STUDIES OF EQUIVALENT FUZZY SUBGROUPS OF FINITE ABELIAN p-GROUPS OF RANK TWO AND THEIR SUBGROUP LATTICES

A thesis submitted in fulfilment of the

requirements for the degree of

DOCTOR OF PHILOSOPHY (SCIENCE)

of

RHODES UNIVERSITY

by

SAKHILE LEONARD NGCIBI

June 2005

Abstract

We determine the number and nature of distinct equivalence classes of fuzzy subgroups of finite Abelian p-group G of rank two under a natural equivalence relation on fuzzy subgroups. Our discussions embrace the necessary theory from groups with special emphasis on finite p-groups as a step towards the classification of crisp subgroups as well as maximal chains of subgroups. Unique naming of subgroup generators as discussed in this work facilitates counting of subgroups and chains of subgroups from subgroup lattices of the groups. We cover aspects of fuzzy theory including fuzzy (homo-) isomorphism together with operations on fuzzy subgroups. The equivalence characterization as discussed here is finer than isomorphism. We introduce the theory of keychains with a view towards the enumeration of maximal chains as well as fuzzy subgroups under the equivalence relation mentioned above. We discuss a strategy to develop subgroup lattices of the groups used in the discussion, and give examples for specific cases of prime p and positive integers n, m. We derive formulas for both the number of maximal chains as well as the number of distinct equivalence classes of fuzzy subgroups. The results are in the form of polynomials in p (known in the literature as Hall polynomials) with combinatorial coefficients. Finally we give a brief investigation of the results from a graph-theoretic point of view. We view the subgroup lattices of these groups as simple, connected, symmetric graphs.

KEYWORDS *Fuzzy Subgroups, Rank two, Equivalence relation, Maximal chains, Keychains, Invariants, Solvability, Isomorphic subgroups, Equivalence classes, Lattice diagrams, Partition, Graphs, Tree orientations, Connectivity, Paths.*

MSC2000 SUBJECT CLASSIFICATION:

Primary	20N25, 20K27, 20K01
Secondary	03E72, 20D30, 20D60

The financial assistance of the National Research Foundation (NRF) towards this research is hereby acknowledged. Opinions expressed and conclusions arrived at, are those of the author and are not necessarily to be attributed to the NRF.

Contents

ILLUSTRATIONS OF FIGURES AND TABLES

NOTATION

$\mathbb{Z}$	integers, additive group of integers
$(x)_m$	falling factorial
$S(n,k)$	Stirling numbers of the second kind
$H \lhd G$	H is a normal subgroup of G
$\lvert G:H\rvert$	the index of H in G
xH	$\{xh : h \in H\}$
G/H	factor group
$\mathbb{Z}(G)$	the center of G, $\{x \in G : xy = yx \quad \text{for all} \quad y \in G\}$
$N(a)$	Normalizer of a in G, $\{x \in G : x^{-1}ax = a\} = \{x \in G : ax = xa\}$
$gcd(k,m)$	greatest common divisor of integers k and m
$f(a)$	image of a under f
$[a]$	equivalence class of S containing a, $\{x \in S : x \sim a\}$
$G \approx H$	G is isomorphic to H
$C(n,k)$	binomial coefficient
$det(a_{ij})$	determinant of (a_{ij})
$\lvert G\rvert$	order of the group G
$H \times K$	internal direct product of H and K
$\phi(n)$	Euler phi function of n
$\mu \wedge \nu$	the intersection of fuzzy subsets μ and ν
$\mu \vee \nu$	the union of fuzzy subsets μ and ν
μ/ν	the quotient of fuzzy subsets μ and ν
$\langle a\rangle$	cyclic group generated by a, $\{na : n \in \mathbb{Z}\}$
$x\Re y$	the relation of x to y
$\phi : G \to H$	mapping of G to H
$\cup_{i\in I} A_i$	union of sets A_i, $\quad i \in I$
$\langle a,b\rangle$	the subgroup generated by the linear combination of $\langle a\rangle$ and $\langle b\rangle$
$\{u,v\}$	the edge with endpoints u and v
$\{[a;b],c\}$	the edges $\{a,c\}$ and $\{b,c\}$.
pnpm	the group $\mathbb{Z}_{p^n} \times \mathbb{Z}_{p^m}$
G_p	for any prime p dividing $\lvert G\rvert$, we set $G_p = \{g : \lvert g\rvert = p^k\}$.

$L(G) \times L(H)$ the product of the subgroup lattices of G and H.

$k_{m,n}$ a complete bipartite graph whose vertex set is partitioned into two subsets of m and n respectively.

$M(G)$ the number of maximal chains of a group G.

$M(G)_n^m$ the number of maximal chains of $G = \mathbb{Z}_{p^n} \times \mathbb{Z}_{p^m}$.

$\mathcal{F}(G)$ the number of fuzzy subgroups of a group G.

$\mathcal{F}(G)_n^m$ the number of fuzzy subgroups of $G = \mathbb{Z}_{p^n} \times \mathbb{Z}_{p^m}$.

Simple graph A graph G in which every pair of distinct vertices is connected by no more than one edge.

Complete graph A graph in which each vertex is connected to each of the others by one edge.

Connected graph A graph G in which there is a path between every pair of distinct vertices.

Valency the number of edges incident to a vertex.

Subgraph a smaller graph remaining after the removal of edges and vertices from the original graph without the removal of endpoints of any remaining edges. Thus $H = (W, F)$ is a subgraph of $G = (V, E)$ if and only if $W \subseteq V$ and $F \subseteq E$.

Regular graph a simple graph in which every vertex has the same valency.

To my Family

This work is dedicated extendedly to my sons.

'Boys' it wasn't easy feeling lonely.

ACKNOWLEDGEMENTS

My sincere gratitude goes to my supervisor, Professor Venkat Murali. I am grateful for his patience and support, reading through endless alterations, making the best out of this project. Over the years he has always gone beyond his call of duty to encourage, advise and boost my personal development. Thank you for all your effort on my behalf.

I wish to thank Professor Sizwe Mabizela, the Head of Department of Mathematics, for providing me with a favourable environment and quality machinery during my research years at the university. He took his time, effort and all the patience in making sure that the final version of this thesis is the best it should be.
I thank all the members of staff at Rhodes University for all their support and kind wishes for me.

My sincere thanks go to the head of Mathematics department at Fort Hare University, Professor B.B. Makamba, for his valuable criticisms, comments and input during the output of the research results.

To my parents, sisters and brothers who have been behind me since the beginning of my studies. Thank you all for not giving up on me. I am very grateful for your love and support. Little guys and girls, you have been an inspiration to me. My friends you have been wonderful during my studies.

My tertiary studies would not have been possible without the kind support of:

- the Armaments Corporation of South Africa (ARMSCOR)
- the National Research Foundation (NRF)
- Andrew Mellon Foundation Scholarship

Overall, I am indebted to **God** for giving me strength to overcome hardships and hurdles; **He** was always there every time I called.

PREFACE

“The important thing in science is not so much to obtain new facts as to discover new ways of thinking about them.” Sir William Bragg.

This work is a product of the analysis of our project from three broad angles of mathematics, namely the crisp group theory, the fuzzy group theory and finally the graph theory. Some ideas that were previously investigated by other authors were too strong in our view not to be included in this thesis. As a tradition, we felt that it would be worthwhile to bring together a collection of surveys by other distinguished authors, hoping it would prove useful to the professionals, experts as well as newcomers. We acknowledge the input whenever it is necessary. The influence of the studies by Murali and Makamba, in particular, in the compilation of this thesis cannot be understated.

We aim at presenting the results in a manner that is accessible to all in the algebra discipline. We start by giving the background and fundamentals of group theory, with special emphasis on terminology necessary for the flow of the subject. We include solvability for the reason that Abelian groups are solvable, as well as in fact any group of prime-power order. This is evident from a well-known hierarchy of classes of groups:

$$\text{Cyclic} \subset \text{Abelian} \subset \text{Nilpotent} \subset \text{Supersolvable} \subset \text{Solvable} \subset \text{Group}.$$

In chapter 3 we count the number of crisp subgroups of finite Abelian p-groups from the developed subgroup lattices of finite Abelian $p-$groups of a specified rank. We describe the process of the development of tree diagrams for the subgroup generators. We explain how we label the generators in a unique fashion. The references [15], [29], [30], [59], and [63] were very helpful in the preparation of this section.

