then, $\alpha = [A, B]$ is a factorization of $\mathbb{Z}_p \times \mathbb{Z}_p$ provided that*

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

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

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

Hence,

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

which contradicts the given assumption. □

Theorem 4.11. *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*

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

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

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

Let us consider Example 4.8 and the automorphism σ_1 of $\mathbb{Z}_3 \times \mathbb{Z}_3$ defined by the matrix $M_1 = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$. The automorphism action of σ_1 on the factorization α yields the factorization: $\sigma_1(\alpha) = [\sigma_1(B_1), \sigma_1(B_2)]$, where

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

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 $f : \begin{pmatrix} 0 & 1 & 2 \\ 0 & 0 & 2 \end{pmatrix}$.

In the following theorem we generalize this approach.

Theorem 4.12. *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. □

Theorem 4.12 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

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

4.6.2 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 4.6. *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 4.13. *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 $V = \mathrm{circ}(c_p, c_{p-1}, \ldots, c_1)$. 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. $\square$

Definition 4.7. *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 4.25. *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,

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

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 $C = \text{circ}(c_p, c_{p-1}, \dots, c_1)$, $b = (b_1, b_2, \dots, b_p)^t$ 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 4.13, 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 [17], the proof presented here is based on a new method, using circulant matrices and cyclotomic polynomials.

Lemma 4.26. *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

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

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

Corollary 4.5. *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 4.8 we have the following result.

Corollary 4.6. *$\alpha = [B_1,\ B_2]$ 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 are 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 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 4.8. 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 4.14. *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* f *and* g *are chained whenever* p *and* q *are different primes.*

Proof. Let us suppose that f and g are free. By Theorem 4.8, $\alpha = [B_1, B_2]$ is a factorization of $\mathbb{Z}_p \times \mathbb{Z}_q$ where

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

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. □

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. The following example shows that the assumption for p and q to be different primes can not 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, $|Im(f)| > 1$, $|Im(g)| > 1$, $f(0) = 0$, $g(0) = 0$. 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

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

4.7 Orbits of blocks of factorization

In this section, we connect the orbits of k complete sets, seen in Chapter 3 with a special kind of factorization of a finite cyclic group G. Namely, we will introduce a group action of the group of automorphisms of G on the blocks of factorization of type (m, n) where $\gcd(m, n) = 1$. Using the results given in the Chapters 2 and 3 we will be able to provide representatives of orbits of the considered action and the number of orbits as well. To achieve a simple exposition and compatibility with the results in the Chapters 2 and 3, we will identify a finite cyclic group G as the group of residue classes modulo an integer.

We start by bringing out one important result which gives useful information on

the nature of blocks in the case when the factorization is of type (m, n), where m and n are coprime.

Lemma 4.27. *Let $\alpha = [A, B]$ be a normalized factorization of $\mathbb{Z}_{mn}$, where $|A| = m$, $|B| = n$ and $\gcd(m, n) = 1$. Then A is an $n-$complete set and B is an $m-$complete set.*

Proof. According to corollary 4.2 it follows that $[mA, B]$ is also a factorization of Z_{mn}. However, mA is contained in the unique cyclic subgroup of order n of the group Z_{mn}. Since $|mA| = n$, it follows that mA is the subgroup of order n. Let us suppose that $b_1 - b_2 \equiv 0 \pmod{m}$ where $b_1, b_2 \in B$. It follows that $b_1 - b_2 = ms$, where $1 \leq s \leq n - 1$. However, $ms \in mA$ and

$$0 + b_1 = ms + b_2,$$

so we have that one element is represented in two different ways and this contradicts the fact that $[mA, B]$ is a factorization. Therefore, B contains all residue classes modulo m and similarly one can prove that A contains all residue classes modulo n. □

Let $\alpha = [A, B]$ be a factorization of type (m, n) of the $\mathbb{Z}_{mn}$, where $\gcd(m, n) = 1$. We say that A, (B) is *complement* of the block B, (A) respectively. From now on, m and n will denote coprime, positive integer numbers.

