



University of Benghazi

Faculty of Science

Department of Mathematics

**The Number of Subgroups of a Finite
Abelian Group**

**Submitted in partial fulfillment of the requirements for the
degree of master of science in mathematics**

By

Wafa Omar Ali

Supervisor

Dr. Mohamed Al-Awami

Benghazi -Libya

(2012-2013)

Dedication

This work is dedicated to my family, who never cease to provide me tremendous support and encouragement.

Acknowledgement

First I want to express my sincere gratitude to Allah, whose great help was the main driving force behind my ability and determination to accomplish this work.

I would also like to thank my parents, for their unceasing encouragement, patience, and great support, which was great help during the completion of this work.

I am grateful to my supervisor, Dr. Mohamed AL-Awami whose guidance enabled me to develop the understanding of the subject. I also wish to express my gratitude and appreciation to my friend Nagla Buzghia, an engineering specialist, who was instrumental in helping me to programming software by MATLAB language.

Special thanks are also owed to the Head of the Department of Mathematics, Dr. Shaban Traina, and all the staff of the Mathematics Department, Benghazi University for their help during the preceding years of the study.

Contents

<i>Subject</i>	<i>Page no.</i>
Abstract	i
Introduction	ii
Chapter One	
Preliminary	1
Chapter Two	
Finite Abelian Groups	
2.1 The structure of Abelian groups	12
2.2 Automorphisms of cyclic groups	17
Chapter Three	
Counting Subgroups of Finite Abelian Groups	
3.1 The total number of subgroups of a finite Abelian group whose orders below thirty	21
3.2 The total number of subgroups of a finite Abelian p-group	25
3.3 The number of cyclic subgroups of a finite Abelian group	33
3.3.1 The number of cyclic subgroups of $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_r}$	33
3.3.2 The number of cyclic subgroups of $\mathbb{Z}_n \times \mathbb{Z}_n \times \cdots \times \mathbb{Z}_n$	36

Chapter Four

Combinatorial Problems On The Subgroup Lattices of Finite Abelian Groups

4.1	Fundamental group lattices	39
4.2	The number of subgroups of a finite Abelian p -group	43
4.3	The number of cyclic subgroups of a finite Abelian p - group....	47
	Appendix	53
	Conclusions and future work	58
	References	59
	Arabic Summary	61

Abstract

The goal of this thesis is to determine the number of subgroups of a finite Abelian group G . Since a finite Abelian group is a direct product of Abelian p -groups, the counting problem is reduced to p -groups. More precisely, suppose that $p_1^{r_1} p_2^{r_2} \dots p_k^{r_k}$ is the decomposition of $|G|$ as a product of prime factors and let $G_{p_1} \times G_{p_2} \times \dots \times G_{p_k}$ be the corresponding primary decomposition of G . In that case, $N(G) = \prod_{i=1}^k N(G_{p_i})$, where $N(G)$ denotes the number subgroups of the group G . Three programs by MATLAB language are introduced, as a convenient method for counting some different subgroup types of a finite Abelian p -group.

Introduction

One of the most important problems pertaining to the Abelian group theory is determining the number of subgroups of finite Abelian group. This topic has been gaining interest of the scientific community since the first half of the 20th century. However, as a finite Abelian group is a direct product of Abelian p-groups, the above counting problem is reduced to p-groups. Mathematical expressions Formulas that give the number of subgroups of type μ of a given finite p-group of type λ were first published by Delsarte, Djubjuk, and Yeh in 1948. An excellent survey on this subject, providing links to symmetric functions was written by Butler in 1994. Another way to determine the total number of subgroups of finite Abelian p-groups is presented in [3] and is applied for rank two p-groups , as well as for elementary Abelian p-groups. Tărnăuceanu gave slightly different method for counting the number of all subgroups of several particular finite Abelian p- groups, based on properties of certain matrices attached to the invariant factors decomposition of an Abelian group G , i.e. $G \cong \mathbb{Z}_{d_1} \times \dots \times \mathbb{Z}_{d_k}$, where $d_1 d_2 \dots d_k = |G|$, $d_1 \mid d_2 \mid \dots \mid d_k$. Finally in 2012, L.Tóth developed explicit formula for determining the number of all cyclic subgroups of a direct product of several finite cyclic groups.

In this thesis we will solve one of the open problems of [14] by introducing three programs by MATLAB language to count the number of all subgroups of a finite Abelian p-group.

The thesis consists of four chapters, organized as follows:

In chapter one, all basic definitions and properties which are mostly used in this thesis are discussed.

Chapter two provides background on the structure of finite Abelian groups of order n .

In Chapter three, different methods for computing the number of subgroups of finite Abelian groups are presented.

Finally, chapter four provides an application of the concept of the fundamental group lattice in counting some different t subgroup types of finite Abelian groups.

Chapter One

Preliminary

In this chapter, some of the basic concepts of finite group theory are introduced, we recall also the basic lattice theoretic concepts.

Definition 1.1 [10]

A nonempty set G is a group, if to every pair $(x, y) \in G \times G$ an element $xy \in G$ is assigned, the product of x and y , satisfying the following axioms:

Associativity: $x(yz) = (xy)z$ for all $x, y, z \in G$.

Existence of an identity: There exists an element $e \in G$ such that $ex = xe = x$ for all $x \in G$.

Existence of inverses: For every $x \in G$ there exists an element $x^{-1} \in G$ such that $xx^{-1} = e = x^{-1}x$.

A group G is Abelian if, in addition, the following holds:

Commutativity: $xy = yx$ for all $x, y \in G$.

Examples 1.1

- i. The set $\mathbb{Z}_n = \{[0], [1], [2], \dots, [n-1]\}$ of congruence classes modulo n forms finite Abelian group with respect to addition.
- ii. The set $U(n)$ of all positive integers smaller than n , for each $n \geq 1$, and relatively prime to n is finite Abelian group under multiplication modulo n . For example, $U(10) = \{[1], [3], [7], [9]\}$.

Definition 1.2 [10]

A group G is finite if G contains only finitely many elements. In this case, the number of elements is called the order of G , denoted by $|G|$.

Definition 1.3 [13]

A subgroup H of a group G is a non-empty subset of G , which forms a group under the operation of G , and we then write $H \leq G$.

Definition 1.4 [18]

- i. A subgroup H of a group G is called proper if $H \neq G$, and is denoted by $H < G$.
- ii. The singleton set $\{e\}$ forms a subgroup of all groups and is called the trivial subgroup.
- iii. A subgroup H of a group G is called maximal in G if it is a proper subgroup of G , and whenever a subgroup M exists satisfying $H \leq M \leq G$, then either $M = H$ or $M = G$.

Proposition 1.1 [10]

A nonempty finite subset H of G is a subgroup if for all $x, y \in H$ also xy is in H .

Remark.

Any intersection of subgroups of a group G is also a subgroup of G .

Definition 1.5 [18]

A group G is called cyclic group if there is an element g in G such that $G = \{g^n \mid n \in \mathbb{Z}\}$. Element g is called a generator of G , and the cyclic group generated by g is $\langle g \rangle$.

Example 1.2

The group \mathbb{Z}_n under addition modulo n is cyclic. If $n > 1$, then both 1 and $n - 1$ are generators, even though there may be others.

Definition 1.6 [9]

The order $o(g)$ of an element g in a group G is the smallest positive integer n such that $g^n = e$.

Remark.

- i. Every cyclic group is Abelian.
- ii. If the cyclic subgroup $\langle g \rangle$ of G is finite, then $o(g) = |\langle g \rangle|$.

Theorem 1.1 [6]

A subgroup of a cyclic group is cyclic.

Theorem 1.2 [13]

A group $G \neq \{e\}$, with no nontrivial subgroup is a finite cyclic group of prime order.

Theorem 1.3 [19]

A cyclic group of order n has a unique subgroup of order d , for each positive divisor d of n .

Remark.

A finite group that contains exactly one maximal subgroup is cyclic of prime power order. The converse is also true.

Theorem 1.4 [8]

If d is a positive divisor of n , the number of elements of order d in a cyclic group of order n is $\phi(d)$.

In the statement above, ϕ is the Euler ϕ -function, and it is defined for

positive integer n by $\phi(n) = m$, where m is the number of positive integers less than or equal to n that are relatively prime to n .

Definition 1.7 [10]

Let H be a subgroup of G and $x \in G$. The subset of G consisting of the product $Hx = \{hx \mid h \in H\}$ and $xH = \{xh \mid h \in H\}$ is respectively a right coset, and a left coset of H in G .

The number of distinct right cosets of H in G is called the index of H in G , and is denoted by $|G:H|$.

Theorem 1.5 (Lagrange's Theorem) [10]

Let H be a subgroup of the finite group G . Then $|G| = |H||G:H|$. In particular, the integers $|H|$ and $|G:H|$ are divisors of $|G|$.

Remark.

If G is a finite Abelian group, then the converse of Lagrange's theorem is true for G .

Corollary 1.1 [10]

For every finite group G and every $g \in G$, the order of g divides $|G|$.

Corollary 1.2 [13]

A cyclic group of prime order contains no nontrivial subgroups.

This is the converse of Theorem 1.2, and follows immediately from Theorem 1.5.

Definition 1.8 [10]

Let G and \bar{G} be groups. A mapping $\varphi: G \rightarrow \bar{G}$ is a homomorphism from G to \bar{G} , if

$$(xy)^\varphi = x^\varphi y^\varphi \quad \text{for all } x, y \in G.$$

Let φ be a homomorphism from G to \bar{G} . We set

$$\text{Ker } \varphi := \{x \in G \mid x^\varphi = e_{\bar{G}}\}, \text{Im } \varphi := G^\varphi.$$

We refer to $\text{Ker } \varphi$ as the kernel of φ and $\text{Im } \varphi$ as the image of φ . The homomorphism φ is an epimorphism if $\text{Im } \varphi = \bar{G}$, an endomorphism if $\bar{G} = G$. Moreover, it is a monomorphism if φ injective, an isomorphism if φ bijective, and an automorphism if φ is a bijective endomorphism.

If φ is an isomorphism, then G is said to be isomorphic to \bar{G} ; in which case we may write $G \cong \bar{G}$.

Theorem 1.6 (The Structure of Cyclic Groups) [10]

Let G be a cyclic group with generator g . If G has finite order n , then G is isomorphic to $\langle \mathbb{Z}_n, +_n \rangle$.

Definition 1.9 [7]

A group G is cocyclic if $G \cong \mathbb{Z}_{p^k}$, where p is a prime number and $k = 1, 2, \dots, \infty$.

Definition 1.10 [10]

A subgroup H of G that satisfies $Hx = xH$ for all $x \in G$ is a normal subgroup of G , which is denoted by $H \triangleleft G$.

It should be noted here that all subgroups of Abelian groups are normal.

Proposition 1.2 (Product Formula) [19]

If H and K are subgroups of a finite group G , then $|HK||H \cap K| = |H||K|$, where $HK = \{hk : h \in H \text{ and } k \in K\}$.

Proposition 1.3 [19]

- i. If H and K are subgroups of a group G , and if one of them is a normal subgroup, then HK is a subgroup of G , and $HK = KH$.

- ii. If both H and K are normal subgroups of a group G , then HK is a normal subgroup.

Definition 1.11 [10]

Let G_1, \dots, G_n be groups. The Cartesian product of the sets G_i

$$\prod_{i=1}^n G_i = G_1 \times \dots \times G_n = \{ (g_1, \dots, g_n) \mid g_i \in G_i \},$$

is a group with respect to componentwise multiplication

$$(g_1, \dots, g_n)(h_1, \dots, h_n) = (g_1 h_1, \dots, g_n h_n).$$

This group is the external direct product of the groups G_1, \dots, G_n .

Theorem 1.7 [6]

The group $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic and is isomorphic to \mathbb{Z}_{mn} if and only if m and n are relatively prime.

Corollary 1.3 [6]

The group $\prod_{i=1}^n \mathbb{Z}_i$ is cyclic and isomorphic to $\mathbb{Z}_{m_1 \dots m_n}$ if and only if the numbers m_i for $i = \overline{1, n}$ are such that the gcd of any two of them is 1.

Theorem 1.8 [8]

The order of an element in a direct product of a finite number of finite groups is the least common multiple of the orders of the components of the element. This can be expressed in the following form:

$$o(g_1, \dots, g_n) = \text{lcm}(o(g_1), \dots, o(g_n)).$$

Example 1.3

We determine the number of elements of order 15 in $\mathbb{Z}_{36} \times \mathbb{Z}_{90}$. Let $(a, b) \in \mathbb{Z}_{36} \times \mathbb{Z}_{90}$ such that $o(a, b) = \text{lcm}(o(a), o(b)) = 15$.

Clearly this requires that either $o(a) = 1$ and $o(b) = 15$, or $o(a) = 3$ and $o(b) = 5$, or $o(a) = 3$ and $o(b) = 15$.

Case 1 $o(a) = 1$ and $o(b) = 15$. According to Theorem 1.4, we have $\phi(1) = 1$ choices for a and $\phi(15) = 8$ choices for b . This gives $1 \times 8 = 8$ elements of order 15.

Case 2 $o(a) = 3$ and $o(b) = 5$. In this case there are $\phi(3) = 2$ choice for a and $\phi(5) = 4$ choices for b . Consequently, there are $2 \times 4 = 8$ elements of order 15.