In chapter 4 we give an account background on the theory of fuzzy subgroups. We give a carry over of the group theoretic terms to the fuzzy case. We touch briefly on the theory of t-norms as a special case of the *min* and mention some few results based on the observation. We cite the important study of the operations on

fuzzy subgroups in the form of sum, union, intersection, and quotient. We close the chapter by studying the mappings on fuzzy subgroups especially with regard to equivalent fuzzy subgroups.
The references [1], [2], [3], [4], [5], [6], [8], [9], [11], [17], [21], [23], [24], [34], [43], [44], [51], [57], [61], [62], [63], [65], [66], [68], [73], [75], [77], [78], and [90] were consulted during the preparation of this section.

In chapter 5 we start the business of maximal chain and keychain enumeration. We enumerate maximal chains based on the developed subgroup lattices, to be used later in chapter 6. We describe a process of conversion from a subgroup lattice into a binary tree diagram and vice versa. We describe a transition from what is commonly known as a series in group theory to the new terminology of flags. We treat pinned flags in connection with an equivalence relation discussed in chapter 4.
We referred to the references [29], [59], [60], [62], [63], and [79] to prepare this section.

In chapter 6 we count the number of distinct equivalence classes of fuzzy subgroups of finite Abelian groups of rank two under the stated equivalence relation. The general problem of classification of fuzzy subgroups of a finite Abelian group of any given order is both important and interesting; but is complicated and enormous. We illustrate how the keychains can be applied to a lattice of maximal chains of G to obtain the number of fuzzy subgroups of G. We demonstrate the process for specific values of prime p and positive integers n and m. We prove by induction some results for a specified m and any n and p. We demonstrate the induction process for a general case. We also give a general formula for a general number of fuzzy subgroups of finite Abelian groups of rank two, and state the result as a conjecture. The discovery of the coefficients of the first term of the combinatorial formula for the number of fuzzy subgroups of these groups is explained in this chapter.
The references [59], [64], [71], [79] were useful during the preparation of this section.

From chapter 7 we devote our attention to looking at lattice diagrams in a graph theoretic point of view. In chapter 7 we introduce the graph terminology as widely used in graph theory. We identify specific kinds of graphs as encountered in graph theory literature. We realize that the lattices we have developed share special features with widely known graphs.

In chapter 8 we introduce the theory of generators and relations. We aim at using the terminology and the results obtained on trees to characterize our tree diagrams. We touch briefly on the theory of digraphs and some applications.
For chapters 7 and 8 the references [30], [12], [38], [72], [85] were used.

We would like to extend a word of appreciation to Professor Shaun Bangay of the Department of Computer Sciences at Rhodes University who checked the validity of computations of maximal chains and fuzzy subgroups by means of a computer program.

Chapter 1

Fundamentals of Group Theory

1.1 Introduction

We owe the term **group** to E. Galois who together with C. Jordan and F. Klein, however though, used only the closure axiom to define a group in the nineteenth century. The other axioms we see nowadays are in no doubt inherent in their work since the authors merely considered finite sets of permutations.

The need for the associative law and for the existence of an identity arose in a paper by A. Cayley, where he defined a group using abstract symbols coupled with either a multiplication table or a set of defining relations. In fact the modern axioms for a group as encountered were published by W.Dyck and H.Weber in 1882, and not until the publication of Weber's textbook in 1886 did the axioms become widely used thereafter. [14]

1.2 Finite Groups

1.2.1 Preliminaries

In this section we discuss basic group theory terminology that will be required in this thesis. We first introduce finite groups in general, *finite Abelian p-groups* in particular. Some details are left out either because they are easy to understand or they can be found in literature. The references [36], [26], [42], [49], to name but a few, contain the details. Although we are dealing with Abelian groups, we will sometimes use multiplicative notation whenever it is convenient and whenever the context is clear.

If a group G has only a finite number k of elements, it is called a finite group and k is known as the *order* of the group, denoted $|G|$.
A.L Cauchy defined the order of an element of a group in 1815. Today we have various versions of the concept.
For $h \in G$, if n is the smallest number for which $h^n = e$, then n is called the order of h, and the sequence $e, h, h^2, \ldots, h^{n-1}$ is called the period of h.
The order k of a subgroup H is a whole number divisor of the order g of the whole group, whereby the quotient $g/k = \ell$ is referred to as the index of the subgroup H in the group G.
Two groups are said to be *isomorphic* if the elements A of the one can be made to correspond to the elements A' of the other uniquely and reciprocally in such a way that $AB = C$ implies that $(AB)' = A'B' = C'$. In fact isomorphic groups are essentially identical with the individual elements just labelled differently. The need for such a notation as isomorphism is innate in C.F Gauss$'$s article, *Disquistiones Arithmeticae* (1801), where he considered the many types of Abelian groups. In fact the notion of isomorphism appears under various names in the work of most 19th-century group theorists.
Any group in which every element has a finite order is called a *torsion* group. A *torsion-free* group is the opposite.
Important result emanating from the concepts of torsion and factor groups is stated below:

Theorem 1.2.1 *The set T of all elements of finite order in a group G is the torsion subgroup of G and the factor group G/T is torsion-free.*

1.2.2 Conjugate Elements and Classes

Every equivalence is a method of extraction of a particular kind of identicalness. For instance, in the symmetric group the identicalness of conjugacy is that of permutations with the same cycle structure.

For $a, x \in G$, the element xax^{-1} is said to be an element *conjugate* to a. Two elements a and b that are conjugate to a third element c are also conjugate to each other, as can easily be checked, that is, conjugacy is transitive in nature. In fact, we say that conjugacy is an *equivalence relation*. Now those elements which are conjugate to each other form a *class*. The identity of the group forms a class by itself, since it is *not* conjugate to any other element except itself.
In an Abelian group, each class consists of just one element, since $xax^{-1} = a$, for all x in G. All the elements of a class have the *same order*. In any group G, the relation of conjugacy partitions the elements into disjoint classes called *conjugacy classes*. Thus $a, b \in G$ lie in the same conjugacy class if and only if $g^{-1}ag = b$ for some $g \in G$.

Definition 1.2.2 *A* centralizer *of a subset H of a group is the set of all elements of G that commute with H, the set $\{g \in G : g^{-1}hg = h, \text{ for all } h \in H\}$.*
The center *of a group G is the set of all elements of G whose centralizer is G itself.*

We next define the concept of commutator in the group sense.

Definition 1.2.3 (Commutator and Commutator subgroup) *Suppose G is a group and $a, b \in G$. Then the* commutator *of a and b is the element $a^{-1}b^{-1}ab$.*
The commutator subgroup *of G is the subgroup $\overline{G}$ of G generated by all the commutators in G.*

Note 1.2.4 The set of commutators need not form a subgroup of G. Also $\overline{G}$ as defined in Definition 1.2.3 is a normal subgroup of G. The factor group $G/\overline{G}$ is Abelian for the following reason:

For any $a, b \in G$, let $a\overline{G}, b\overline{G}$ be elements of $G/\overline{G}$. Then

$$\begin{aligned}(a\overline{G})(b\overline{G}) = ab\overline{G} &= ba(a^{-1}b^{-1}ab)\overline{G} \\ &= ba\overline{G} \text{ (because } a^{-1}b^{-1}ab \in \overline{G}) \\ &= (b\overline{G})(a\overline{G}).\end{aligned}$$

$\overline{G}$ is a group and thus has its commutator subgroup, which is the subgroup of G generated by all elements of the form $(\overline{a})^{-1}(\overline{b})^{-1}\overline{a}\overline{b}$ where $\overline{a}, \overline{b} \in \overline{G}$.

1.2.3 Invariant Subgroups

A subgroup which consists entirely of the whole class of the original group is called an *invariant subgroup.*

Let $H = \{e, h_2, \ldots, h_n\}$ be an invariant subgroup. Now since H is a group, H must contain together with h_i and h_j their product h_ih_j. Further, H contains ah_ia^{-1} where a is an element of the big group. This is the case since an invariant subgroup contains all the elements ah_ia^{-1} of a class if and only if it contains one element h_i of the class.

Note 1.2.5 Every subgroup of an Abelian group is an invariant subgroup. Every element is a class in itself; hence every subgroup must consist entirely of whole classes.

Groups which have no invariant subgroups are called *simple* groups.