Like in Section 3.2, let $\mathcal{C}_m$, $\mathcal{C}_n$ be the collection of m, $n-$complete subsets of $\mathbb{Z}_{mn}$. Let us consider the action of the group of automorphisms of $\mathbb{Z}_{mn}$ on the sets $\mathcal{C}_m$ and $\mathcal{C}_n$. Using the results provided in Lemma 3.3, Lemma 3.4, and Cauchy-Frobenius Theorem we obtain the number of orbits of $m-$complete or $n-$complete sets. Similarly, using the algorithm **IsInOrbit** it is possible to check if two $m, n-$complete sets are in the

same orbit or not. The following lemma enlightens a practical use of action of the group $\mathcal{I}(mn)$ on the collection of m or n complete sets regarding factorization of $\mathbb{Z}_{mn}$.

Lemma 4.28. *Let O_m, O_n be arbitrary orbits of $m-$complete sets, $n-$complete sets under the action of $\mathcal{I}(mn)$ on the sets $\mathcal{C}_m$, $\mathcal{C}_n$ respectively. Suppose that there exists $A \in O_m$ and $B \in O_n$ such that $\alpha = [A, B]$ is a factorization of $\mathbb{Z}_{mn}$. Then A, B can be replaced by any element of O_m, O_m respectively.*

Proof. Statement is the direct consequence of corollary 4.2. □

Clearly, every m complete set in $\mathbb{Z}_{mn}$ can be completed by an n complete set $K = \{ni \mid 0 \leq i \leq m-1\}$ and every $n-$complete set can be completed by $m-$complete set $H = \{mj \mid 0 \leq j \leq n-1\}$. Note that H and K are unique subgroups of order m and n respectively of $\mathbb{Z}_{mn}$. We say that the orbits O_m, O_n are *connected* if there exist $A \in O_m$ and $B \in O_n$ such that $[A, B]$ is a factorization of $\mathbb{Z}_{mn}$.

Example 4.11. *Consider the group $\mathbb{Z}_{12}$ and its factorizations of type $(4, 3)$. There are 10 orbits of 4 complete sets in $\mathbb{Z}_{12}$. We list them all.*

$$\mathcal{U}_1 = \{\{0,1,2,3\},\{0,2,7,9\},\{0,3,5,10\},\{0,9,10,11\}\},$$
$$\mathcal{U}_2 = \{\{0,1,2,7\},\{0,5,10,11\}\},\ \mathcal{U}_3 = \{\{0,1,6,7\},\{0,5,6,11\}\},$$
$$\mathcal{U}_4 = \{\{0,1,2,11\},\{0,5,7,10\},\{0,1,10,11\},\{0,2,5,7\}\},$$
$$\mathcal{U}_5 = \{\{0,1,3,6\},\{0,3,5,6\},\{0,6,7,9\},\{0,6,9,11\}\},$$
$$\mathcal{U}_6 = \{\{0,1,6,11\},\{0,5,6,7\}\},\ \mathcal{U}_7 = \{\{0,2,3,9\},\{0,3,9,10\}\},$$
$$\mathcal{U}_8 = \{\{0,1,3,10\},\{0,7,9,10\},\{0,2,9,11\},\{0,2,3,5\}\},$$
$$\mathcal{U}_9 = \{\{0,1,7,10\},\{0,2,5,11\}\},\ \mathcal{U}_{10} = \{\{0,3,6,9\}\}$$

There are 7 *orbits of* 3 *complete sets in* $\mathbb{Z}_{12}$.

$$\mathcal{V}_1 = \{\{0,1,2\},\{0,10,11\},\{0,2,7\},\{0,5,10\}\},$$
$$\mathcal{V}_2 = \{\{0,1,5\},\{0,7,11\}\},\ \mathcal{V}_3 = \{\{0,1,11\},\{0,5,7\}\},$$
$$\mathcal{V}_4 = \{\{0,1,8\},\{0,4,11\},\{0,4,5\},\{0,7,8\}\},$$
$$\mathcal{V}_5 = \{\{0,2,4\},\{0,8,10\}\},\ \mathcal{V}_6 = \{\{0,2,10\}\},\ \mathcal{V}_7 = \{\{0,4,8\}\}$$

Let $M = (m_{ij})$ *be a matrix of type* 10×7 *such that* $m_{ij} = 1$ *if* $\mathcal{U}_i$ *is connected to* $\mathcal{V}_j$. *By examination, we see that* $m_{ij} = 1$ *if* $i = 10$ *or* $j = 7$, *when* $i = 3, j = 5$ *and* $i = 3, j = 6$. *In all other cases,* $m_{ij} = 0$.