Case 3 $o(a) = 3$ and $o(b) = 15$. In this case there are $\phi(3) = 2$ choices for a and $\phi(15) = 8$ choices for b . This gives $2 \times 8 = 16$ elements of order 15. Thus, $\mathbb{Z}_{36} \times \mathbb{Z}_{90}$ has $8 + 8 + 16 = 32$ elements of order 15.

Theorem 1.9 [13]

Let G be a group with two normal subgroups H and K , with the conditions that $H \cap K = \{e\}$ and $HK = G$, then $G \cong H \times K$.

Whereby HK is referred to as the internal direct product of H and K .

Definition 1.12 [19]

If p is a prime, then a finite group G is called a p -group if $|G| = p^n$ for some $n \geq 0$.

Theorem 1.10 [19]

If p is a prime, then every group G of order p^2 is Abelian.

Definition 1.13 [9]

If p is a prime and m is a positive integer such that $p^m \mid |G|$ and $p^{m+1} \nmid |G|$, then a subgroup of G that has order p^m is called a Sylow

p -subgroup of G .

Remark.

For a finite Abelian group G the Sylow p -subgroups are called the p -primary components of G .

Theorem 1.11 (Cauchy's Theorem) [8]

Let G be a finite Abelian group and let p be a prime that divides the order of G . Then G has an element of order p .

Definition 1.14 [6]

A group G is decomposable if it is isomorphic to a direct product of two proper nontrivial subgroups. Otherwise G is indecomposable.

Theorem 1.12 [6]

The finite indecomposable Abelian groups are exactly the cyclic groups with order a power of a prime.

Definition 1.15 [12]

A partially ordered set or poset is a set P together with a binary relation \leq such that the following conditions are satisfied for all $x, y, z \in P$:

- i. Reflexivity: $x \leq x$.
- ii. Antisymmetry: $x \leq y$ and $y \leq x$ imply that $x = y$.
- iii. Transitivity: $x \leq y$ and $y \leq z$ imply that $x \leq z$.

Example 1.4

If G is any finite group, the subset $L(G)$ of G consisting of all subgroups of G is partially ordered set with respect to set inclusion, and is called the subgroup lattice of G .

Definition 1.16 [12]

Let H be a subset of a poset P and $x \in P$. The element x is an upper bound of H if $h \leq x$ for all $h \in H$. An upper bound x of H is the least upper bound (supremum) of H if, for any upper bound y of H , we have $x \leq y$. This will be denoted as $x = \sup H$ or $x = \vee H$.

The concepts of lower bound and greatest lower bound (infimum) are similarly defined; whereby the latter is denoted by $\inf H$ or $\wedge H$.

Remark.

In the following text, the notation $x \wedge y = \inf \{x, y\}$, $x \vee y = \sup \{x, y\}$ will be adopted and \wedge will be referred to as the meet and \vee as the join.

Definition 1.17 [4]

Let $\langle L, \leq \rangle$ be a non-empty ordered set.

- i. If $x \vee y$ and $x \wedge y$ exist for all $x, y \in L$, then L is called a lattice.
- ii. If $\vee H$ and $\wedge H$ exist for all $H \subseteq L$, then L is called a complete lattice.

Examples 1.5

- i. Every finite lattice is complete.
- ii. Let G be a group. The set $\mathcal{L}(G) = \{H \mid H \triangleleft G\}$ forms a complete lattice, any subset of $\mathcal{L}(G)$ has a greatest lower bound in $\mathcal{L}(G)$ (the intersection of all its elements) and a least upper bound in $\mathcal{L}(G)$ (the join of all its elements).

Remark.

The lattice $\mathcal{L}(G)$ is called the normal subgroup lattice of G and its binary operations \vee, \wedge are defined by $H \wedge K = H \cap K$, $H \vee K = HK$ for all $H, K \in \mathcal{L}(G)$.

Definition 1.18 [12]

Let P be a poset. In that case, two elements x, y in P are comparable if $x \leq y$ or $y \leq x$. A subset H of P is a chain if any two elements in H are comparable. Similarly, H is an antichain if no two different elements of H are comparable.

Definition 1.19 [2]

If P_1 and P_2 are two posets and α is a map from P_1 to P_2 , then we say α is order preserving if $\alpha(a) \leq \alpha(b)$ holds in P_2 whenever $a \leq b$ holds in P_1 .

Theorem 1.13 [2]

Two lattices L_1 and L_2 are isomorphic iff there is a bijection α from L_1 to L_2 such that both α and α^{-1} are order preserving.

Definition 1.20 [4]

Let L be a lattice and $\emptyset \neq M \subseteq L$. Then M is called a sublattice of L if $x, y \in M$ implies $x \vee y \in M$ and $x \wedge y \in M$.

Examples 1.6

- i. Every chain in a lattice is a sublattice.
- ii. The normal subgroup lattice $\mathcal{L}(G)$ is sublattice of subgroup lattice $L(G)$ of a group G .
- iii. For $x, y \in L$, if $x \leq y$, the interval $[x, y] = \{z \in L \mid x \leq z \leq y\}$ is a sublattice of a lattice L .

Theorem 1.14 [12]

Every finite lattice is isomorphic to a sublattice of the subgroup lattice of some finite group.

Definition 1.21 [12]

A lattice L is called modular if for all $x, y, z \in L$ the modular law holds:

If $x \leq z$, then $(x \vee y) \wedge z = x \vee (y \wedge z)$.

Theorem 1.15 [12]

The lattice of normal subgroups of an arbitrary group and the subgroup lattice of an Abelian group are modular.

Chapter Two

Finite Abelian Groups

In this chapter, a complete classification of finite Abelian groups is given. In essence, all finite Abelian groups are built from cyclic groups, which may have prime power orders, or orders n_1, \dots, n_r where $n_i | n_{i+1}$, for all $i = \overline{1, r}$. In addition, also in this chapter, the automorphism groups of cyclic groups as examples of Abelian groups will also be determined.

2.1 The Structure of Abelian Groups

Theorem 2.1.1 [10]

Every finite Abelian group is a direct product of cyclic groups. Thus, for every finite Abelian group G

$$G \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \dots \times \mathbb{Z}_{n_r}, \text{ where}$$

- i. $n_j \geq 2$ for all $j \in \{1, 2, \dots, r\}$, and,
- ii. $n_i | n_{i+1}$, for $1 \leq i \leq r - 1$.

The n_i are referred to as the invariant factors of G , and the rank of G is defined as the number of invariant factors.

If $|G| = n_1 n_2 \dots n_r$, and m is a divisor of $|G|$, then there exist divisors m_i of n_i ($i = \overline{1, r}$) such that $m = m_1 \dots m_r$. Hence $\mathbb{Z}_{m_1} \times \dots \times \mathbb{Z}_{m_r}$ isomorphic to a subgroup of order m of G . This implies the corollary given below.

Corollary 2.1.1 [10]

Let G be an Abelian group and m a divisor of $|G|$. Then G contains a subgroup of order m .

Remark.

Theorem 2.1.1 gives an effective way of listing all finite Abelian groups of order n . It stipulates that all finite sequence of integers n_1, n_2, \dots, n_r must be found, such that

- i. $n_j \geq 2$ for all $j \in \{1, 2, \dots, r\}$
- ii. $n_i | n_{i+1}$, $1 \leq i \leq r - 1$, and
- iii. $n_1 n_2 \dots n_r = n$

It should be note here that finitely generated Abelian groups have a structure similar to that of finite Abelian groups. They are a direct product of finite Abelian groups and groups isomorphic to \mathbb{Z} .

Definition 2.1.1 [9]

If G is a finite Abelian group of order divisible by the prime p , then G_p is the set of all elements of G that have orders that are powers of p .

Example 2.1.1

Consider the additive group $G = \mathbb{Z}_6$. The order of \mathbb{Z}_6 is 6, which is divisible by the prime numbers 2 and 3. In this group:

Each of $[1]$, and $[5]$ has order 6.

Each of $[2]$ and $[4]$ has order 3.

$[3]$ has order 2.

$[0]$ has order 1.

For $p = 2$ or $p = 3$, the subgroups G_p are given by

$$G_2 = \{[0], [3]\},$$

$$G_3 = \{[0], [2], [4]\}.$$

Theorem 2.1.2 [9]

If G is a finite Abelian group and p is a prime, such that $p \mid |G|$, then G_p is a Sylow p -subgroup.

Theorem 2.1.3 (Primary Decomposition Theorem) [5]

Let G be an Abelian group of order $n > 1$ and let the unique factorization of n into distinct prime powers be given as

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}.$$

Then

- i. $G \cong \prod_{i=1}^k G_{p_i}$, where $|G_{p_i}| = p_i^{\alpha_i}$, for all $i = \overline{1, k}$.
- ii. For each $G_p \in \{G_{p_1}, G_{p_2}, \dots, G_{p_k}\}$ with $|G_p| = p^\alpha$,

$$G_p \cong \mathbb{Z}_{p^{\beta_1}} \times \mathbb{Z}_{p^{\beta_2}} \times \dots \times \mathbb{Z}_{p^{\beta_t}}$$

with $1 \leq \beta_1 \leq \beta_2 \leq \dots \leq \beta_t$ and $\beta_1 + \beta_2 + \dots + \beta_t = \alpha$.

It should be noted here that the decomposition in (i) and (ii) is unique.

The last theorem yields the following conclusions:

- i. Every finite Abelian group G can be expressed as a direct product of its p -primary components.
- ii. The number of (distinct, i.e. nonisomorphic) Abelian groups of order p^α is equal the number of partitions of α .

In particular, if $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, and q_i is the number of partitions of α_i , then the number of nonisomorphic Abelian groups of order n is

$$\lambda(n) = q_1 q_2 \dots q_k.$$

Example 2.1.2

If $n = 1800 = 2^3 3^2 5^2$, then there are exactly 12 Abelian groups of this order, as presented in the table below:

Order of p^α	Partitions of α	Abelian groups
2^3	3, 1, 2, 1, 1, 1	$\mathbb{Z}_8, \mathbb{Z}_2 \times \mathbb{Z}_4, \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$
3^2	2, 1, 1	$\mathbb{Z}_9, \mathbb{Z}_3 \times \mathbb{Z}_3$
5^2	2, 1, 1	$\mathbb{Z}_{25}, \mathbb{Z}_5 \times \mathbb{Z}_5$

All Abelian groups of order 1800 can be obtained by taking one Abelian group from each of the three lists above and taking their direct product. Doing this in all possible combinations yields ways gives all isomorphism types:

$\mathbb{Z}_8 \times \mathbb{Z}_9 \times \mathbb{Z}_{25}$	$\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{25}$
$\mathbb{Z}_8 \times \mathbb{Z}_9 \times \mathbb{Z}_5 \times \mathbb{Z}_5$	$\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_5$
$\mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{25}$	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_{25}$
$\mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_5$	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_5 \times \mathbb{Z}_5$
$\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_9 \times \mathbb{Z}_{25}$	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{25}$
$\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_9 \times \mathbb{Z}_5 \times \mathbb{Z}_5$	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_5$

Every Abelian group of order 1800 is isomorphic to only one of the previous groups and no two of these groups are isomorphic.

In order to find the Abelian group G that is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{25}$, we first must find the invariant factors n_i satisfying the divisibility condition $n_i | n_{i+1}$ by regrouping, as follows:

$p = 2$	$p = 3$	$p = 5$
2	1	1
2	3	1
2	3	25

Hence, $n_1 = 2.1.1$, $n_2 = 2.3.1$, $n_3 = 2.3.25$ and $G \cong \mathbb{Z}_2 \times \mathbb{Z}_6 \times \mathbb{Z}_{150}$.

Theorem 2.1.4 (Fundamental Theorem of Finite Abelian Groups)

Every finite Abelian group G is a direct product of cyclic groups of the form

$$\mathbb{Z}_{p_1^{\alpha_1}} \times \mathbb{Z}_{p_2^{\alpha_2}} \times \dots \times \mathbb{Z}_{p_k^{\alpha_k}}$$

where the p_i 's need not be distinct primes and prime powers are uniquely determined by G . [18]

Example 2.1.3

Determine the isomorphism type of the Abelian group $U(40)$.

Solution:

Since $U(40) = \{ 1, 3, 7, 9, 11, 13, 17, 19, 21, 23, 27, 29, 31, 33, 37, 39 \}$ is of order 16, it isomorphic to one of the following

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$$

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4$$

$$\mathbb{Z}_4 \times \mathbb{Z}_4$$

$$\mathbb{Z}_2 \times \mathbb{Z}_8$$

$$\mathbb{Z}_{16}.$$

To identify the solution, we must first determine the orders of all elements of Abelian group $U(40)$:

Element	1	3	7	9	11	13	17	19	21	23	27	29	31	33	37	39
Order	1	4	4	2	2	4	4	2	2	4	4	2	2	4	4	2

Based the table of orders, we can instantly rule out all but $\mathbb{Z}_4 \times \mathbb{Z}_4$ and $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4$ as possibilities. Notice that in $\mathbb{Z}_4 \times \mathbb{Z}_4$, the subgroups $\mathbb{Z}_4 \times \{0\}$ and $\{0\} \times \mathbb{Z}_4$ have intersection $\{(0, 0)\}$. However, if we list all the cyclic subgroups of order 4 in $U(40)$, namely $\langle 3 \rangle = \{3, 9, 27, 1\}$, $\langle 7 \rangle = \{7, 9, 23, 1\}$, $\langle 13 \rangle = \{13, 9, 37, 1\}$, and $\langle 17 \rangle = \{17, 9, 33, 1\}$ it becomes apparent that none intersect trivially. Thus, $U(40) \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4$.