The factor-group of the invariant subgroup H

The elements $eU = U, h_2U, \ldots, h_nU$ form a (right) coset of the invariant subgroup H denoted as HU. Now if all the elements of HU are multiplied by all the elements of another coset HV, then

$$h_jUh_\ell V = h_jUh_\ell U^{-1}UV = h_kUV \tag{1.1}$$

since both h_j and $Uh_\ell U^{-1}$ and hence their product are in $\Re$. Thus the multiplication gives rise to the elements of a single coset HUV. In this context, the cosets themselves form a subgroup called the *factor-group* of the invariant subgroup.

Note 1.2.6 It is easy to confuse the factor group with a subgroup. The elements of a subgroup are elements of the group whereas *the elements of the factor group are cosets.*

The cardinality of the different cosets mod H is called the *index* of H in G, generally denoted as $[G : H]$. If G is a finite group, then $[G : H] =\mid G \mid : \mid H \mid$.

We next define the concept of a *solvable* group in general. By a group is meant a group G which has a normal series with Abelian group factors. (What we call a *series* here will bear a new name when we tackle fuzzy subgroups.).

Definition 1.2.7 *A group G is said to be solvable if G has a series of subgroups*

$$\{0\} = G_0 \subset G_1 \subset G_2 \subset \cdots \subset G_m = G$$

where G_i is normal in G_{i+1} and every factor group G_{i+1}/G_i for each $0 \leq i < m$, is Abelian.

From definition (1.2.7) we observe that Abelian groups are solvable, in fact any group of prime-power order is solvable.

Example 1.2.8 S_3, the symmetric group of order 3, is solvable. Take $H_1 = \{e, (1, 2, 3), (1, 3, 2)\}$ and observe that H_1 is a normal subgroup of S_3, and that the factor groups S_3/H_1 and $H_1/\{e\}$ are both Abelian groups with $\mid S_3/H_1 \mid = 2$ and $\mid H_1/\{e\} \mid = 3$. Δ

The same cannot be said about S_n when $n \geq 5$.

The following result is a consequence of definition (1.2.7):

Theorem 1.2.9 *A factor group of a solvable group is solvable.*

Proof. Let G be a group. Let $\{0\} = G_0 \subset G_1 \subset \cdots \subset G_n = G$ be a solvable series, and let H be a normal subgroup of G. Now $\{0\} \subset H \subset G$ is a normal series. Hence the two series have equivalent refinements (see Theorem 2.5.6). Now any refinement of a solvable series is also a solvable series. Hence there exists a solvable series $\{0\} \subset \ldots \subset H \subset \ldots \subset K_{n-1} \subset K_n = G$. We then consider the series $1 = H/H \subset \ldots \subset K_{n-1}/H \subset G/H$ and use the third isomorphism theorem to show

that this series is normal with Abelian natural isomorphism . Thus G/H is solvable.
□

William Burnside was the first to conjecture that a group of odd order is solvable. This conjecture was finally proved more than fifty years later by (Feit and Thomson, 1963) in their lengthy paper [25].

1.3 Isomorphism and Homomorphism

From the way isomorphism has been defined, it is obvious that isomorphic groups must be of the same order.

A not so sharp correspondence between two groups is that of simple *homomorphism*, which resembles isomorphism in every respect with the exception that the correspondence need not be one-to-one.

The correspondence must be such that the product of a and b of G corresponds to the product $a'b'$ of the corresponding elements of G'.

The following points are worth noting as regards isomorphism and homomorphism:

- In a homomorphism, one element $\overline{A}$ of G' may correspond to several different elements of G, hence homomorphism is not a reciprocal property.
- If G is homomorphic to G', then G' is not necessarily homomorphic to G.
- every group is isomorphic to itself. Every group is also homomorphic onto the group which consists only of the identity element $\overline{e}$.

The set of all $x \in G$ mapped by a homomorphism, say f, onto the *zero* of G' is called the *kernel* of f. It is a subgroup K of G and the inverse image of $x' \in G'$ in G is a coset $x + K$ of G. Thus f induces an isomorphism

$$G' \approx G/K \text{ which maps } x' \to x + K \tag{1.2}$$

The consequence is the birth of the following isomorphism theorems [Noether]:

1. $\langle H, K\rangle/K \ \approx H/(H \cap K)$ for all $H, K \leq G$,
2. $G/H \ \approx (G/K)/(H/K)$ if $H, K \leq G$ such that $K \subseteq H \subseteq G$.

1.4 Direct Sums

This is the most important concept in the theory of Abelian groups for the following reasons:

- If a group can be decomposed into a direct sum of subgroups, then in most cases the study of the given group can be reduced to the consideration of groups which are in general of a simple structure;
- New groups can be constructed as direct sums of known groups.

Let A, B be two subgroups of G satisfying:

1. $\langle A, B\rangle = G$, (implying that $g \in G$ may be written in the form $g = a + b$, where $a \in A$ and $b \in B$); and
2. $A \cap B = 0$ (from the fact that if $g = a + b = a' + b'$ with $a' \in A$ and $b' \in B$ then $a - a' = b - b' \in A \cap B = 0$)

Then G is called the direct sum of its subgroups A, B denoted as $G = A + B$.
A subgroup A of G is called a *direct summand* of G if there exists a subgroup B of G such that $G = A + B$, in which case B is called a *complementary direct summand* of A in G.

1.5 p-Groups

The term primary group or a *p-group* refers to a group in which the orders of the elements are powers of one and the same prime p, in which case p is sometimes called a relevant prime for G. As a consequence, we have the following result

Theorem 1.5.1 [29]. *A finite group G is a p-group if and only if $\mid G \mid$ is a power of p.*

A cyclic p-group is of the form $\mathbb{Z}_{p^n}$ for $n \in \mathbb{Z}^+$. It is well known that in a cyclic group, any subgroup is determined uniquely by its order. Hence we state the following theorem.

Theorem 1.5.2 *If G is a finite Abelian p-group and G has a unique subgroup H of order p, then G is cyclic.*

From group theory we know that $\mathbb{Z}_{p^n} \times \mathbb{Z}_{p^m}$ is non-cyclic for any positive integers n and m. For instance a direct product $\mathbb{Z}_p \times \mathbb{Z}_p$ has order p^2 but is not cyclic because it has no element of order p^2; each of its non identity elements has order p. These p-groups are the ones that will be characterized in this thesis.

If two finite Abelian p-groups do not have the same invariants (see Definition 2.2.11), they are not isomorphic.

Chapter 2

Finite Abelian Groups

2.1 Introduction

We address a very important topic in Group theory, the Finite Abelian groups. For flow of content we browse over some topics that enrich the subject. We deliberate on the fundamentals of finite Abelian groups and why is there such a study in the first place. The equivalence relations and partitions are given special attention in their crisp form. We also brush through the class of groups called Basic groups while heading towards a component of algebra called Composition series. Earlier in the literature, Birkhoff posed a problem which was later called the Birkhoff problem: How to classify subgroups of finite Abelian groups. All this and more coming up in this chapter.

2.2 Fundamentals of Finite Abelian Groups

We open this section by stating the so called first main theorem for finite Abelian groups. It has been known since at least the 1870's. Finite Abelian groups are almost completely understood due to the fact that there is a simple structure which describes all of them. Subgroups of finite Abelian groups, however, can be very complicated.

Theorem 2.2.1 [29], [30]. *Every finite Abelian group is a direct product of cyclic groups of prime-power order. The factorization is unique except for the rearrangement of* **factors**.

This theorem shows that every finite Abelian group G is isomorphic to a group of the form $\mathbb{Z}_{p_1^{n_1}} \times \mathbb{Z}_{p_2^{n_2}} \times \cdots \times \mathbb{Z}_{p_k^{n_k}}$, where the p_i's need not be distinct primes and the prime-powers are uniquely determined by G. This process of writing a group in this form is called 'determining the isomorphism class of G'. Moreover, there is one group of order p^k for each set of positive integers whose sum is k. That is, if $k = n_1 + n_2 + \cdots + n_s$ where each $n_i \in \mathbb{Z}^+$, then $\mathbb{Z}_{p^{n_1}} \times \mathbb{Z}_{p^{n_2}} \times \cdots \times \mathbb{Z}_{p^{n_s}}$ is an Abelian group of order p^k.