Bibliography

[1] Nataša Božović and Žarko Mijajlović. *Uvod u Teoriju Grupa*. Naučna knjiga, Beograd, 1990.

[2] Vladimir Božović and Nicola Pace. Factorization of groups using free mappings. *Journal of Algebra and its Applications*, 7(5):647–662, 2008.

[3] N.G. De Bruijn. *Polyas Theory of Counting*, chapter 5, pages 144–184. E.F., Wiley, 1964.

[4] N.G. De Bruijn. A survey of generalizations of polyas enumeration theorem. *Nieuw Archief voor Wiskunde*, 19:89–112, 1971.

[5] D.S. Dummit and Foote. *Abstract Algebra*. Prentice-Hall, Upper Saddle River, NJ, 1999.

[6] G. Haj'os. *Ü*ber einfache und mehrfache bedeckung des n-dimensionalen raumes mit einem w*ü*rfelgitter. *Math. Zeitschr.*, 47:427–467, 1941.

[7] M.A. Harrison and R.G. High. On the cycle index of a product of permutation groups. *Journal of Combinatorial Theory*, (4):277–299, 1968.

[8] I.N. Herstein. *Topics in algebra*. John Wiley and Sons, 1975.

[9] M.W. Liebeck, C.E. Praeger, and J.Saxl. The maximal factorizations of the finite simple groups and their automorphism groups. *Memoirs Amer. Math. Soc.*, 86:1–151, 1990.

[10] S.S. Magliveras. A cryptosystem from logarithmic signatures over finite groups. In *Proceedings 29th Midwest Symposium on Circuits and Systems*, pages 972–975. Elsevier, 1986.

[11] S.S. Magliveras and N.D. Memon. Algebraic properties of cryptosystem pgm. *Journal of Cryptology*, 5(3):167–184, 1992.

[12] H. Minkowski. *Diophantische Approximationen*. Thubner, Leipzig, 1907.

[13] G. Pólya. Kombinatorische anzahlbestimmungen fr gruppen, graphen und chemische verbindungen. *Acta Math.*, 68:145–254, 1937.

[14] G. Pólya and R.C. Read. *Combinatorial Enumeration of Groups, Graphs and Chemical Compounds*. Springer Verlag, New York, Berlin, Heidelberg, London, Paris, Tokyo, 1987.

[15] L. Rédei. Die neue theorie der endlichen abelschen gruppen und verallgemeinerung des hauptsatzes von hajós. *Acta Math. Acad. Sci. Hung.*, 16:329–373, 1965.

[16] D. R. Stinson S. S. Magliveras and T. van Trung. New approaches to designing public key cryptosystems using one-way functions and trap-doors in finite groups. *Journal of Cryptology*, 15:285–297, 2002.

[17] A. D. Sands. On the factorization of finite groups. *J. London Math. Soc.*, 2(7):627–631, 1974.

[18] S. K. Stein. Factoring by subsets. *Pacific Journal of Mathematics*, 22(3):523–543, 1967.

[19] S. Szabó. *Topics in Factorization of Abelian Groups*. Birkhäuser, 2004.

[20] V.A. Ustimenko. Graphs with special arcs and cryptography. *Acta Applicandae Mathematicae*, 74:117–153, 2002.

[21] Wan-Di Wei and Ju-Yong Xu. Cycle index of direct product of permutation groups and number of equivalence classes of subsets of $\mathbb{Z}_v$. *Discrete Mathematics*, 123:179–188, 1993.

[22] Hans J. Zassenhaus. *The Theory of Groups*. Dover, 1958.