2.2 Automorphisms of Cyclic Groups [10]

As examples of Abelian groups, in this section, the automorphism groups of cyclic groups are determined.

Let G be a group and let $\text{Aut}(G)$ denote the set of all automorphisms of G .

This set forms a group under the operation of function composition.

For an Abelian group G and every $k \in \mathbb{Z}$ the mapping

$$\alpha_k: G \rightarrow G \text{ such that } x \mapsto x^k$$

is an endomorphism with

$$\text{Ker } \alpha_k = \{x \in G \mid x^k = e\},$$

Thus, $\text{Ker } \alpha_k$ contains all elements of G , whose orders divide k .

Theorem 2.2.1

α_k is an automorphism of the Abelian group G , if and only if $(k, |G|) = 1$.

Proof.

If $(k, |G|) = 1$, then $\text{Ker } \alpha_k = \{e\}$. Conversely, if $(k, |G|) \neq 1$, then there exists a common prime divisor p of k and $|G|$. Now, according to Theorem 2.1.3, the p -subgroup G_p is nontrivial, and there exists a subgroup of order p in G . This subgroup is contained in $\text{Ker } \alpha_k$.

Definition 2.2.1

A subgroup H of a group G is a characteristic subgroup of G , if $H^\alpha = H$, for all $\alpha \in \text{Aut}(G)$.

Evidently, characteristic subgroups are normal in G . Moreover, $\{e\}$ and G are characteristic subgroups of G

Theorem 2.2.2

Let G be an Abelian group. Then G_p is a characteristic p -subgroup of order $|G|_p$, where $|G|_p$ is the greatest p -power dividing $|G|$.

Theorem 2.2.3

Let $G = G_1 \times \dots \times G_n$. If the factors G_1, \dots, G_n are characteristic subgroups of G , then $\text{Aut } G \cong \text{Aut } G_1 \times \dots \times \text{Aut } G_n$.

It is well known that any finite Abelian group G may be expressed as the direct product of its Sylow subgroups:

$$G = G_{p_1} \times G_{p_2} \times \dots \times G_{p_n}$$

Since the Sylow subgroups of an Abelian group G are characteristic, then

$$\text{Aut } G \cong \prod_{i=1}^n \text{Aut } G_{p_i}$$

Hence, it suffices to determine the automorphism group of cyclic p -groups.

If G is a cyclic p -group of order $p^n > 1$, then $|\text{Aut } G|$ is the number of integers k such that $1 \leq k < p^n$ and $(k, p) = 1$. Thus

$$|\text{Aut } G| = p^{n-1}(p - 1).$$

In particular, $|\text{Aut } G| = p - 1$ if $|G| = p$.

Definition 2.2.2 [18]

Let p be a prime number. An Abelian group G is said to be an elementary Abelian p -group if every element x of G satisfies $x^p = e$.

Proposition 2.2.1 [5]

- i. If p is an odd prime and $n \in \mathbb{N}^*$, then the automorphism group of the cyclic group of order p is cyclic of order $p - 1$. More generally, the automorphism group of the cyclic group of order p^n is cyclic of order $p^{n-1}(p - 1)$.
- ii. For all $n \geq 3$, the automorphism group of the cyclic group of order 2^n is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_{2^{n-2}}$. In particular is not cyclic but has a cyclic subgroup of index 2.
- iii. Let p be a prime and let G be an elementary Abelian p -group. If $|G| = p^n$, then G is an n -dimensional vector space V over the field \mathbb{Z}_p . The subgroups of G correspond to the subspaces of V and the automorphisms of G to the automorphisms of V .

Remark.

The Gaussian binomial coefficient $\begin{bmatrix} n \\ k \end{bmatrix}_p$ gives the number of subspace of dimension k in a vector space of dimension n over the field of order p .

The number $\begin{bmatrix} n \\ k \end{bmatrix}_p$ is defined as

$$\begin{cases} \prod_{i=1}^k \frac{p^{n-k+i}-1}{p^i-1}, & \text{if } 1 \leq k \leq n-1 \\ 1, & \text{if } k=0 \text{ or } n \\ 0, & \text{otherwise} \end{cases}$$

Chapter Three

Counting Subgroups of Finite Abelian Groups

The process of finding the number of subgroups of a finite Abelian group, or drawing the subgroup lattice of a given finite Abelian p -group, is a difficult task. In this chapter, different methods that partially solve these two problems are introduced.

In Section 3.1, some simpler methods of [11] are outlined, and are used to calculate the number of subgroups of a finite Abelian group of orders below thirty. Similarly, Section 3.2 included an expression that gives the total number of subgroups of a finite Abelian p -group of rank two.

In the sections below, a different formula, concerning the number of elements of a fixed order and the number of cyclic subgroups of a finite Abelian group, is presented by using number-theoretic arguments in [17].

3.1 The Total Number of Subgroups of a Finite Abelian Group Whose Orders Below Thirty:

If G is a finite Abelian group of order $p^n, n \geq 1$, then it is well known that G can be decomposable into a direct product of indecomposable cyclic groups:

$$G \cong \mathbb{Z}_p^{n_1} \times \mathbb{Z}_p^{n_2} \times \dots \times \mathbb{Z}_p^{n_k}, \text{ where}$$

p is a prime, $1 \leq n_1 \leq n_2 \leq \dots \leq n_k$ and $n_1 + n_2 + \dots + n_k = n$. In this case the Abelian group G is said to be of type $\langle n_1, n_2, \dots, n_k \rangle$.

The following simpler methods will be useful in counting the number of all subgroups of a finite Abelian group in Table 1, and since a finite Abelian group of prime order contains no proper subgroups, these groups are not included in Table 1.

1. The number of all subgroups of a cyclic group of order p^n , $n \geq 1$ is $n + 1$.
2. For $n \geq 1$, the number of all subgroups of an elementary Abelian p -group \mathbb{Z}_p^n , type $\langle 1, 1, \dots, 1 \rangle$ is

$$2 + \sum_{k=1}^{n-1} \frac{(p^n-1)(p^{n-1}-1) \dots (p^{n-k+1}-1)}{(p^k-1)(p^{k-1}-1) \dots (p-1)}$$

Proof.

Since \mathbb{Z}_p^n is an n -dimensional vector space over \mathbb{Z}_p , and $\begin{bmatrix} n \\ k \end{bmatrix}_p$ gives the number of all subgroups of dimension (rank) k , then $\sum_{k=0}^n \begin{bmatrix} n \\ k \end{bmatrix}_p$ gives the total number of subgroups, as follows

$$\begin{aligned} \sum_{k=0}^n \begin{bmatrix} n \\ k \end{bmatrix}_p &= \begin{bmatrix} n \\ 0 \end{bmatrix}_p + \begin{bmatrix} n \\ 1 \end{bmatrix}_p + \begin{bmatrix} n \\ 2 \end{bmatrix}_p + \dots + \begin{bmatrix} n \\ n-1 \end{bmatrix}_p + \begin{bmatrix} n \\ n \end{bmatrix}_p \\ &= 1 + \frac{p^n-1}{p-1} + \frac{(p^n-1)(p^{n-1}-1)}{(p-1)(p^2-1)} + \dots + \frac{p^n-1}{p-1} + 1 \\ &= 2 + \sum_{k=1}^{n-1} \frac{(p^n-1)(p^{n-1}-1) \dots (p^{n-k+1}-1)}{(p^k-1)(p^{k-1}-1) \dots (p-1)}. \end{aligned}$$

Here, $\sum_{k=0}^n \begin{bmatrix} n \\ k \end{bmatrix}_p$ is referred to as Galois numbers and is denoted by $G_{n,p}$.

3. For $n \geq 2$, the number of all subgroups of Abelian group of order p^n , type $\langle 1, n - 1 \rangle$ is $(n - 1)(p + 1) + 2$.
4. The Abelian group of order p^4 , type $\langle 2, 2 \rangle$ contains exactly $p^2 + 3p + 5$ subgroups.

Remark.

The proof of statement (3) follows directly from Theorem 4.2.1, when $\alpha_1 = 1$ and $\alpha_2 = n - 1$. Moreover, statement (4) is proven true by taking $\alpha_1 = \alpha_2 = 2$.

5. Let G be an Abelian group of order $p_1^{n_1} p_2^{n_2} \dots p_k^{n_k}$, then the number of all its subgroups $N(G)$ is

$$N(G) = \prod_{i=1}^k N(G_{p_i}),$$

where $N(G_{p_i})$ is the total number of the subgroups of p_i -primary components of G .

Example 3.1.1

The number of all subgroups of a finite Abelian group $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_6$ is 32 since $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$. Then

$$\begin{aligned} N(\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_6) &= N(\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3) \\ &= N(\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2) N(\mathbb{Z}_3) \\ &= 16 \times 2 \\ &= 32. \end{aligned}$$

Remark.

The number $s(m,n)$ of all subgroups of a finite Abelian group $\mathbb{Z}_m \times \mathbb{Z}_n$ is given by

$$s(m,n) = \sum_{d_1|m, d_2|n} \gcd(d_1, d_2) \quad (m, n \geq 1).$$

For example, if $m = 3$, $n = 6$, then the number of all subgroups of the Abelian group $\mathbb{Z}_3 \times \mathbb{Z}_6$ is

$$s(m,n) = \sum_{d_1|3, d_2|6} \gcd(d_1, d_2) = \gcd(1, 1) + \gcd(1, 2) + \gcd(1, 3) + \gcd(1, 6) + \gcd(3, 1) + \gcd(3, 2) + \gcd(3, 3) + \gcd(3, 6) = 12.$$

Now, if $n \geq 1$, we define $\lambda(n)$ as the number of non-isomorphic Abelian groups of order n . Table 1 provides the classification and the number of subgroups of all Abelian groups of order < 30 .

Table (1)

Order n	$\lambda(n)$	Abelian groups of the same order	Number of their subgroups
4	2	$\mathbb{Z}_4, \mathbb{Z}_2 \times \mathbb{Z}_2$	3, 5
6	1	\mathbb{Z}_6	4
8	3	$\mathbb{Z}_8, \mathbb{Z}_2 \times \mathbb{Z}_4, \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	4, 8, 16
9	2	$\mathbb{Z}_9, \mathbb{Z}_3 \times \mathbb{Z}_3$	3, 6
10	1	\mathbb{Z}_{10}	4
12	2	$\mathbb{Z}_{12}, \mathbb{Z}_2 \times \mathbb{Z}_6$	6, 10
14	1	\mathbb{Z}_{14}	4
15	1	\mathbb{Z}_{15}	4
16	5	$\mathbb{Z}_{16}, \mathbb{Z}_2 \times \mathbb{Z}_8, \mathbb{Z}_4 \times \mathbb{Z}_4, \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4, \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	5, 11, 15, 27, 67
18	2	$\mathbb{Z}_{18}, \mathbb{Z}_3 \times \mathbb{Z}_6$	6, 12
20	2	$\mathbb{Z}_{20}, \mathbb{Z}_2 \times \mathbb{Z}_{10}$	6, 10

21	1	\mathbb{Z}_{21}	4
22	1	\mathbb{Z}_{22}	4
24	3	$\mathbb{Z}_{24}, \mathbb{Z}_2 \times \mathbb{Z}_{12}, \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_6$	8, 16, 32
25	2	$\mathbb{Z}_{25}, \mathbb{Z}_5 \times \mathbb{Z}_5$	3, 8
26	1	\mathbb{Z}_{26}	4
27	3	$\mathbb{Z}_{27}, \mathbb{Z}_3 \times \mathbb{Z}_9, \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$	4, 10, 28
28	2	$\mathbb{Z}_{28}, \mathbb{Z}_2 \times \mathbb{Z}_{14}$	6, 10

3.2 The Total Number of Subgroups of a Finite Abelian p -Group

The aim of this section is to determine the subgroups that add to the direct product of the subgroup lattice of the direct components. In addition, the expression providing the total number of subgroups of a finite Abelian group whose p -ranks do not exceed two is also introduced.

If $G = H \times K$, then in general $\mathcal{L}(G) \not\cong \mathcal{L}(H) \times \mathcal{L}(K)$. Therefore, it is possible to construct $\mathcal{L}(G)$ of $\mathcal{L}(H)$, $\mathcal{L}(K)$ and all isomorphisms between intervals in the subgroup lattice. Moreover, the term "interval" is used as follows: if H, K are subgroups of G , the interval $[H, K] = \{U \in \mathcal{L}(G) \mid H \leq U \leq K\}$.

Definition 3.2.1 [12]

Let $G = H \times K$. A subgroup D of G is called a diagonal in G (with respect to H and K) if

- i. $DH = G = DK$, and
- ii. $D \cap H = \{e\} = D \cap K$.