For any $g \in G$, let

$$G_p = \{g : |g| = p^k\}.$$

We note that the decomposition of G given in the theorem is unique. Hence the subgroup G_p is uniquely identified for any given p. Imagine that G_p has been expressed as a product of cyclic groups in two ways

$$G_p = H_1 \times \ldots \times H_m$$

and as

$$G_p = K_1 \times \ldots \times K_n$$

with the property that $|H_i| \geq |H_j|$ and $|K_i| \geq |K_j|$ whenever $i < j$. Then it can be concluded that the two decompositions are indeed the same.

Definition 2.2.2 *Suppose H and K are groups. The direct product of H and K is the set of all ordered pairs (h, k). Thus if we denote the direct product as $H \times K$ then*

$$H \times K = \{(h, k) : h \in H, k \in K\} \tag{2.1}$$

under the binary operation

$$(h_1, k_1)(h_2, k_2) = (h_1 h_2, k_1 k_2). \tag{2.2}$$

Note: The direct product operation is commutative as well as associative.

Thus $H \times K$ is a group containing $H \times \{1\}$ and $\{1\} \times K$ called the isomorphic copies of H and K, which are also normal to each other.
Definition 2.2.2 shows how to multiply two groups together. How can the reverse be done? That is, given a group how can it be factored? The following theorem suggests a way of factoring a given group. For convenience we include a proof of the result.

Theorem 2.2.3 [74]. *Suppose G is a given group whose normal subgroups are H and K. If $H \cap K = \{e\}$ and $HK = G$, then $G \approx H \times K$.*

Proof. Let $x \in G$. By hypothesis, we have that $HK = G$, and so there exist some $h \in H$ and $k \in K$ such that $x = hk$. This is a unique representation of an element $x \in G$. For if $x = hk$ and $x = h_1k_1$, we have that $hk = h_1k_1 \Longrightarrow h^{-1}h_1 = kk_1^{-1} \in H \cap K$. This means that $h = h_1$ and $k = k_1$.
We proceed to show that $G \approx H \times K$. To do this, let $\phi : G \to H \times K$ be a map defined by $\phi(x) = (h, k)$. We show that ϕ is a homomorphism that is one-to-one and onto. We first show that $\phi(xx_1) = \phi(x)\phi(x_1)$. This is true if $kh_1 = h_1k$ which can be shown to be. For any $h \in H$ and $k \in K$, the equality $kh = hk$ can be shown to hold by showing the commutator $h^{-1}k^{-1}hk$ to be in $H \cap K$. Since H and K are normal, then $h^{-1}(k^{-1}hk) \in H$ and $(h^{-1}k^{-1}h)k \in K$ which proves the commutator is in $H \cap K$. Hence $kh = hk$.
Next assume that $\phi(x) = \phi(x_1)$. This means that $(h, k) = (h_1, k_1)$ and so
$h = h_1, \;\; k = k_1$, hence $hk = h_1k_1$. Lastly for any $(h, k) \in H \times K$ there is an $x \in G$ such that $\phi(x) = (h, k)$. This completes the proof. □

We give the consequent results of Definition 2.2.2 and theorem 2.2.3.

Theorem 2.2.4 *Let $G = H \times K$, and let $H_1 \lhd H$ and $K_1 \lhd K$. Then $H_1 \times K_1 \lhd G$ and*

$$G/(H_1 \times K_1) \approx (H/H_1) \times (K/K_1). \tag{2.3}$$

Definition 2.2.5 *A group G is said to be* cyclic *if there is an element a in G such that*

$$G = \{na : n \in \mathbb{Z}\}.$$

Such an element is called a generator *of G, and we write $G = \langle a \rangle$ to indicate that G is a cyclic group generated by a.*

It is instructive to notice that if group multiplication is understood to be the usual numerical multiplication, the cyclic groups are *all Abelian*.

Theorem 2.2.6 [29]. *Let G be a cyclic group with n elements and generated by a. Let $b \in G$ and let $b = sa$. Then b generates a cyclic subgroup H of G containing n/d elements, where $d = gcd(n, s)$.*

Theorem 2.2.7 [30]. *If a is a generator of a finite cyclic group G of order n, then the other generators of G are elements of the form ra, where $gcd(r, n) = 1$.*

Example 2.2.8 Suppose that $\langle a \rangle, \langle b \rangle$ and $\langle c \rangle$ are cyclic groups of orders 6, 8 and 20 respectively. To find all generators of $\langle a \rangle, \langle b \rangle$ and $\langle c \rangle$ we use the fact that
$U(6) = \{1, 5\}, U(8) = \{1, 3, 5, 7\}$ and $U(20) = \{1, 3, 7, 9, 11, 13, 17, 19\}$.
$U(n) = \{x \in \mathbb{N} : \text{gcd}(x, n) = 1\}$
Thus,

$$\begin{aligned} \langle a \rangle &= \langle 5a \rangle \\ \langle b \rangle = \langle 3b \rangle &= \langle 5b \rangle = \langle 7b \rangle \\ \langle c \rangle = \langle 3c \rangle &= \cdots = \langle 19c \rangle \end{aligned}$$

Δ

The following result appears, with its proof, in [30]:

Theorem 2.2.9 *For each divisor k of n, the group $\langle a \rangle$ has exactly one subgroup of order k which is $\langle \frac{n}{k} a \rangle$.*

Proof. Let k be any divisor of n. Now $k(\frac{n}{k}a) = na = e$ and $t(\frac{n}{k}a) \neq e$.
claim: $\langle (\frac{n}{k}a) \rangle$ is a unique subgroup of order k.

To verify our claim, we let H be any subgroup of order k. Now $H = \langle ma \rangle$ for any least positive integer m such that $ma \in H$. By the division algorithm, there exist integers q and r such that $n = mq + r$ where $0 \leq r < m$. Then we have $na = (mq + r)a$ so that $ra = -q(ma) \in H$. This implies that $r = 0$ and so $n = mq$. So $k =\mid H \mid=\mid \langle ma \rangle \mid= n/m$. It follows that $m = n/k$ and so $H = \langle ma \rangle = \langle \frac{n}{k} a \rangle$. □

In general, a generating element of a cyclic group is called a *primitive* element of this group. Thus $G = \langle a \rangle$ implies that a is the primitive element of G.
Suppose a cyclic group of order m is given as follows

$$\mathbb{Z}_m = \{\alpha\} \text{ so that } \mid \alpha \mid= m > 0. \tag{2.4}$$

In this case α is a primitive element of $\mathbb{Z}_m (m > 0)$. Now for the finite cyclic group $\mathbb{Z}_m$ we have that

$$k\alpha = \ell\alpha \text{ if and only if } k \equiv \ell (\text{mod} m), \tag{2.5}$$

for which

$$k\alpha = e \text{ if and only if } m \mid k. \tag{2.6}$$

is a special case, where e is the identity element.
Now, α^k is a primitive element of $\mathbb{Z}_m$ if and only if $gcd(k, m) = 1$.

Note 2.2.10 Note that according to (2.5) the number of primitive elements of $\mathbb{Z}_m$ is given by Euler's function.
Whereas other cyclic groups of finite order are decomposable, the cyclic groups of prime-power order are indecomposable.

Definition 2.2.11 *Suppose G is an Abelian group of order p^n where p is a prime number. If $G = H_1 \times H_2 \times \cdots \times H_k$ where each H_i is cyclic of order p^{n_i} with $n_1 \geq n_2 \geq \cdots \geq n_k > 0$, the integers $n_1, n_2, \cdots, n_k$ are then called the* invariants *of a group G.*

Suppose we have

$$G = \mathbb{Z}_1 \times \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_s. \tag{2.7}$$

Since these $\mathbb{Z}_i's$ are indecomposable, we call them the invariants of the finite Abelian group G since their orders $\mid \mathbb{Z}_1 \mid, \ldots, \mid \mathbb{Z}_s \mid$ are defined in one and the only one way. Now (2.7) can be written in the form $G = \{\alpha_1\} \times \{\alpha_2\} \times \cdots \times \{\alpha_s\}$ in which a primitive element α_1, α_s describes each of the direct factors, hence α_1, α_s is called a prime-power basis of the finite Abelian group G.

([Redei, 1967]) Let G be a finite Abelian p-group with n equal invariants p^k. If α_1, α_n is a basis of G, then all its bases $\omega_1, \ldots, \omega_n$ are given by $\omega_i = \alpha_1^{a_{i1}} \ldots \alpha_n^{a_{in}}$ $(i = 1, \ldots, n)$ where a_{ij} are such that their determinant $det(a_{ij})$ is not divisible by p.

For any prime p, $(\mathbb{Z}_p, +)$ is a finite Abelian group whose only subgroups $\{0\}$ and $\mathbb{Z}_p$ itself form a *chain* $\{0\} \subset \mathbb{Z}_p$ with only two components.

A chain is said to be *maximal* if it cannot be refined anymore.

Every finite Abelian group can be expressed as a direct product of cyclic groups of orders $n_1, n_2, \ldots, n_r$ where $n_{i+1} \mid n_i, \;\; i = 1, 2, \ldots, r-1$. Also, every finite Abelian group is isomorphic to some direct product of cyclic groups of prime-power order. This can be shown by choosing, for each distinct prime, the largest factor of that prime-power and forming one factor of some order,n_1 say, from all of these. Repeating the process (until all the factors have been considered) with the remaining original factors to obtain a factor of some other order,n_2 say, and using the fact that each prime divisor of n_2 also divides n_1 implying $n_2 \mid n_1$, gives the result.

Example 2.2.12 If

$$G \;\; \approx \mathbb{Z}_{27} \times \mathbb{Z}_3 \times \mathbb{Z}_{125} \times \mathbb{Z}_{25} \times \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \tag{2.8}$$

then

$$G \;\; \approx \mathbb{Z}_{3^3 5^3 2^2} \times \mathbb{Z}_{3 5^2 2} \times \mathbb{Z}_2.$$

Δ

The following are some of the important results pertaining to the study of finite Abelian groups:

Lemma 2.2.13 *If G is a finite Abelian group whose order is divisible by a prime p, then G contains an element of order p.*

Theorem 2.2.14 (Cauchy's) *Suppose G is a finite group whose order is divisible by a prime p. Then G contains at least one element of order p.*

Theorem 2.2.15 [29], [74]. *If G is a group of order p^2 where p is a prime number, then G is Abelian.*

Theorem 2.2.16 [74]. *A finite Abelian group H is cyclic if and only if its invariants are pairwise relatively prime.*

Another way of looking at a finite Abelian group is to notice the following description:

For each finite Abelian group $G \neq 0$ there is a unique list of integers $m_1, \ldots, m_k$, where each $m_i > 1$ and each is a multiple of the next, satisfying the isomorphism $G \approx \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_k}$. The product $m_1 m_2 \cdots m_k$ is the order of G.

The list $m_1, \ldots, m_k$ is called the list of invariant factors of the Abelian group G.

Note 2.2.17 The above description implies that two finite Abelian groups are isomorphic if and only if their invariant factors are the same.

For, let G and G' be Abelian groups of order p^n defined as follows:

$G = H_1 \times H_2 \times \cdots \times H_r$ where each H_i is cyclic of order p^{n_i} with

$$n_1 \geq n_2 \geq \cdots \geq n_r > 0$$

and

$G' = K_1 \times K_2 \times \cdots \times K_s$ where each K_i is cyclic of order p^{m_i} with

$$m_1 \geq m_2 \geq \cdots \geq m_s > 0.$$

Define a map $\phi : G \to G'$ by $\phi(h_1^{\alpha_1} h_2^{\alpha_2} \cdots h_r^{\alpha_r}) = (k_1)^{\alpha_1}(k_2)^{\alpha_2} \cdots (k_r)^{\alpha_r}$. Then ϕ is an isomorphism , thus, $r = s$ and for each $i, n_i = m_i$.

The other way round is to show that groups G and G' that have the same invariants are isomorphic.

2.3 Basic Subgroups

The notion of basic subgroups and its importance for the general theory of Abelian p-groups was introduced by Kulikov. The driving factor in this section is the observation that a p- group cannot always be decomposed into a direct sum of cyclic groups.

Definition 2.3.1 *A subgroup H of a p-group G is called a basic subgroup if it satisfies the following conditions:*

1. *H is a direct sum of cyclic groups*
2. *H is pure[1] in G*
3. *G/H is divisible.*

On this note we give the following result:

Theorem 2.3.2 (Kulikov) *Every torsion group G contains a basic subgroup.*

Proof. By showing that every p-primary group has a basic subgroup, it follows from the primary decomposition that every torsion group contains a basic subgroup. □

We define what is meant by a height of an element of a p-group G.

Definition 2.3.3 *The equation $p_n^k x = a$ in which p_n is fixed, $k \in \mathbb{Z}^+$ and a is an arbitrary nonzero element of a group G, may or may not have solutions in G. The greatest nonnegative integer k for which the equation is solvable is called the* height *of a at the prime p_n.*

Before we deal with basic subgroups, it is important to be reminded in passing about important results concerning cyclic groups. The relevance of the theory of cyclic groups to the study of Abelian groups cannot be underemphasized. *"Although cyclic groups constitute a very narrow class of finite groups, they play the role of building blocks for all finite Abelian groups in much the same way that primes are*

[1] A subgroup H of G is said to be pure in G in case, for every integer n, $nG \cap H = nH$.

the building blocks for the integers and that chemical elements are the building blocks for the chemical compounds", Gallian [30].
Many results stated hereunder are due by Kulikov himself. Let G be a direct sum of cyclic p-groups. The following result gives a criterion for a p-group to be a direct sum of cyclic groups.

Theorem 2.3.4 (Kulikov) *A p- group G is a direct sum of cyclic groups provided it is the union of an ascending chain of subgroups $G_n (n = 1, 2, \ldots)$ in such a way that the heights of the nonzero elements in G_n remain under some finite bound k_n.*

In his study, Kulikov further came up with the following results:

Theorem 2.3.5 *The subgroups of direct sums of cyclic groups are themselves direct sums of cyclic groups.*

Theorem 2.3.6 *Any two direct decompositions of a group which is a direct sum of cyclic groups have isomorphic refinements.*

Closer to the results above, we have the following consequence:

Corollary 2.3.7 *Let G be a group. Then G is a union of a sequence of subgroups*

$$G_1 \subset G_2 \subset \cdots \subset G_n \subset \cdots$$

arranged in ascending order, where each G_i is a direct sum of cyclic groups.

More results in this topic can be found in [26].

2.4 Equivalence Relations and Partitions

Things that are considered different in one context may be viewed as equivalent in another context.
We investigate the relationship between partition and equivalence relation.
A relation $\Re$ on a set A is an *equivalence relation* if it is *reflexive, symmetric*, and *transitive.*

Definition 2.4.1 *Given a set A and an index set I, let $\emptyset \neq A_i \subseteq A$ for each $i \in I$. Then $\{A_i\}_{i \in I}$ is a partition of A if:*

1. $A = \cup_{i \in I} A_i$

2. $A_i \cap A_j = \emptyset, \ \ i, j \in I, \ \ i \neq j,$

where each set A_i is called a block of the partition.

Definition 2.4.2 *Let $\Re$ be an equivalence relation on a set A. For any $x \in A$, the equivalence class of x denoted by $[x]$ is defined by*

$$[x] = \{y \in A \mid y \ \Re \ x\}. \tag{2.9}$$

Consequently, we have the following result which is not difficult to show:

Theorem 2.4.3 *If $\Re$ is an equivalence relation on a set A, and $x, y \in A$, then*

1. $x \in [x]$,

2. $x \ \Re \ y$ *if and only if* $[x] = [y]$,

3. $[x] = [y]$ *or* $[x] \cap [y] = \emptyset$.

Note 2.4.4 If $\Re$ is an equivalence relation on A, then by 1 and 3 above, the distinct equivalence classes determined by $\Re$ form a partition of A.

The theory of partitions is widely applicable as the following discussion illustrates. Let $S(n, k)$ denote the number of partitions of an n-set A into k parts, where $1 \leq k \leq n$. ($S(n, k)$ are popularly known as Stirling numbers of the second kind). Then the following are true:

1. $S(n, 1) = 1$,

2. $S(n, n) = 1$,

3. $S(n, k) = S(n-1, k-1) + kS(n-1, k), \ \ (2 \leq k \leq n-1)$

The Stirling numbers of the second kind can be computed from the sum

$$S(n, k) = \frac{1}{k!} \sum_{i=0}^{k-1} (-1)^i \binom{k}{i} (k-1)^n, \tag{2.10}$$

or the generating function

$$x^n = \sum_{m=0}^{n} S(n,m)(x)_m = \sum_{m=0}^{n} S(n,m)x(x-1)\cdots(x-m+1), \tag{2.11}$$

and various other forms.