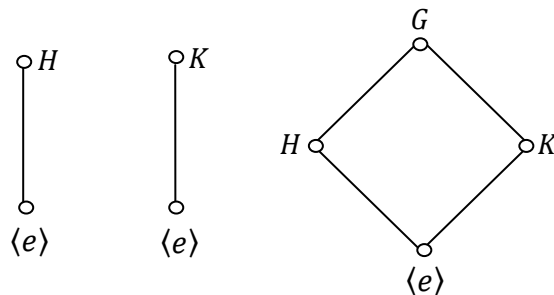
Theorem 3.2.1 [12]

Let $H, K \leq G$ and $G = H \times K$. If $\varphi: H \rightarrow K$ is an isomorphism, then $D(\varphi) = D(H, \varphi) = \{xx^\varphi | x \in H\}$ is a diagonal in G (with respect to H and K).

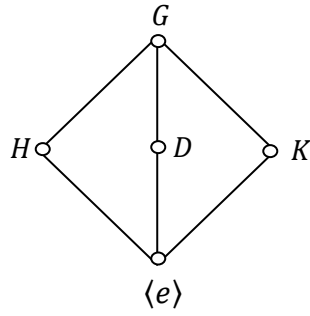
Conversely, if D is a diagonal in G (with respect to H and K), then there exists a unique isomorphism $\varphi: H \rightarrow K$ such that $D = D(\varphi)$. Thus there is a bijection between diagonals (with respect to H and K) and isomorphism of H and K , and between diagonals and automorphisms of H (if $H \cong K$).

Examples 3.2.1 [3]

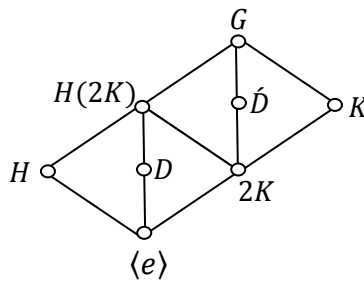
1. Consider the Klein group $G = \mathbb{Z}_2 \times \mathbb{Z}_2 = \{e, a, b, ab \mid a^2 = b^2 = e\}$. Each $\mathcal{L}(\mathbb{Z}_2)$ is a chain with two elements and the direct product of these two chains is the four element lattice, as shown below.



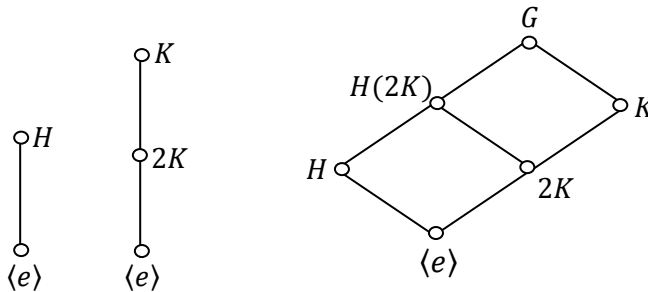
Based on Theorem 3.2.1, we have to add as many diagonals as there are isomorphisms $\mathbb{Z}_2 \rightarrow \mathbb{Z}_2$ (i.e. $H \rightarrow K$). From $H = \{e, a\}$ to $K = \{e, b\}$ there is only one isomorphism, so only one diagonal (namely $D(\varphi) = D(H, \varphi) = \{e, ab\}$) has to be added to the direct product. Hence we have $2 \times 2 = 4$ subgroups in the direct product +1 diagonal corresponding to the isomorphism $\mathbb{Z}_2 \rightarrow \mathbb{Z}_2$. Thus, the total number of subgroups is $4 + 1 = 5$, and G has the "diamond" as subgroup lattice



2. The group $G = \mathbb{Z}_2 \times \mathbb{Z}_4 = \{e, a, b, ab, b^2, ab^2, b^3, ab^3 \mid a^2 = b^4 = e\}$ has the subgroup lattice shown below:

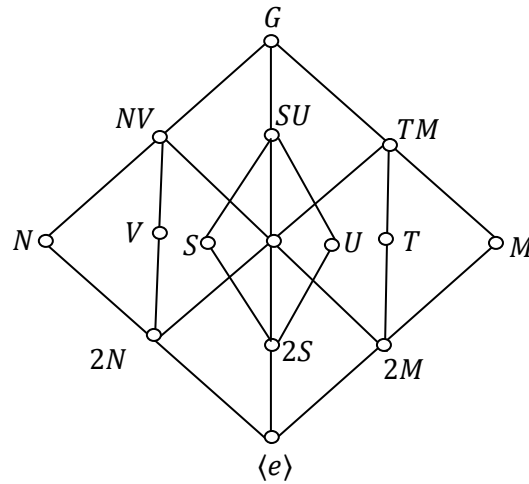


Indeed, to the direct product of chains

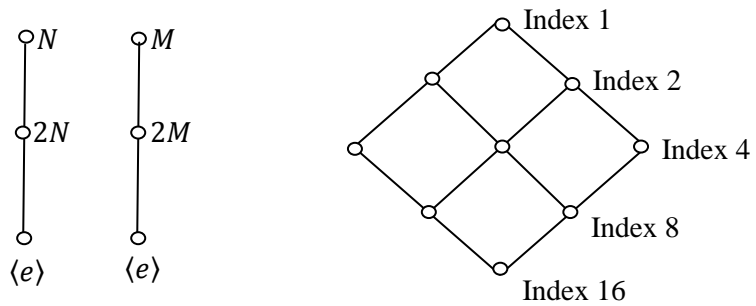


we have to add only two diagonals, D corresponding to the isomorphism $[e, H] \rightarrow [e, 2K]$ and D' to the isomorphism $[e, H] \rightarrow [2K, K]$. Thus, we have $2 \times 3 = 6$ subgroups in the direct product + 2 diagonals corresponding two isomorphisms, equal to 8 subgroups, as previously noted.

3. The group $G = \mathbb{Z}_4 \times \mathbb{Z}_4 = \langle a, b \mid a^4 = b^4 = e \rangle$ with cyclic subgroups $N = \langle a \rangle = \langle a^3 \rangle$, $M = \langle b \rangle = \langle b^3 \rangle$ has the subgroup lattice



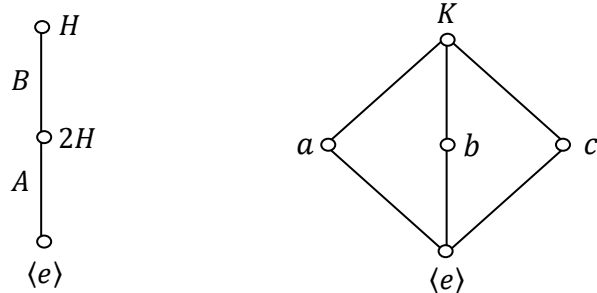
Each $\mathcal{L}(\mathbb{Z}_4)$ is a chain with three elements and the direct product of these two chains is the nine element lattice



Now, we have two types of isomorphism: four isomorphisms $\mathbb{Z}_2 \rightarrow \mathbb{Z}_2$ $[e, 2N] \rightarrow [e, 2M]$, $[e, 2N] \rightarrow [2M, M]$, $[2N, N] \rightarrow [e, 2M]$, and $[2N, N] \rightarrow [2M, M]$ as well as two isomorphisms $\mathbb{Z}_4 \rightarrow \mathbb{Z}_4$ ($[e, N] \rightarrow [e, M]$ - \mathbb{Z}_4 has two automorphisms). Thus, we add 6 diagonals $2S, T, V, SU, S,$ and U for a total of 15 subgroups.

4. Let us now consider the 2-group $G = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4$.

First, we take $H = \mathbb{Z}_4$ with 3-element chain subgroup lattice, and $K = \mathbb{Z}_2 \times \mathbb{Z}_2$ with the 'diamond' subgroup lattices, as follows



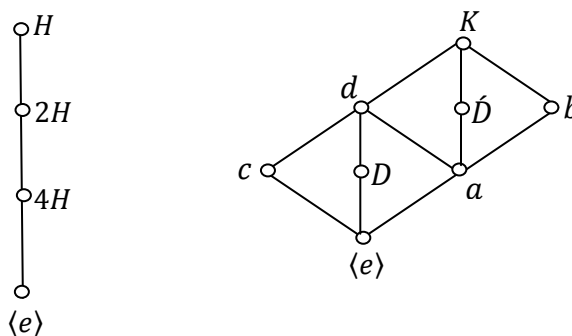
Hence we have $3 \times 5 = 15$ subgroups in the direct product, and we must add 6 diagonals corresponding to 6 isomorphisms from $A = [e, 2H]$ to each 1-segments on the 'diamond' and other 6 isomorphisms from $B = [2H, H]$ to the same-segments. Consequently, the total number of subgroups is $15 + 6 + 6 = 27$.

Remark.

There is no isomorphism from the interval (chain) $[e, H]$ to some 3-element chains in the "diamond"(namely $[e, a, K]$, $[e, b, K]$ or $[e, c, K]$) because none of these is an interval in the subgroup lattice $\mathcal{L}(K)$.

5. $G = \mathbb{Z}_8 \times (\mathbb{Z}_2 \times \mathbb{Z}_4)$.

First, we have $4 \times 8 = 32$ subgroups in the direct product + 3×11 diagonals corresponding to all isomorphism between 1-segments and



$2 \times 2 \times 4 = 16$ more diagonals to be added corresponding to all isomorphism between 2-segments (2 number of 2-segments in $\mathcal{L}(\mathbb{Z}_4)$, $|\text{Aut}(\mathbb{Z}_4)| = 2(2 - 1) = 2$, and 4 number of 2-segments in $\mathcal{L}(\mathbb{Z}_2 \times \mathbb{Z}_4)$), for a total of $32 + 33 + 16 = 81$ subgroups.

6. $G = \mathbb{Z}_4 \times (\mathbb{Z}_4 \times \mathbb{Z}_4)$

In this case, we take $H = \mathbb{Z}_4$ with 3-element chain subgroup lattice, and $K = \mathbb{Z}_4 \times \mathbb{Z}_4$ with the subgroup lattice in Example 3.

Therefore, we have $3 \times 15 = 45$ subgroups in the direct product, $2 \times 24 = 48$ diagonals (between 1-segments) corresponding to all the $\mathbb{Z}_2 \rightarrow \mathbb{Z}_2$ isomorphisms and $2 \times 18 = 36$ diagonals (between 2-segments) corresponding to all the $\mathbb{Z}_4 \rightarrow \mathbb{Z}_4$ isomorphisms. The total in this example is $45 + 48 + 36 = 129$ subgroups.

The rank two formula

In this section, proof of the formula giving the total number of subgroups for a finite Abelian p -group of rank two will be given.

First, set $G = \mathbb{Z}_{p^t} \times \mathbb{Z}_{p^k}$ for arbitrary positive integers t and k .

Here, we have the direct product of chains of length t and k , respectively. In other words, we have $(t + 1)(k + 1)$ subgroups. Next, we determine the diagonals corresponding to the automorphisms $\mathbb{Z}_p \rightarrow \mathbb{Z}_p$, which give $p - 1$ diagonals for each pair of 1-segments, i.e., $tk(p - 1)$.

Further, the diagonals corresponding to the automorphisms $\mathbb{Z}_{p^2} \rightarrow \mathbb{Z}_{p^2}$, give $p(p - 1)$ diagonals for each pair of 2-segments.

Hence, $(t - 1)(k - 1)p(p - 1)$ diagonals have to be added.

We must continue this process until we exhaust the adjacent $\min(t, k)$ -length segments, which is obviously the chain $\mathcal{L}(H)$ or the chain $\mathcal{L}(K)$.

This chain produces $|k - t| + 1$ pairs of chains of length $\min(t, k)$, each generating $p^{\min(t,k)-1}(p - 1)$ diagonals.

Therefore, the total number of subgroups is

$$(t + 1)(k + 1) + tk(p - 1) + (t - 1)(k - 1)p(p - 1) + \dots + 2(|k - t| + 2)p^{\min(t,k)-2}(p - 1) + (|k - t| + 1)p^{\min(t,k)-1}(p - 1).$$

Finite Elementary Abelian p -Groups

A finite elementary Abelian p -group has a direct decomposition of type

$$\mathbb{Z}_p^n = \mathbb{Z}_p \times \mathbb{Z}_p \times \dots \times \mathbb{Z}_p,$$

where p is a prime and $n \in \mathbb{N}^*$.

This is denoted by $N(\mathbb{Z}_p^n)$ for the total number of subgroups of \mathbb{Z}_p^n and by $n(1\text{-seg}(\mathcal{L}(\mathbb{Z}_p^n)))$ for the number of 1-segments of the subgroup lattice $\mathcal{L}(\mathbb{Z}_p^n)$.

Using $|\text{Aut}(\mathbb{Z}_p)| = p - 1$ and $\mathbb{Z}_p^n = \mathbb{Z}_p \times \mathbb{Z}_p^{n-1}$, whereby $\mathcal{L}(\mathbb{Z}_p)$ is a chain with two elements, by counting the subgroups in the direct product and the diagonals, respectively, we obtain

$$N(\mathbb{Z}_p^n) = 2N(\mathbb{Z}_p^{n-1}) + (p - 1)n(1\text{-seg}(\mathcal{L}(\mathbb{Z}_p^{n-1}))).$$

Consequence

$$\begin{aligned} n(1\text{-seg}(\mathcal{L}(\mathbb{Z}_p^n))) &= \frac{1}{p-1} [N(\mathbb{Z}_p^{n+1}) - 2N(\mathbb{Z}_p^n)] \\ &= \frac{1}{p-1} [G_{n+1,p} - 2G_{n,p}] \end{aligned}$$

$$= \frac{p^n - 1}{p - 1} G_{n-1,p}.$$

Where $G_{n,p} = \sum_{k=0}^n \begin{bmatrix} n \\ k \end{bmatrix}_p$, and for all $n \in \mathbb{N}$

$$G_{0,p} = 1, G_{1,p} = 2,$$

$$G_{n+1,p} = 2G_{n,p} + (p^n - 1)G_{n-1,p}.$$

Remark.