The above properties can be used to show that

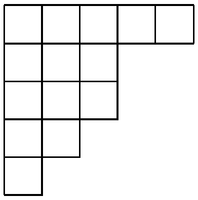
$$S(n,2) = 2^{n-1} - 1, \text{ and } S(n,n) = \binom{n}{2}. \tag{2.12}$$

Suppose also that a partition of an n-set A is given, $A = A_1 \cup A_2 \cup \cdots \cup A_n$, there exists a corresponding equation $n = n_1 + n_2 + \cdots + n_k$, where n_i is the size of A_i, $(1 \leq i \leq k)$ referred to as a partition of the integer n into k parts, $n_i \neq 0$.

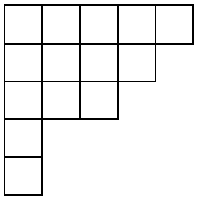
The standard notation for partitions of a positive integer n, to be followed throughout this work involves counting the number of blocks of each size. In this context, for instance, if there are α_i parts of size i then the partition is written as $1^{\alpha_1}2^{\alpha_2}\cdots n^{\alpha_n}$.

The calculation of the number $p(n)$ of partitions of n is not a simple matter. Some techniques involve the use of *generating functions.* It is often useful to use a diagrammatic representation of partitions popularly called a Young diagram which is very handy in proving theorems about partitions.

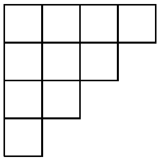
Using diagrammatic representation, it is possible to transform one partition, say λ into another,say λ', by simply switching the rows and columns. Such λ'^s are said to be *conjugate.* In essence, we say, pairs of partitions for a single number whose Young diagrams transform into one another when flipped about the line $y = -x$ while fixing the upper left box are called conjugate partitions. It is possible that this process results in no change in the original partition as observed in the diagrams below. We thus say that λ is self-conjugate if $\lambda = \lambda'$.



$\lambda = (5,3,3,2,1)$



$\lambda' = (5,4,3,1,1)$



(self-conjugate)

$\lambda = \lambda' = (4, 3, 2, 1)$

The partitions on a number n correspond to the set of solutions $(j_1, j_2, \ldots, j_n)$ to the *Diophantine equation* $1j_1 + 2j_2 + 3j_3 + \cdots + nj_n$.

Example 2.4.5 The partitions of five are given by

$$\{(5), (4, 1), (3, 2), (3, 1, 1), (2, 2, 1), (2, 1, 1, 1), (1, 1, 1, 1, 1)\}.$$

It corresponds to the solutions

$$(j_1, j_2, j_3, j_4, j_5) = (0, 0, 0, 0, 1), (1, 0, 0, 1, 0), (0, 1, 1, 0, 0), (2, 0, 1, 0, 0),$$

$$(1, 2, 0, 0, 0), (3, 1, 0, 0, 0), (5, 0, 0, 0, 0).$$

Δ

2.5 Composition Series

Before we venture into the discussion about *composition series*, we begin by explaining the critical terms necessary in the proper definition of the composite series.
The first term we define is what is meant by a *simple group.*
A group is *simple* if it has no proper normal subgroups. The only simple Abelian groups are the $\mathbb{Z}_p$, where p is a prime.
A group is said to be *solvable* if it contains a normal series with commutative factors.
Next we need to know what is meant by a *subnormal series.*

Definition 2.5.1 *A* **subnormal series** *of a group G is a* chain *of subgroups* $\{0\} = G_0 < G_1 < \cdots < G_n$ *such that* $G_i \triangleleft G_{i+1},\ \ 0 \leq i \leq n.$ *The* factors *of the* *series are the quotient groups $G_{i+1} \mid G_i$. The* length *of the series is the number of non identity factors.*

Note: *A subnormal series such that $G_i \lhd G$, for all i, is said to be normal.*

Definition 2.5.2 *By a* **refinement** *of a series S is meant a series obtained from S by successive insertions of an additional subgroup properly between two successive subgroups of the series.*

With all this in hand we are ready to discuss the composition series.

Definition 2.5.3 *A* **composition series** *for a group G is a subnormal series in which all the factors are simple or equal to 1. In fact it can be said that a composition series is a subnormal series with no* refinements *except itself.*
Alternatively, a **normal series** $\{0\} = G_0 \subset G_1 \subset G_2 \subset \cdots \subset G_n = G$ *of the group G is called a composition series if each G_i is maximal subject to being normal in G_{i-1}, in which case the composition factors Gi/G_{i-1}, $1 \leq i \leq n-1$ are simple.*

In this regard we are reminded of the two important theorems concerning composition series. The first is due to Schreier:

Theorem 2.5.4 *Every normal series with distinct members can be refined to a composition series.*

The second is a well-known Jordan-Holder theorem:

Theorem 2.5.5 *Any two composition series of G have the same length and the corresponding composition factors are pairwise isomorphic up to permutation.*

Schreier also proved the following result:

Theorem 2.5.6 [26], [35]. *Any two normal series of an arbitrary group G have equivalent refinements.*

Proof. Assume

$$\{0\} = G_0 \subset G_1 \subset G_2 \subset \cdots \subset G_n = G \qquad (2.13)$$

$$\{0\} = H_0 \subset H_1 \subset H_2 \subset \cdots \subset H_m = G \qquad (2.14)$$

are normal series. We insert the groups $G_{i+1}(G_i \cap H_j)$ and $H_{j+1}(H_j \cap G_i)$ in first and second equations respectively to obtain normal series with mn inclusions, where $0 \leq i \leq n$ and $0 \leq j \leq m$. Hence we have

$$\cdots \subset G_{i+1}(G_i \cap H_j) \subset G_{i+1}(G_i \cap H_{j+1}) \subset \cdots \tag{2.15}$$

$$\cdots \subset H_{i+1}(H_j \cap G_i) \subset H_{j+1}(H_j \cap G_{i+1}) \subset \cdots \tag{2.16}$$

These can be seen to be the refinements of (2.13) and (2.14) above in the following way: (2.15) is a refinement of (2.13) by taking $j = m$, and also since given any j there exists an index i with $G_i \subset H_j \subset G_{i+1}$ such that $H_j = G_{i+1}(G_i \cap H_j)$ to refine (2.14).

The same can be said about (2.16). By isomorphism, the result follows.(see Zassenhaus Lemma in Appendix I). □

Chapter 3

Finite Abelian p-Groups of Rank Two

3.1 Introduction

The process of drawing the subgroup lattice of a given finite Abelian p-group, or finding the number of subgroups of a finite Abelian group is a difficult task. Similar works on this problem were carried out by authors such as [70], [81], [83], to name a few, and even earlier.

In this chapter we try to describe a simpler method that addresses this task. In our first problem we will develop the tree diagrams of subgroups of a finite Abelian p-group in question which will be followed by stating the procedure which accomplishes this. In our second problem we will describe which outstanding subgroups are to be added to the tree to form a subgroup lattice. Finally we will count the number of subgroups of a finite Abelian p-group of rank two.

3.2 The Structure of the Group

We open this section by giving the following illustrative result found in group theory. **If a is a generator of a finite cyclic group G of order n, then the other generators of G are the elements of the form ra, where r is relatively prime to n.**

Example 3.2.1 Consider the problem of finding all the subgroups of $\mathbb{Z}_{20}$ and giving their lattice diagram.

All subgroups of $\mathbb{Z}_{20}$ are cyclic, and $1, 3, 7, 9, 11, 13, 17, 19$ are all generators of $\mathbb{Z}_{20}$. The subgroup generated by 2,

$$\langle 2 \rangle = \{0, 2, 4, 6, 8, 10, 12, 14, 16, 18\}$$

is of order 10 and has as generators elements of the form $k2$, where k is relatively prime to 10, namely, $k = 1, 3, 7, 9$, so $k2 = 2, 6, 14, 18$. The element 4 of $\langle 2 \rangle$ generates $\{0, 4, 8, 12, 16\}$ and 8,12,16 also are generators of this group.

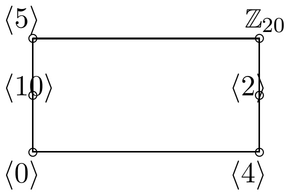
So far we have found all subgroups generated by

$$0, 1, 2, 3, 4, 6, 7, 8, 9, 11, 12, 13, 14, 16, 17, 18, 19.$$

We are just left with $5, 10, 15$ to consider.

$$\langle 5 \rangle = \{0, 5, 10, 15\}$$

and 15 also generates this group of order 4, since $15 = 3.5$ and $(3, 4) = 1$. Lastly $\langle 10 \rangle = \{0, 10\}$. We have exhausted the number of subgroups. Therefore the diagram for $\mathbb{Z}_{20}$ is



A finite Abelian group of rank two is a finite group G of the form $\mathbb{Z}_{p^n} \times \mathbb{Z}_{q^m}$ where p and q are prime numbers, while m and n are any natural numbers. The subgroups of any cyclic group of prime-power order form a chain. The cyclic nature of G determines the nature of the primes under consideration thus,

$$G \text{ is cyclic, if and only if } p \neq q \tag{3.1}$$

otherwise,

$$p = q, \text{ whenever } G \text{ is non-cyclic.} \tag{3.2}$$

The latter case indicates that $G = \mathbb{Z}_{p^n} \times \mathbb{Z}_{p^m}$ which is a p-group, and is the one to be discussed in this work.

3.2.1 Tree diagrams of Subgroups

We describe the tree diagrams for selected examples of groups (consistent with existing literature), including the well-known groups like, for instance, the Klein group. Conventionally, a line segment between two subgroups will mean that the subgroup generated on the left is entirely contained in the subgroup generated on the right, while the generators on the same level mean that the generated subgroups have the same order and are disjoint.

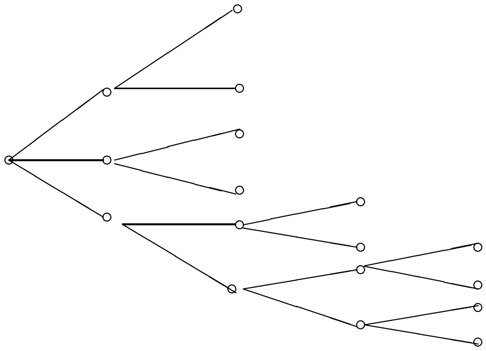
3.2.2 General Procedure

We write ab to mean $(a, b) \in \mathbb{Z}_{p^n} \times \mathbb{Z}_{p^m}$, where p is prime, and $n, m \in \mathbb{Z}^+$. We develop the cyclic subgroups of $\mathbb{Z}_{p^n} \times \mathbb{Z}_{p^m}$ with the property that $h(a, b) = (ha \mod p^n, hb \mod p^m)$, $h \in \mathbb{N}$, and $|(a, b)| = lcm\ (|a|, |b|)$, (see example 3.3.4). Some elements will generate the same subgroups. As in group theory requirements, we choose representative subgroup generators and arrange them in the form of a tree diagram according to the order of subgroups they generate. All subgroup generated in this process are cyclic. Lemma 3.3.5 can be used to count the number of subgroups that should be there for each order.

3.2.3 Observations

In all cases, the identity is contained in $p + 1$ subgroups of order p, which in turn are contained in subgroups of order p^2. After this each subgroup is contained in p subgroups of the next higher order, and the procedure repeats up to the index of p^m.

We choose to name the bottom branch of the tree the *characteristic branch*, while the upper branch we call the *top branch.* The process of splitting explained above happens for m times. The difference between the values of n and m tells how many times the characteristic branch has to proceed after m times. After this the process terminates and in this way the tree diagram of cyclic subgroups has been generated. For illustration of the process, see the diagram below for the case $\mathbb{Z}_{2^4} \times \mathbb{Z}_{2^2}$.



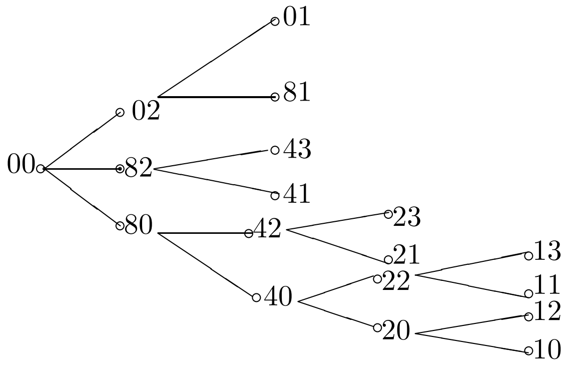
Now that the tree diagram has been generated, we are in the process of naming the maximal chains occurring in the lattice diagrams of p-groups. Before we explain the process of the formation of lattice diagrams, we do almost half the job by giving names to the cyclic subgroup generators found in tree diagram.

3.2.4 Labeling of the Tree Diagram

We describe a unique method of naming the subgroup generators. (This is the author's description). The generators are given labels in order from the right most node, bottom of the characteristic branch in the following way:
$10, p0, p^20, \ldots, p^{n-1}0, 00$. Next all the nodes, except those on the top branch, whose roots are those named above are obtained in the following manner: For each root find the label of one of its nodes by dividing the root by p. Then find the rest by fixing the first coordinate of the *determined* node label for all while adding a factor of the form αp^{m-1} to the second coordinate of the *determined* label, where $\alpha = 0, \ldots, p-1$.

Finally we label the top branch in this way: $00, 0p^{m-1}$ and divide $0p^{m-1}$ by p to get the rest along the main branch of the top branch. Now with these roots, find the label of one of its nodes as described above (but add a factor αp for the second coordinate of the rest). To illustrate this process we give the following example:

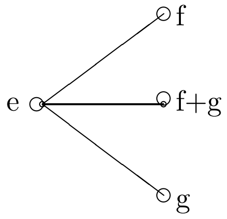
Example 3.2.2 Consider the group $G = \mathbb{Z}_{2^4} \times \mathbb{Z}_{2^2}$.



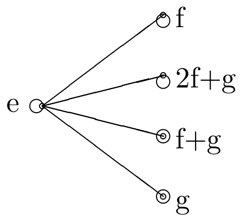
We give a version of labelling as found in group presentations. This labelling agrees with ours in every sense.

Examples 3.2.3

1. Consider the Klein group $G = \mathbb{Z}_2 \times \mathbb{Z}_2 = \{e, f, g, f+g : 2f = 0 = 2g\}$. All the elements of this group, except the identity, generate subgroups of the same order that are disjoint. Hence G has a tree diagram

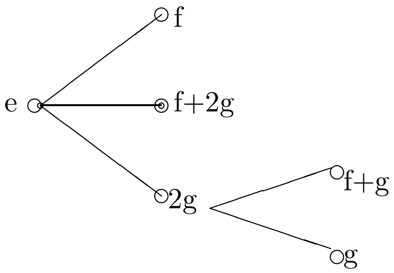


2. The group $G = \mathbb{Z}_3 \times \mathbb{Z}_3 = \{e, f, g, 2f, f+g, 2f+g, 2g, f+2g, 2f+2g : 3f = 0 = 3g\}$ has some of its members generating identical subgroups, as can be easily checked algebraically (see example 2.2.8). Hence G has the diagram

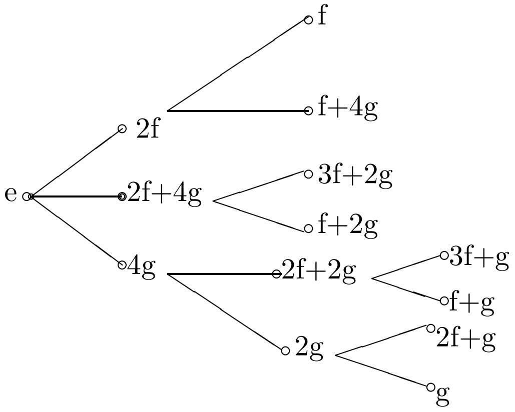


As we get closer to the algorithm, we give some more examples

3. The group $G = \mathbb{Z}_4 \times \mathbb{Z}_2 = \{e, f, g, f+g, 2g, f+2g, 3g, f+3g : 2f = 0 = 4g\}$ has the diagram



4. The group $G = \mathbb{Z}_8 \times \mathbb{Z}_4 = \langle f, g : 4f = 0 = 8g \rangle$ has the diagram



Note 3.2.4 All the subgroups generated at this stage are cyclic. The number of cyclic groups at each level can be verified by the check illustrated in example 3.3.4.