Each finite Abelian p -group G can be written as $\mathbb{Z}_{p^l} \times \hat{G}$ where \hat{G} is a finite direct product of finite cocyclic groups of order greater or equal to p^l . If we know how to count the 1-segements, 2-segements, ..., the l -segements in $\mathcal{L}(\hat{G})$, we can calculate the total number of subgroups of G as follows:

$$N(\mathbb{Z}_{p^l} \times \hat{G}) = N(\mathbb{Z}_{p^l}) \times N(\hat{G}) + l(p - 1)n(1\text{-seg}) + (l - 1)p(p - 1)n(2\text{-seg}) + (l - 2)p^2(p - 1)n(3\text{-seg}) + \dots + 2p^{l-2}(p - 1)n((l - 1)\text{-seg}) + p^{l-1}(p - 1)n(l\text{-seg}).$$

In the expression above, $n(u\text{-seg})$ denotes the number of u -segements in $\mathcal{L}(\hat{G})$.

For example, let G be an Abelian p -group $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_8$, then G can be written as $\mathbb{Z}_8 \times (\mathbb{Z}_2 \times \mathbb{Z}_4)$, where $\hat{G} = \mathbb{Z}_2 \times \mathbb{Z}_4$, $l = 3$, $p = 2$. Moreover, $n(1\text{-seg})$ and $n(2\text{-seg})$ in $\mathcal{L}(\mathbb{Z}_2 \times \mathbb{Z}_4)$ is 11 and 4, respectively. Thus, the total number of subgroups of G is

$$N(\mathbb{Z}_8 \times (\mathbb{Z}_2 \times \mathbb{Z}_4)) = (4 \times 8) + 3 \times 11 + 2 \times 2 \times 4 = 81.$$

3.3 The Number of Cyclic Subgroups of a Finite Abelian Group

This section presents several theoretical arguments and mathematical expressions concerning the number of elements of a fixed order and the number of cyclic subgroups of a direct product of several finite cyclic groups.

3.3.1 The Number of Cyclic Subgroups of $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \dots \times \mathbb{Z}_{n_r}$

In this subsection, we denote by $c(n_1, \dots, n_r)$ for the number of all cyclic subgroups of the direct product $\mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_r}$, where r, n_1, \dots, n_r are arbitrary positive integers.

Theorem 3.3.1 [17]

For any $n_1, \dots, n_r \geq 1$, $c(n_1, \dots, n_r)$ is given by the expression

$$c(n_1, \dots, n_r) = \sum_{d_1 | n_1, \dots, d_r | n_r} \frac{\phi(d_1) \dots \phi(d_r)}{\phi(\text{lcm}(d_1, \dots, d_r))} \quad (3.1)$$

In particular, the number of cyclic subgroups of $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$

$$c(n_1, n_2) = \sum_{d_1 | n_1, d_2 | n_2} \phi(\text{gcd}(d_1, d_2)) \quad (3.2)$$

Remark.

The expression (3.2) follows from (3.1) by using the identity

$$\phi(m)\phi(n) = \phi(\text{gcd}(m, n))\phi(\text{lcm}(m, n)) \quad (m, n \geq 1).$$

The following expression relates to the number $o_\delta(n_1, \dots, n_r)$ of elements of order δ in $\mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_r}$. Let $n = \text{lcm}(n_1, \dots, n_r)$, where the

order of every element of the direct product is obviously a divisor of n . Let μ denote the Möbius function, and define it as

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n \text{ is not square free} \\ (-1)^r & \text{if } n = p_1 p_2 \dots p_r \end{cases}$$

Theorem 3.3.2 [17]

For every $n_1, \dots, n_r \geq 1$ and every $\delta | n$,

$$o_\delta(n_1, \dots, n_r) = \sum_{e|\delta} \gcd(e, n_1) \cdots \gcd(e, n_r) \mu(\delta/e) \tag{3.3}$$

$$= \sum_{\substack{d_1 | n_1, \dots, d_r | n_r \\ \text{lcm}(d_1, \dots, d_r) = \delta}} \phi(d_1) \cdots \phi(d_r) \tag{3.4}$$

Let $c_\delta(n_1, \dots, n_r)$ denote the number of cyclic subgroups of order δ ($\delta | n$) of the group $\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_r}$. Since a cyclic subgroup of order δ has $\phi(\delta)$ generators,

$$c_\delta(n_1, \dots, n_r) = \frac{o_\delta(n_1, \dots, n_r)}{\phi(\delta)} \tag{3.5}$$

Now (3.1) follows immediately from (3.4) and (3.5) by

$$c(n_1, \dots, n_r) = \sum_{\delta | n} c_\delta(n_1, \dots, n_r) \tag{3.6}$$

Example 3.3.1

Let us compute the number of all cyclic subgroups of a finite Abelian group $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$. For every $\delta | \text{lcm}(2, 2, 3)$, there exist cyclic subgroups of order δ . Hence, there are cyclic subgroups of orders

1, 2, 3, 6, and the number of cyclic subgroups corresponding to each of these orders are:

$$\begin{aligned} o_1(2,2,3) &= \phi(d_1)\phi(d_2)\phi(d_3) \\ &= \sum_{\substack{d_1|2, d_2|2, d_3|3 \\ \text{lcm}(d_1, d_2, d_3)=1}} \phi(1)\phi(1)\phi(1) = 1 \end{aligned}$$

$$c_1(2, 2, 3) = \frac{o_1(2,2,3)}{\phi(1)} = 1.$$

$$\begin{aligned} o_2(2,2,3) &= \sum_{\substack{d_1|2, d_2|2, d_3|3 \\ \text{lcm}(d_1, d_2, d_3)=2}} \phi(d_1)\phi(d_2)\phi(d_3) \\ &= \phi(1)\phi(2)\phi(1) + \phi(2)\phi(1)\phi(1) + \phi(2)\phi(2)\phi(1) = 3 \end{aligned}$$

$$c_2(2, 2, 3) = \frac{o_2(2,2,3)}{\phi(2)} = 3.$$

$$\begin{aligned} o_3(2,2,3) &= \sum_{\substack{d_1|2, d_2|2, d_3|3 \\ \text{lcm}(d_1, d_2, d_3)=3}} \phi(d_1)\phi(d_2)\phi(d_3) \\ &= \phi(1)\phi(1)\phi(3) = 2 \end{aligned}$$

$$c_3(2, 2, 3) = \frac{o_3(2,2,3)}{\phi(3)} = 1.$$

$$\begin{aligned} o_6(2,2,3) &= \sum_{\substack{d_1|2, d_2|2, d_3|3 \\ \text{lcm}(d_1, d_2, d_3)=6}} \phi(d_1)\phi(d_2)\phi(d_3) \\ &= \phi(1)\phi(2)\phi(3) + \phi(2)\phi(1)\phi(3) + \phi(2)\phi(2)\phi(3) = 6 \end{aligned}$$

$$c_6(2, 2, 3) = \frac{o_6(2,2,3)}{\phi(6)} = 3.$$

Consequently, the total number of all cyclic subgroups of a finite Abelian group $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$ is:

$$c(2, 2, 3) = c_1(2, 2, 3) + c_2(2, 2, 3) + c_3(2, 2, 3) + c_6(2, 2, 3) = 8.$$

Corollary 3.3.1 [17]

For every prime p and every $a_1, \dots, a_r \geq 1, 1 \leq v \leq \max(a_1, \dots, a_r)$,

$$c_{p^v}(p^{a_1}, \dots, p^{a_r}) = \frac{1}{p^{v-1}(p-1)} \left(p^{\min(v, a_1) + \dots + \min(v, a_r)} - p^{\min(v-1, a_1) + \dots + \min(v-1, a_r)} \right).$$

Example 3.3.2

Let $\mathbb{Z}_p \times \mathbb{Z}_{p^2}$ be a finite Abelian p -group of type $\langle 1, 2 \rangle$. Then $a_1 = 1$, $a_2 = 2$. Hence, the number of all cyclic subgroups of order p is

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

Alternative Method:

This method allows us to determine the number of cyclic subgroups of order p in $\mathbb{Z}_p \times \mathbb{Z}_{p^2}$ by counting the number of elements using the fact that $|(a, b)| = p = \text{lcm}(o(a), o(b))$. This requires that both $o(a)$ and $o(b)$ be p or $o(a) = p$ and $o(b) = 1$ and vice versa. The first case yields $(p-1)^2$ elements, while the second case yields $2(p-1)$ elements of order p . However, as each cyclic subgroup of order p has $p-1$ elements of order p , $\mathbb{Z}_p \times \mathbb{Z}_{p^2}$ has $\frac{p^2-1}{p-1} = p+1$ cyclic subgroups of order p .

3.3.2 The Number of Cyclic Subgroups of $\mathbb{Z}_n \times \mathbb{Z}_n \times \dots \times \mathbb{Z}_n$

In this subsection we consider the special case $n_1 = \dots = n_r = n$. According to (3.3),

$$o_\delta(n, \dots, n) = \sum_{e|\delta} e^r \mu(\delta/e) = \phi_r(\delta) \quad (3.7)$$

The expression above is the Jordan function of order r . Note that $\phi_1(\delta) = \phi(\delta)$ is the Euler's function.

This means that the number of all elements of order δ ($\delta|n$) in the direct product $\mathbb{Z}_n \times \dots \times \mathbb{Z}_n$, with r factors, is $\phi_r(\delta) = \delta^r \prod_{p|\delta} (1 - \frac{1}{p^r})$.

Hence the number of cyclic subgroups of order δ ($\delta|n$) of the Abelian group $\mathbb{Z}_n \times \dots \times \mathbb{Z}_n$ is $\phi_r(\delta) / \phi(\delta)$.

Now, let $c^r(n)$ denote the number of all cyclic subgroups of $\mathbb{Z}_n \times \dots \times \mathbb{Z}_n$ with r factors. In this case, for every $n \geq 1$, the following equality holds:

$$c^r(n) = \sum_{\delta|n} \frac{\phi_r(\delta)}{\phi(\delta)} \quad (3.8)$$

In particular, let $c(n) = c^2(n)$. We obtain from (3.8) that

$$c(n) = \sum_{\delta|n} \psi(\delta) \quad (3.9)$$

where $\psi(\delta) = \delta \prod_{p|\delta} (1 + \frac{1}{p})$ is the Dedekind function. For every prime power p^a ($a \geq 1$), $c(p^a) = 2(1 + p + \dots + p^{a-1}) + p^a$.

For example, by using expressions (3.7) and (3.8) we can easily count the number of all cyclic subgroups of an elementary Abelian p -group $\mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_5$, where for every $\delta | lcm(5, 5, 5)$ there exist cyclic subgroups of order δ . Consequently, there are cyclic subgroups of orders 1, 5 and the number of cyclic subgroups corresponding to each of these orders is determined as shown below.

$$o_1(5, 5, 5) = 1, c_1(5) = 1.$$

$$\begin{aligned} o_5(5, 5, 5) &= 5^3 \prod_{p|5} \left(1 - \frac{1}{p^3}\right) \\ &= 5^3 \left(1 - \frac{1}{5^3}\right) \\ &= 124. \end{aligned}$$

$$\begin{aligned} c_5(5) &= \frac{124}{\phi(5)} \\ &= 31. \end{aligned}$$

Hence, the total number of all cyclic subgroups is:

$$\begin{aligned} c^3(5) &= 1 + 31 \\ &= 32. \end{aligned}$$

Chapter Four

Combinatorial Problems on the Subgroup Lattices of Finite Abelian Groups

In this chapter, the concept of the fundamental group lattices is applied to the practical example of counting some different types of subgroups of finite Abelian groups. Explicit formulas are obtained for the number of subgroups of a given order in a finite Abelian p -group of rank two and for the number of maximal subgroups and cyclic subgroups of a given order of arbitrary finite Abelian groups. The number of elements of a prescribed order in such a group will be also found.

4.1 Fundamental Group Lattices [16]

Let $(G, +)$ be an Abelian group. Then the set $\mathcal{L}(G)$ of all subgroups of G is a modular and complete lattice.

If we suppose that G is finite of order n , the fundamental theorem of finitely generated Abelian groups implies that there exist the numbers $k \in \mathbb{N}^*$, $d_1, d_2, \dots, d_k \in \mathbb{N} \setminus \{0,1\}$ satisfying $d_1 \mid d_2 \mid \dots \mid d_k$,

$$d_1 d_2 \dots d_k = n \text{ and } G \cong \prod_{i=1}^k \mathbb{Z}_{d_i}.$$

This decomposition of a finite Abelian group into a direct product of cyclic groups initiated the concept of fundamental group lattice, defined below.

Let $k \geq 1$ be a natural number. Then for each $(d_1, d_2, \dots, d_k) \in (\mathbb{N} \setminus \{0, 1\})^k$, we consider the set $L_{(k; d_1, d_2, \dots, d_k)}$ consisting of all matrices $A = (a_{ij}) \in \mathcal{M}_k(\mathbb{Z})$ that have the following properties:

- i. $a_{ij} = 0$, for any $i > j$,
- ii. $0 \leq a_{1j}, a_{2j}, \dots, a_{j-1j} < a_{jj}$, for any $j = \overline{1, k}$,
- iii. 1. $a_{11} \mid d_1$
 2. $a_{22} \mid (d_2, d_1 \frac{a_{12}}{a_{11}})$,
 3. $a_{33} \mid (d_3, d_2 \frac{a_{23}}{a_{22}}, d_1 \frac{\begin{vmatrix} a_{12} & a_{13} \\ a_{22} & a_{23} \end{vmatrix}}{a_{22} a_{11}})$,
 \vdots
 K. $a_{kk} \mid (d_k, d_{k-1} \frac{a_{k-1k}}{a_{k-1k-1}}, d_{k-2} \frac{\begin{vmatrix} a_{k-2k-1} & a_{k-2k} \\ a_{k-1k-1} & a_{k-1k} \end{vmatrix}}{a_{k-1k-1} a_{k-2k-2}}, \dots,$
 $d_1 \frac{\begin{vmatrix} a_{12} & a_{13} & \dots & a_{1k} \\ a_{22} & a_{23} & \dots & a_{2k} \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ 0 & 0 & \dots & a_{k-1k} \end{vmatrix}}{a_{k-1k-1} a_{k-2k-2} \dots a_{11}})$,

where (x_1, x_2, \dots, x_m) denotes the greatest common divisor of the numbers $x_1, x_2, \dots, x_m \in \mathbb{Z}$.

On the set $L_{(k; d_1, d_2, \dots, d_k)}$ we introduce the next partial ordering relation (denoted by \leq), as follows:

For $A = (a_{ij}), B = (b_{ij}) \in L_{(k; d_1, d_2, \dots, d_k)}$, $A \leq B$ if and only if the relations:

- 1. $b_{11} \mid a_{11}$,

$$\begin{aligned}
& 2. \quad b_{22} \mid \left(a_{22}, \frac{\begin{vmatrix} a_{11} & a_{12} \\ b_{11} & b_{12} \end{vmatrix}}{b_{11}} \right), \\
& 3. \quad b_{33} \mid \left(a_{33}, \frac{\begin{vmatrix} a_{22} & a_{23} \\ b_{22} & b_{23} \end{vmatrix}}{b_{22}}, \frac{\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ b_{11} & b_{12} & b_{13} \\ 0 & b_{22} & b_{23} \end{vmatrix}}{b_{22}b_{11}} \right), \\
& \vdots \\
& \text{K. } b_{kk} \mid \left(a_{kk}, \frac{\begin{vmatrix} a_{k-1 \ k-1} & a_{k-1 \ k} \\ b_{k-1 \ k-1} & b_{k-1 \ k} \end{vmatrix}}{b_{k-1 \ k-1}}, \frac{\begin{vmatrix} a_{k-2 \ k-2} & a_{k-2 \ k-1} & a_{k-2 \ k} \\ b_{k-2 \ k-2} & b_{k-2 \ k-1} & b_{13} \\ 0 & b_{k-1 \ k-1} & b_{k-1 \ k} \end{vmatrix}}{b_{k-1 \ k-1}b_{k-2 \ k-2}}, \dots, \right. \\
& \left. \frac{\begin{vmatrix} a_{12} & a_{13} & \dots & a_{1k} \\ a_{22} & a_{23} & \dots & a_{2k} \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ 0 & 0 & \dots & a_{k-1 \ k} \end{vmatrix}}{b_{k-1 \ k-1}b_{k-2 \ k-2} \dots b_{11}} \right)
\end{aligned}$$

hold.

Now, for any $A = (a_{ij})$, $B = (b_{ij}) \in L_{(k; d_1, d_2, \dots, d_k)}$, we consider the matrices $U_{A,B} = (u_{ij})$ and $V_{A,B} = (v_{ij})$, where :

- $u_{ij} = 0$ and $v_{ij} = 0$, respectively, for any $i > j$,
- $u_{ii} = [a_{ii}, b_{ii}]$ as well as $v_{ii} = (a_{ii}, b_{ii})$, for any $i = \overline{1, k}$,
- the element u_{ij} (as well as v_{ij}) for $i < j$ are uniquely determined by the condition $U_{A,B} \in L_{(k; d_1, d_2, \dots, d_k)}$ and $V_{A,B} \in L_{(k; d_1, d_2, \dots, d_k)}$, respectively.

We have $U_{A,B} = \inf \{A, B\}$ and $V_{A,B} = \sup \{A, B\}$ respectively,

$(L_{(k; d_1, d_2, \dots, d_k)}, \leq)$ forms a lattice, referred to as a fundamental group lattice of degree k .

The next proposition establishes the connection between the fundamental group lattice and the finite Abelian groups.

Proposition 4.1.1 [15]

For a lattice L , the following two conditions are equivalent :

- i. There exists a finite Abelian group G , such that $L \cong \mathcal{L}(G)$.
- ii. There exist the numbers $k \in \mathbb{N}^*$, $d_1, d_2, \dots, d_k \in \mathbb{N} \setminus \{0,1\}$ such that $d_1 \mid d_2 \mid \dots \mid d_k$ and $L \cong L_{(k; d_1, d_2, \dots, d_k)}$.

Remarks.

1. If G is a finite Abelian group of order $p_1^{n_1} p_2^{n_2} \dots p_m^{n_m}$, then it is well known that G can be written as the direct product of its primary components

$$G \cong \prod_{i=1}^m G_{p_i},$$

where $|G_i| = p_i^{n_i}$, for all $i = \overline{1, m}$. Since the subgroups of a direct product of groups having coprime orders are also direct products, so we obtains that

$$\mathcal{L}(G) \cong \prod_{i=1}^m \mathcal{L}(G_{p_i})$$

Therefore, our counting problem is reduced to p -groups. In this case, we need to study only fundamental group lattice of type $L_{(k; p^{\alpha_1}, p^{\alpha_2}, \dots, p^{\alpha_k})}$, which consists of all matrices of integers $A = (a_{ij})_{i,j=\overline{1,k}}$ satisfying the conditions:

$$\left. \begin{array}{l}
\text{i. } a_{ij} = 0, \text{ for any } i > j, \\
\text{ii. } 0 \leq a_{1j}, a_{2j}, \dots, a_{j-1j} < a_{jj}, \text{ for any } j = \overline{1, k}, \\
\text{iii. } \begin{array}{l}
1. a_{11} \mid p^{\alpha_1}, \\
2. a_{22} \mid \left(p^{\alpha_2}, p^{\alpha_1} \frac{a_{12}}{a_{11}} \right), \\
3. a_{33} \mid \left(p^{\alpha_3} p^{\alpha_2} \frac{a_{23}}{a_{22}}, p^{\alpha_1} \frac{\begin{vmatrix} a_{12} & a_{13} \\ a_{22} & a_{23} \end{vmatrix}}{a_{22} a_{11}} \right), \\
\vdots \\
k. a_{kk} \mid \left(p^{\alpha_k}, p^{\alpha_{k-1}} \frac{a_{k-1k}}{a_{k-1k-1}}, p^{\alpha_{k-2}} \frac{\begin{vmatrix} a_{k-2k-1} & a_{k-2k} \\ a_{k-1k-1} & a_{k-1k} \end{vmatrix}}{a_{k-1k-1} a_{k-2k-2}}, \dots, \right. \\
\left. p^{\alpha_1} \frac{\begin{vmatrix} a_{12} & a_{13} & \dots & a_{1k} \\ a_{22} & a_{23} & \dots & a_{2k} \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ 0 & 0 & \dots & a_{k-1k} \end{vmatrix}}{a_{k-1k-1} a_{k-2k-2} \dots a_{11}} \right)
\end{array}
\right\} *$$

Where p is a prime and $1 \leq \alpha_1 \leq \alpha_2 \leq \dots \leq \alpha_k$.

2. The order of the subgroup of $\prod_{i=1}^k \mathbb{Z}_{p^{\alpha_i}}$ corresponding to the matrix

$A = (a_{ij}) \in L(k; p^{\alpha_1}, p^{\alpha_2}, \dots, p^{\alpha_k})$ is

$$\frac{p^{\sum_{i=1}^k \alpha_i}}{\prod_{i=1}^k a_{ii}}$$

4.2 The Number of Subgroups of a Finite Abelian p-Group

As shown in the previous section, in order to determine the number of subgroups of a finite Abelian group, it suffices to reduce the study to

p -groups. Hence, the problem is equivalent to determining the number of distinct solutions $A = (a_{ij}) \in \mathcal{M}_k(\mathbb{Z})$ of the system (*).

The following is the first result in this section, providing an explicit formula that can be used for counting the number of subgroups of finite

Abelian p -group $\times_{i=1}^k \mathbb{Z}_p^{\alpha_i}$ in the particular case $\alpha_1 = \alpha_2 = \dots = \alpha_k$.

Proposition 4.2.1 [14]

For $\alpha \in \{0, 1, \dots, k\}$, the number of all subgroups of order p^α in the finite elementary Abelian p -group \mathbb{Z}_p^k is 1 if $\alpha = 0$ or $\alpha = k$, and

$\sum_{1 \leq i_1 < i_2 < \dots < i_\alpha \leq k} p^{i_1 + i_2 + \dots + i_\alpha - \frac{\alpha(\alpha+1)}{2}}$ if $1 \leq \alpha \leq k - 1$. In particular, the

total number of subgroups of \mathbb{Z}_p^k is

$$2 + \sum_{\alpha=1}^{k-1} \sum_{1 \leq i_1 < i_2 < \dots < i_\alpha \leq k} p^{i_1 + i_2 + \dots + i_\alpha - \frac{\alpha(\alpha+1)}{2}}.$$

In the general case, the number of maximal subgroups of a finite Abelian

p -group $\times_{i=1}^k \mathbb{Z}_p^{\alpha_i}$ is $\sum_{i=1}^k p^{i-1} = \frac{p^k - 1}{p - 1}$.

Example 4.2.1

The aim of this example is to determine the total number of all subgroups in elementary Abelian p -group \mathbb{Z}_2^4 . For $\alpha \in \{0, 1, 2, 3, 4\}$, we begin by counting the number of all subgroups of order $2^{4-\alpha}$.

For $\alpha = 1$, we must have $1 \leq i_1 \leq 4$ which implies that the number of subgroups of order 2 in \mathbb{Z}_2^4 is in this case

$$\sum_{1 \leq i_1 \leq 4} 2^{i_1 - 1} = 2^{1-1} + 2^{2-1} + 2^{3-1} + 2^{4-1} = 15.$$

Let us now suppose that $\alpha = 2$. Then $1 \leq i_1 < i_2 \leq 4$ and thus i_1 and i_2 can be chosen respectively as follows:

(1, 2), (1, 3), (1, 4), (2, 3), (2, 4), (3, 4) which implies that the number of subgroups of order 4 in \mathbb{Z}_2^4 is in this case

$$\sum_{1 \leq i_1 < i_2 \leq 4} 2^{i_1+i_2-3} = 2^{1+2-3} + 2^{1+3-3} + 2^{1+4-3} + 2^{2+3-3} + 2^{2+4-3} + 2^{3+4-3} = 35.$$

Finally, if $\alpha = 3$, then $1 \leq i_1 < i_2 < i_3 \leq 4$, and thus i_1, i_2 and i_3 can be chosen respectively as follows:

(1, 2, 3), (1, 2, 4), (1, 3, 4), (2, 3, 4).

This implies that the number of subgroups of order 8 in \mathbb{Z}_2^4 is in this case

$$\sum_{1 \leq i_1 < i_2 < i_3 \leq 4} 2^{i_1+i_2+i_3-6} = 2^{1+2+3-6} + 2^{1+2+4-6} + 2^{1+3+4-6} + 2^{2+3+4-6} = 15.$$

Thus, the total number of all subgroups in elementary Abelian p -group \mathbb{Z}_2^4 is $2 + 15 + 35 + 15 = 67$.

Now, we return to the problem of finding the total number of subgroups

of $\prod_{i=1}^k \mathbb{Z}_p^{\alpha_i}$. We shall apply our method for rank two Abelian p -group,

i.e., for the case when $k = 2$.

Theorem 4.2.1 [14]

For every $0 \leq \alpha \leq \alpha_1 + \alpha_2$, the number of all subgroups of order $p^{\alpha_1+\alpha_2-\alpha}$ in the finite Abelian p -group $\mathbb{Z}_p^{\alpha_1} \times \mathbb{Z}_p^{\alpha_2}$ is

$$\left\{ \begin{array}{ll} \frac{p^{\alpha+1}-1}{p-1}, & \text{if } 0 \leq \alpha \leq \alpha_1 \\ \frac{p^{\alpha_1+1}-1}{p-1}, & \text{if } \alpha_1 \leq \alpha \leq \alpha_2 \\ \frac{p^{\alpha_1+\alpha_2-\alpha+1}-1}{p-1}, & \text{if } \alpha_2 \leq \alpha \leq \alpha_1 + \alpha_2. \end{array} \right.$$

In particular, the total number of subgroups of $\mathbb{Z}_{p^{\alpha_1}} \times \mathbb{Z}_{p^{\alpha_2}}$ is

$$\frac{1}{(p-1)^2} [(\alpha_2 - \alpha_1 + 1) p^{\alpha_1+2} - (\alpha_2 - \alpha_1 - 1) p^{\alpha_1+1} - (\alpha_1 + \alpha_2 + 3)p + (\alpha_2 - \alpha_1 + 1)].$$

Proof.

Let $A = (a_{ij})$ be a solution of (*) for $k = 2$, corresponding to a subgroup of order $p^{\alpha_1+\alpha_2-\alpha}$. In this case, the condition (iii) of (*) becomes

$$a_{11} \mid p^{\alpha_1} \quad \text{and} \quad a_{22} \mid (p^{\alpha_2}, p^{\alpha_1} \frac{a_{12}}{a_{11}}).$$

put $a_{11} = p^i$, where $0 \leq i \leq \alpha_1$. Then $a_{22} = p^{\alpha-i}$ and so

$$p^{\alpha-i} \mid (p^{\alpha_2}, p^{\alpha_1-i} a_{12}), \text{ that is } p^{\alpha-i} \mid p^{\alpha_1-i} (p^{\alpha_2-\alpha_1+i}, a_{12}).$$

If $0 \leq \alpha \leq \alpha_1$, we must have $i \leq \alpha$ and the above condition is satisfied by all $a_{12} < p^{\alpha-i}$.

Hence, there are $p^{\alpha-i}$ distinct solutions of (*), and the number of subgroups of order $p^{\alpha_1+\alpha_2-\alpha}$ in $\mathbb{Z}_{p^{\alpha_1}} \times \mathbb{Z}_{p^{\alpha_2}}$ is in this case

$$S_1(\alpha) = \sum_{i=0}^{\alpha} p^{\alpha-i} = \frac{p^{\alpha+1}-1}{p-1} \quad (4.1)$$

Now, if $\alpha_1 \leq \alpha \leq \alpha_2$, then $p^{\alpha_1-\alpha} \mid (p^{\alpha_2-\alpha_1+i}, a_{12})$ and thus a_{12} can be any multiple of $p^{\alpha_1-\alpha}$ in the set $\{0, 1, \dots, p^{\alpha-i} - 1\}$.

It is clear that there are p^{α_1-i} distinct solutions of (*) and the number of subgroups of order $p^{\alpha_1+\alpha_2-\alpha}$ in $\mathbb{Z}_{p^{\alpha_1}} \times \mathbb{Z}_{p^{\alpha_2}}$ is in this case

$$S_2(\alpha) = \sum_{i=0}^{\alpha_1} p^{\alpha_1-i} = \frac{p^{\alpha_1+1}-1}{p-1} \quad (4.2)$$

Finally, if $\alpha_2 \leq \alpha \leq \alpha_1 + \alpha_2$. Then $\alpha_1 - \alpha \leq \alpha_2 - \alpha_1 + i$ and the number of distinct solutions of (*) is again p^{α_1-i} . Thus the number of subgroups of order $p^{\alpha_1+\alpha_2-\alpha}$ in $\mathbb{Z}_{p^{\alpha_1}} \times \mathbb{Z}_{p^{\alpha_2}}$ is in this case

$$S_3(\alpha) = \sum_{i=\alpha-\alpha_2}^{\alpha_1} p^{\alpha_1-i} = \frac{p^{\alpha_1+\alpha_2-\alpha+1}-1}{p-1} \quad (4.3)$$

By using the equalities (4.1), (4.2) and (4.3), we obtain the total number of subgroups of Abelian p -group $\mathbb{Z}_{p^{\alpha_1}} \times \mathbb{Z}_{p^{\alpha_2}}$, which can be written as

$$\sum_{\alpha=0}^{\alpha_1} S_1(\alpha) + \sum_{\alpha=\alpha_1+1}^{\alpha_2} S_2(\alpha) + \sum_{\alpha=\alpha_2+1}^{\alpha_1+\alpha_2} S_3(\alpha) = \frac{1}{(p-1)^2} [(\alpha_2 - \alpha_1 + 1)p^{\alpha_1+2} - (\alpha_2 - \alpha_1 - 1)p^{\alpha_1+1} - (\alpha_1 + \alpha_2 + 3)p + (\alpha_1 + \alpha_2 + 1)].$$

4.3 The Number of Cyclic Subgroups of a Finite Abelian p -Group

Another application of fundamental group lattices is the counting of cyclic subgroups of finite Abelian groups. First, we need to obtain this number for a finite Abelian p -group of rank 2.

Lemma 4.3.1 [14]

The subgroup of $\mathbb{Z}_{p^{\alpha_1}} \times \mathbb{Z}_{p^{\alpha_2}}$ corresponding to the matrix $A = (a_{ij}) \in L_{(2; p^{\alpha_1}, p^{\alpha_2})}$ is cyclic if and only if $a_{22} = (p^{\alpha_2}, p^{\alpha_1} \frac{a_{12}}{a_{11}})$.

Theorem 4.3.1 [14]

For every $0 \leq \alpha \leq \alpha_2$, the number of cyclic subgroups of order p^α in the finite Abelian p -group $\mathbb{Z}_{p^{\alpha_1}} \times \mathbb{Z}_{p^{\alpha_2}}$ is:

$$\begin{cases} 1, & \text{if } \alpha = 0 \\ p^\alpha + p^{\alpha-1}, & \text{if } 1 \leq \alpha \leq \alpha_1 \\ p^{\alpha_1}, & \text{if } \alpha_1 < \alpha \leq \alpha_2 \end{cases}$$

In particular, the number of all cyclic subgroups of $\mathbb{Z}_{p^{\alpha_1}} \times \mathbb{Z}_{p^{\alpha_2}}$ is

$$2 + 2p + \cdots + 2p^{\alpha_1-1} + (\alpha_2 - \alpha_1 + 1)p^{\alpha_1}.$$

Proof.

Let $g_p^2(\alpha)$ be denote by the number of cyclic subgroups of order p^α in $\mathbb{Z}_{p^{\alpha_1}} \times \mathbb{Z}_{p^{\alpha_2}}$ and let $A = (a_{ij}) \in L_{(2; p^{\alpha_1}, p^{\alpha_2})}$ be the matrix corresponding to such a subgroup. Then

$$a_{11} \mid p^{\alpha_1}, a_{22} = (p^{\alpha_2}, p^{\alpha_1} \frac{a_{12}}{a_{11}}) \text{ and } a_{11}a_{22} = p^{\alpha_1+\alpha_2-\alpha}.$$

Put $a_{11} = p^i$, $0 \leq i \leq \alpha_1$. Then

$$a_{22} = p^{\alpha_1+\alpha_2-\alpha-i} = (p^{\alpha_2}, p^{\alpha_1-i}a_{12}) = p^{\alpha_1-i}(p^{\alpha_2-\alpha_1+i}, a_{12}),$$

which implies that

$$p^{\alpha_2-\alpha} = (p^{\alpha_2-\alpha_1+i}, a_{12}). \quad (4.4)$$

If $\alpha = 0$, then $a_{11} = p^{\alpha_1}$, $a_{22} = p^{\alpha_2}$, $a_{12} = 0$, and thus

$$g_p^2(0) = 1 \quad (4.5)$$

For $1 \leq \alpha \leq \alpha_1$ we must have $\alpha_1 - \alpha \leq i$. If $i = \alpha_1 - \alpha$, the condition (4.4) is equivalent to $p^{\alpha_2-\alpha} \mid a_{12}$, therefore a_{12} can be chosen in p^α

ways. If $\alpha_1 - \alpha + 1 \leq i$, (4.4) is equivalent to $p^{\alpha_2 - \alpha} \mid a_{12}$ and $p^{\alpha_2 - \alpha + 1} \nmid a_{12}$.

There are $p^{\alpha_1 - i} - p^{\alpha_1 - i - 1}$ elements of the set $\{0, 1, \dots, p^{\alpha_1 + \alpha_2 - \alpha - i}\}$ satisfying the previous relations. Therefore,

$$g_p^2(\alpha) = p^\alpha + \sum_{i=\alpha_1 - \alpha + 1}^{\alpha_1} (p^{\alpha_1 - i} - p^{\alpha_1 - i - 1}) = p^\alpha + p^{\alpha - 1} \quad (4.6)$$

If $\alpha_1 < \alpha \leq \alpha_2$, then the condition $\alpha_1 - \alpha \leq i$ is satisfied by all $i = \overline{1, \alpha_1}$, and hence

$$g_p^2(\alpha) = \sum_{i=0}^{\alpha_1} (p^{\alpha_1 - i} - p^{\alpha_1 - i - 1}) = p^{\alpha_1} \quad (4.7)$$

Now, from the equalities (4.5)-(4.7) we conclude that the total number of cyclic subgroups of $\mathbb{Z}_{p^{\alpha_1}} \times \mathbb{Z}_{p^{\alpha_2}}$ is

$$1 + \sum_{\alpha=1}^{\alpha_1} (p^\alpha + p^{\alpha-1}) + \sum_{\alpha=\alpha_1+1}^{\alpha_2} p^{\alpha_1} = \frac{1}{p-1} [(\alpha_2 - \alpha_1 + 1)p^{\alpha_1+1} - (\alpha_2 - \alpha_1 - 1)p^{\alpha_1} - 2] = 2 + 2p + \dots + 2p^{\alpha_1-1} + (\alpha_2 - \alpha_1 + 1)p^{\alpha_1}.$$

The above method can be used for an arbitrary $k > 2$, too. In order to do this we need to remark that

$$g_p^2(\alpha) = \frac{p^\alpha h_p^1(\alpha) - p^{\alpha-1} h_p^1(\alpha-1)}{p^\alpha - p^{\alpha-1}}$$

for all $\alpha \neq 0$, where

$$h_p^1(\alpha) = \begin{cases} p^\alpha, & \text{if } 0 \leq \alpha \leq \alpha_1 \\ p^{\alpha_1}, & \text{if } \alpha_1 \leq \alpha \end{cases}$$

This equality extends to the general case, as described below.

Theorem 4.3.2 [14]

For every $1 \leq \alpha \leq \alpha_k$, the number of cyclic subgroups of order p^α in the finite Abelian p -group $\prod_{i=1}^k \mathbb{Z}_p^{\alpha_i}$ is

$$g_p^k(\alpha) = \frac{p^\alpha h_p^{k-1}(\alpha) - p^{\alpha-1} h_p^{k-1}(\alpha-1)}{p^\alpha - p^{\alpha-1}},$$

where

$$h_p^{k-1}(\alpha) = \begin{cases} p^{(k-1)\alpha}, & \text{if } 0 \leq \alpha \leq \alpha_1 \\ p^{(k-2)\alpha + \alpha_1}, & \text{if } \alpha_1 \leq \alpha \leq \alpha_2 \\ \vdots & \\ p^{\alpha_1 + \alpha_2 + \dots + \alpha_{k-1}}, & \text{if } \alpha_{k-1} \leq \alpha \leq \alpha_k. \end{cases}$$

Since the numbers of cyclic subgroups and of elements of a given order in a finite Abelian p -group are connected by Euler's function ϕ , so we infer the following consequence of Theorem 4.3.2.

Corollary 4.3.1 [14]

The number of all elements of order p^α , $1 \leq \alpha \leq \alpha_k$, in the finite Abelian p -group $\prod_{i=1}^k \mathbb{Z}_p^{\alpha_i}$ is

$$g_p^k(\alpha)\phi(p^\alpha) = g_p^k(\alpha)(p^\alpha - p^{\alpha-1}) = p^\alpha h_p^{k-1}(\alpha) - p^{\alpha-1} h_p^{k-1}(\alpha - 1).$$

For example, let us compute the number of all cyclic subgroups of a finite Abelian p -group $\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_{p^2}$.

If $\alpha = 1$, then the number of all cyclic subgroups (as well as elements) of order p in $\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_{p^2}$ is

$$g_p^3(1) = \frac{ph_p^2(1) - h_p^2(0)}{p-1} = p^2 + p + 1$$

$$g_p^3(1)\phi(p) = (p^2 + p + 1)(p - 1).$$

If $\alpha = 2$, then the number of all cyclic subgroups (as well as elements) of order p^2 in $\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_{p^2}$ is

$$g_p^3(2) = \frac{p^2 h_p^2(2) - p h_p^2(1)}{p^2 - p} = p^2,$$

$$g_p^3(2)\phi(p^2) = p^2(p^2 - p).$$

Hence, the number of all cyclic subgroups of finite Abelian p -group $\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_{p^2}$ is $2p^2 + p + 2$.

Remark.

Let G be a finite Abelian group of order $p_1^{n_1} p_2^{n_2} \dots p_m^{n_m}$ and let $\bigtimes_{i=1}^m G_{p_i}$ be the corresponding primary decomposition of G . Then every cyclic subgroup H of order $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m}$ of G can be uniquely expressed as a direct product $\bigtimes_{i=1}^m H_{p_i}$, where H_{p_i} is a cyclic subgroup of order $p_i^{\alpha_i}$ of G_{p_i} , $i = \overline{1, m}$.

This remark leads to the following result, that generalizes Theorem 4.3.2 and Corollary 4.3.1.

Corollary 4.3.2 [14]

Based on the previous remark, for every $(\alpha_1, \alpha_2, \dots, \alpha_m) \in \mathbb{N}^m$ with $\alpha_i \leq n_i$, $i = \overline{1, m}$, the number of cyclic subgroups (and elements) of order $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m}$ in G is

$$\prod_{i=1}^m g_{p_i}^{k_i}(\alpha_i)$$

and

$$\prod_{i=1}^m g_{p_i}^{k_i}(\alpha_i)\phi(p_i^{\alpha_i}),$$

respectively, where k_i denotes the number of direct factors of G_{p_i} , $i = \overline{1, m}$.

For example, consider the Abelian group $\mathbb{Z}_{36} \times \mathbb{Z}_{90}$ used in Example 1.3, whereby the number of all of cyclic subgroups of order 15, and the number of elements of the same order can be obtained as follows:

Since $\mathbb{Z}_{36} \times \mathbb{Z}_{90} \cong \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_9 \times \mathbb{Z}_9 \times \mathbb{Z}_5$, then $p_1 = 3$, $p_2 = 5$, $k_1 = 2$, $k_2 = 1$, $\alpha_1 = \alpha_2 = 1$. So the number of all cyclic subgroups of order 15 is

$$\begin{aligned} \prod_{i=1}^2 g_{p_i}^{k_i}(\alpha_i) &= g_{p_1}^{k_1}(\alpha_1)g_{p_2}^{k_2}(\alpha_2) \\ &= g_3^2(1)g_5^1(1) \\ &= \left(\frac{3h_3^1(1)-h_3^1(0)}{3-1}\right)\left(\frac{5h_5^0(1)-h_5^0(0)}{5-1}\right) \\ &= 4. \end{aligned}$$

Where, $h_3^1(1) = 3$ and $h_3^1(0) = 1$, therefore $g_3^2(1) = 4$. Also $h_5^0(1) = h_5^0(0) = 1$, therefore $g_5^1(1) = 1$, also the number of elements of order 15 is

$$\begin{aligned} \prod_{i=1}^2 g_{p_i}^{k_i}(\alpha_i)\phi(p_i^{\alpha_i}) &= g_{p_1}^{k_1}(\alpha_1)\phi(p_1^{\alpha_1})g_{p_2}^{k_2}(\alpha_2)\phi(p_2^{\alpha_2}) \\ &= g_3^2(1)\phi(3)g_5^1(1)\phi(5) \\ &= 32. \end{aligned}$$

Appendix

The program to calculate the total number of subgroups and the number of subgroups of order $p^n, 0 \leq n \leq n_1 + n_2$, in a finite Abelian p -group $\mathbb{Z}_{p^{n_1}} \times \mathbb{Z}_{p^{n_2}}$:

```

clear
P =input('Please inter P ');
n1=input('Please inter n1 ');
n2=input('Please inter n2 ');
if n1>n2
m =n2;
n2=n1;
n1=m;
end
x=1/(P-1)^2* ((n2-n1+1)*P^(n1+2)-(n2-n1-1)*P^(n1+1)-
(n1+n2+3)*P+(n1+n2+1));
disp(['The total number of subgroups is ',num2str(x)])
n=0;
while n<=(n1+n2)
if n>=0 & n<=n1
y=(P^(n+1)-1)/(P-1);
w=P^n;
disp(['The number of all subgroups of order ',num2str(w),'
is ',num2str(y)])
else if n>=n1 & n<=n2
y=(P^(n1+1)-1)/(P-1);
w=P^n;
disp(['The number of all subgroups of order ',num2str(w),'
is ',num2str(y)])
else if n>=n1 & n <=(n1+n2)
y=(P^(n1+n2-n+1)-1)/(P-1);
w=P^n;
disp(['The number of all subgroups of order ',num2str(w),'
is ',num2str(y)])
end
n=n+1;
end

```

Input

```

Please inter P      3
Please inter n1     1
Please inter n2     2

```

Output

```

The total number of subgroups is 10
The number of all subgroups of order 1 is 1
The number of all subgroups of order 3 is 4
The number of all subgroups of order 9 is 4
The number of all subgroups of order 27 is 1

```

The program to calculate the total number of cyclic subgroups and the number of cyclic subgroups of order $p^n, 1 \leq n \leq n_k$, respectively the number of all elements of a finite Abelian p -group $\mathbb{Z}_{p^{n_1}} \times \mathbb{Z}_{p^{n_2}} \times \dots \times \mathbb{Z}_{p^{n_k}}$.

```

clear
p=input('please inter p ');
k=input('please inter k ');
N=zeros(1,k);
for i=1:k
N(1,i)=input(['Please inter n',num2str(i)]);
end
SUM=0;
n=1;
disp('The number of all cyclic subgroups of order 1 is 1 ')
disp('The number of all elements of order 1 is 1 ')
while n<=N(1,k)
if n>=0 & n<=N(1,1)
x=p^((k-1)*n);
y=p^((k-1)*(n-1));
m=(x*p^n-y*p^(n-1))/(p^n-p^(n-1));
SUM=SUM+m;
B=m*(p^n-p^(n-1));
w=p^n;
disp(['The number of all cyclic subgroups of order ',num2str
(w),' is ', num2str(m)])
disp(['The number of all elements of order ',num2str(w),'
is ', num2str(B)])
else if n>=N(1,1) & n<=N(1,2)
x=p^((k-2)*n+ N(1,1));
y=p^((k-2)*(n-1)+ N(1,1));
m=(x*p^n-y*p^(n-1))/(p^n-p^(n-1));
SUM=SUM+m;
B=m*(p^n-p^(n-1));
w=p^n;
disp(['The number of all cyclic subgroups of order ',num2str
(w),' is ', num2str(m)])
disp(['The number of all elements of order ', num2str(w),'
is ', num2str(B)])
elseif N(1,k-1)<= n
x=p^(sum(N(1,1:k-1)));
m=x*(p^n-p^(n-1))/(p^n-p^(n-1));
SUM=SUM+m;
B=m*(p^n-p^(n-1));
w=p^n;
disp(['The number of all cyclic subgroups of order ',num2str
(w),' is ', num2str(m)])
disp(['The number of all elements of order ', num2str(w),'
is ',num2str(B)])
end
n=n+1;
end

```

```
x=SUM+1;
disp(['The total number of cyclic subgroups is ',num2str(x)])
```

Input

```
Please inter P      2
please inter k      3
Please inter n1     1
Please inter n2     1
Please inter n3     2
```

Output

```
The number of all cyclic subgroups of order 1 is 1
The number of all elements of order 1 is 1
The number of all cyclic subgroups of order 2 is 7
The number of all elements of order 2 is 7
The number of all cyclic subgroups of order 4 is 4
The number of all elements of order 4 is 8
The total number of cyclic subgroups is 12
```


The program to calculate the total number of subgroups and the number of subgroups of order $p^n, 0 \leq n \leq k$, of elementary Abelian p -group \mathbb{Z}_p^k , of arbitrary rank:

```

clear
P=input(' Please inter p ');
k=input ('Please inter k ');
sum=0;
n=0;
while n<=k
if n==0
disp(' The number of all subgroups of order 1 is 1 ')
else if n>=1 & n <=k
%the power of P in the Numerator:
m1=k:-1:(k-n+1);
NUM=prod(P.^m1-1);
%the power of P in the Denominator:
m2=n:-1:1;
DUM=prod(P.^m2-1);
y=NUM/DUM;
sum=sum+y;
w=P^n;
disp(['The number of all subgroups of order ',num2str(w),'
is ', num2str(y)])
end
n=n+1;
end
x=sum+1;
disp(['The total number of subgroups is ',num2str(x)])

```

Input

```

Please inter P    5
please inter k    3

```

Output

```

The number of all subgroups of order 1 is 1
The number of all subgroups of order 5 is 31
The number of all subgroups of order 25 is 31
The number of all subgroups of order 125 is 1
The total number of subgroups is 64

```

Conclusions and Future Work

The results presented in this work indicate that the counting of subgroups of a finite Abelian group is an interesting combinatorial aspect of group theory. In this study, although different types of subgroups of a finite Abelian group were counted, it was not possible to produce explicit formulas for counting the number of subgroups of fixed order or total number of subgroups of finite Abelian p -group of arbitrary rank.

Consequently, as a potential direction of further research in this field, the following subjects are noted :

- The number of Fuzzy subgroups of a finite Abelian groups.
- The number of Characteristic subgroups of finite Abelian groups.
- Create computer algebra programmes to count the number of subgroups of finite Abelian group.

References

- [1] Awami, M., The Number of Subgroups of Finite Abelian Groups, Unpolished.
- [2] Burris, S., Sankappanavar, H.P., A Course in Universal Algebra, Springer-Verlag, (1981).
- [3] Călugăreanu, G., The Total Number of Subgroups of a Finite Abelian Group, Sci., Math. Jpn. (2004), 1-11.
- [4] Davey, B.A., Priestley, H.A., Introduction to Lattices and Order, Cambridge Press, (1990).
- [5] David S. Dummit and Richard M. Foote, Abstract Algebra, John Wiley and Sons , Third Edition, (2004).
- [6] Fraleigh, J.B., A First Course in Abstract Algebra, Addison Wesley, Seventh Edition, (2002).
- [7] Fuchs, L., Infinite Abelian Groups, I, New York, (1970).
- [8] Gallian, J.A., Contemporary Abstract Algebra, Houghton Mifflin Company Boston New York, (2002).
- [9] Gilbert, J., Gilbert, L., Elements of Modern Algebra, Brooks/Cole, fifth Edition, (2000).
- [10] Kurzweil, H., Stellmacher, B., The Theory of Finite Groups, Springer-Verlag , (2004).
- [11] Miller, G. A., Subgroups of The Groups Whose Orders are Below Thirty, Proc. Nat. Acad. Sci. (1940), 500-502.
- [12] Schmidt, R., Subgroup Lattices of Groups, de Gruyter Expositions , Berlin, (1994).

- [13] Suzuki, M., Group Theory, I, Springer-Verlag, Berlin, (1982).
- [14] Tărnăuceanu, M., An Arithmetic Method of Counting The Subgroups of a Finite Abelian Group, Bull. Math. Soc. Sci. Math. Romanic (N.S.), 53 (101) (2010), 373-386.
- [15] Tărnăuceanu, M., A New Method of Proving Some Classical Theorems of Abelian Groups, Southeast Asian Bull. Math. (6) 31 (2007), 1191-1203.
- [16] Tărnăuceanu, M., Fundamental Group Lattices, Current Research in computer Science, Theory and Applications (F. Eugeniu, H. Luchian eds.), Editor Panfilius, Iasi, (2003), 1-10.
- [17] Tóth, L., On The Number of Cyclic Subgroups of a Finite Abelian Group, Bull. Math. Soc. Sci. Math. Roumania (N.S.), 55(103) (2012), 423-428.
- [18] Rose, H.E., A Course on Finite Groups, Springe-Verlag, University of Bristol, (2009).
- [19] Rotman , J.J., Advanced Modern Algebra, prentice Hall, Second Edition, (2003).

الخلاصة

في هذا العمل خضنا في موضوع يعتبر احد أهم المواضيع في نظرية الزمر وهو حساب عدد الزمر الجزئية في الزمرة . و الصعوبة في الولوج لهذا الموضوع انه يتطلب معرفة عميقة في نظرية الزمر، ولذلك قمنا بتقديم نعتقد انه كاف لكل من يريد مناقشة هذه المسألة بتتبع كل المحاولات من قبل الرياضيين منذ 1940[11] إلي 2012 [17] وتناول الرياضيون هذا الموضوع عن طريق حالات خاصة وكلهم اقتصروا علي الزمر المحدودة بل الزمر التبديلية المحدودة ولذلك قمنا بدراسة هذا النوع الأخير من الزمر، حيث - كما معروف انه إذا كانت لدينا زمرة تبديلية محدودة ، فانه يمكن كتابتها علي صورة الضرب المباشر لزمر جزئية تبديلية مرتبتها p^n ، وبالتالي يصبح حساب الزمر الجزئية في الزمرة التبديلية المحدودة يعتمد علي معرفتنا لحساب عدد الزمر الجزئية ذات المرتبة p^n ، أيضا في [14] أورد Tărnăuceanu طرق لحساب عدد الزمر الجزئية في الزمر التبديلية المحدودة، وفي نهاية الورقة اقترح الباحث مشكلة مفتوحة وهي إمكانية تصميم منظومة برامج لحساب الزمر الجزئية لزمر التبديلية ذات الأنواع المختلفة. وبالفعل قمت بتصميم هذه المنظومة من البرامج كخوارزميات أولا ثم بمساعدة بعض المختصين تم تحويلها إلي لغة المتلاب، وهو يعتبر إضافة لهذا الموضوع واثني عليه الباحث نفسه ولقد قمت بتبويب هذا العمل على النحو الآتي :

- **الباب الأول :** في هذا الباب تم عرض كل التعاريف والمفاهيم الأساسية المستخدمة في هذه الأطروحة .
- **الباب الثاني :** تم تقديم تركيب الزمر التبديلية المحدودة وأوردنا Automorphism للزمر الدورية كمثال علي الزمر التبديلية المحدودة .
- **الباب الثالث :** وفيه ناقشنا طرق مختلفة لحساب عدد الزمر الجزئية للزمرة التبديلية المحدودة.
- **الباب الرابع :** في هذا الباب استخدمنا مفهوم Fundamental group lattice لحساب الزمر الجزئية ذات الأنواع المختلفة في الزمرة التبديلية المحدودة.

وفي نهاية العمل أرفقنا ملحقا يوضح البرامج وتطبيقاتها بأمثلة لحساب عدد الزمر الجزئية في الزمر التبديلية المحدودة.