Theorem 3.2.5 *The number of subgroups of order p^β in a group of order $p^\alpha \equiv 1(mod p)$.*

Example 3.2.6 The number of subgroups of order 25 in a group of order $125 \equiv 1(\text{mod}\,5)$. If the group is $\mathbb{Z}_{25} \times \mathbb{Z}_5$ and x is the number of subgroups, then $x \equiv 1(\text{mod}\,5)$, that is $x - 1 = 5t$ for some t. Hence $x = 6$ is the required number of subgroups of order 5 in the given group. Δ

We proceed to the development of lattice diagrams.

3.3 Subgroup Lattices

Definition 3.3.1 *A* **subgroup lattice** *is a diagrammatic illustration which describes the relationship between the various subgroups of a group. All the subgroups of a group are included in a lattice diagram with the property that a subgroup H at one level is connected to a subgroup K at a higher level by means of a sequence of line segments, provided H is properly contained in K.*

Consequently there are more than one ways to draw a subgroup lattice, but the fundamental thing is that the connection between the subgroups must be the same.

3.3.1 Primary Decomposition

As mentioned in the introduction above, the process of determining the subgroup lattice of a given finite Abelian group is a difficult task. However, the method of breaking down the group into its components (or factors) and working from the properties of the latter reduces the burden. This process is called *decomposition.*
To illustrate this fact, consider a finite Abelian group G. Let n be the order of G, where $n = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$. We call $|G| = n = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$ the decomposition of the order of G into prime power factors.
Suppose $G = G_{p_1} \times G_{p_2} \times \cdots \times G_{p_k}$ is the corresponding primary decomposition. Then there is a one-one correspondence between the subgroup lattice of G and the direct product of the corresponding subgroup lattices.

Definition 3.3.2 (Product of Subgroup Lattices) *Suppose L and M are the two subgroup lattices with $\ell \in L$ and $m \in M$. By the product of L and M we mean*

$$L \times M = \{(\ell, m) \mid \ell \in L, m \in M\}$$

with the property that

$$\begin{aligned} (\ell_1, m_1) &\leq (\ell_2, m_2) \text{ if and only if} \\ \ell_1 &\leq \ell_2 \text{ and} \\ m_1 &\leq m_2 \end{aligned}$$

If $L(G)$ denotes the subgroup lattice of G, then

$$L(G) \approx L(G_{p_1}) \times L(G_{p_2}) \times \cdots \times L(G_{p_k}), \tag{3.3}$$

(see Suzuki, 1951). This process reduces the problem to p-groups and works both ways. That is, given the subgroup lattices of the primary components, then the direct product of such lattices can be constructed from which the subgroup lattice $L(G)$ can be inferred.

3.3.2 Number of Subgroups

The counting of subgroups of Abelian groups was started as early as in the 1930's by G. Birkhoff. People became interested in this kind of work and the contributions began to flow.

We explain how we use the tree diagrams of subgroups to arrive at the total number of subgroups for the specific cases. Before we do so, we make the following note:

Note 3.3.3 (Butler, 1991) A finite Abelian p-group is said to be of type $\lambda = (\lambda_1, \ldots, \lambda_k)$ if it is isomorphic to the direct product of cyclic groups $\mathbb{Z}_{p^{\lambda_1}} \times \cdots \times \mathbb{Z}_{p^{\lambda_k}}$, where $\lambda_1 \geq \cdots \geq \lambda_k$ and λ is a partition of n.

3.3.3 Hall Polynomial

Hall started his process of subgroup counting. He studied the subgroups H of type μ of a finite Abelian p-group G of type λ which have the property that G/K is of type ν. He proved that the number of such subgroups was a polynomial in p with integral coefficients. The polynomial is called a *Hall polynomial* and is denoted by $g^{\lambda}_{\mu\nu}$. Hall also found the degree of this polynomial together with its leading coefficient, and further showed that $g^{\lambda}_{\mu\nu} = g^{\lambda}_{\nu\mu}$.

The following example will be useful in illustrating the counting of vertices and edges in any graph of $\mathbb{Z}_{p^n} \times \mathbb{Z}_{p^m}$ form.

Example 3.3.4 The number of cyclic subgroups of order p in $\mathbb{Z}_{p^2} \times \mathbb{Z}_p$ can be found by counting the number of elements using the fact that $\mid (a, b) \mid = p = \operatorname{lcm}(\mid a \mid, \mid b \mid)$.

This requires that both $| a |$ and $| b |$ be p or $| a |= p$ and $| b |= 1, p$ and vice versa. The first case yields $(p-1)^2$ elements, while the second case yields $2(p-1)$ elements of order p. But each cyclic subgroup of order p has $p-1$ elements of order p no two of which have an element of order p in common. Thus $\mathbb{Z}_{p^2} \times \mathbb{Z}_p$ has $p+1$ cyclic subgroups of order p.

By similar argument, $\mathbb{Z}_{p^2} \times \mathbb{Z}_p$ has p cyclic subgroups of order p^2. Δ

For the following case of m, we note the following

Lemma 3.3.5 *The number of cyclic subgroups of order p^2 in $\mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2}$ is $p^2 + p$.*

Proof. For $(a, b) \in \mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2}$ we have $| a |= p^2 =| b |$ implying $p^2 - p$ choices for a and b resulting in $(p^2 - p)^2$ elements of order p^2. Also when $| a |= p^2, \ | b |= 1, p$ we have $(p^2-p)(p-1)+(p^2-p)$ choices for a and b accordingly. Similarly $| a |= 1, p, \ | b |= p^2$ yields $(p^2 - p) + (p^2 - p)(p - 1)$ elements of order p^2.

But each cyclic subgroup of order p^2 has $p^2 - p$ elements of order p^2. Thus $\mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2}$ has

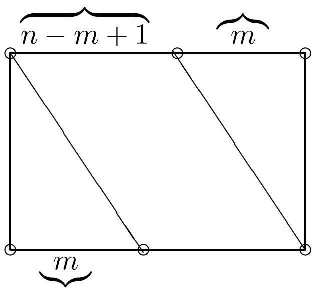
$$\frac{2[(p^2 - p)(p - 1) + (p^2 - p)] + (p^2 - p)}{(p^2 - p)} = (p^2 + p)$$

cyclic subgroups of order p^2. □

3.3.4 Tree Orientation

The finite Abelian group in question, i.e $G = \mathbb{Z}_{p^n} \times \mathbb{Z}_{p^m}$, is noncyclic, hence, apart from cyclic subgroups, it contains noncyclic subgroups as well. To recover some of the outstanding noncyclic subgroups once a cyclic subgroup tree-diagram is known, our method involves the orientation of the discovered tree-diagram about 180^0 to create symmetry. Most noncyclic subgroups are recovered in this way with the exception of a few as will be illustrated.

In a lattice, the subgroups of the same order are said to be on the same **level**. Thus each lattice of G has $n + m + 1$ levels, with the identity on the first and the whole group on the $n + m + 1$-th level. The number of subgroups at each order is observed to grow from 1 in monic polynomial order up to the degree of m, levels up for $n-m+1$ times then decreases in monic polynomials again. In fact all the terms of the polynomials have coefficients of 1. This process is best illustrated by the figure below.



The non-cyclic subgroups appear in every level except the first two. The non-cyclic subgroups too occur in increasing polynomial order with effect from the level after the first two up to a polynomial of degree $m-1$, repeat the number at degree $m-1$ for $n-m+1$ times before decreasing.

This description makes it easy to count the number of subgroups in each lattice diagram. We use this description together with the knowledge of example 3.3.4 to count the number of ordinary subgroups of a group G.

We next account for the missing edges as well as some subgroup generators. To do so we need to consider the groups for various cases of positive integers n and m.

Case 1: Let $m=1$ and let n be any positive integer. We are dealing with groups of the form $\mathbb{Z}p^n \times \mathbb{Z}_p$. Generally for these groups all the generators at this stage have been accounted for by the tree inversion. We need only account for the missing edges. When $n=1$, nothing is missing, that is all the edges and generators are there. When $n=2$, only one edge is needed, and can be denoted by $\{p0, \langle 01, p0\rangle\}$. When $n=3$, two edges are missing. They are given by

$$\{p^2 0, \langle 01, p^2 0\rangle\} \text{ and } \{p0, \langle 01, p0\rangle\}.$$

In general, in $\mathbb{Z}p^n \times \mathbb{Z}_p$ for $n>1$, there are $\{p^i 0, \langle 01, p^i 0\rangle\}_{i=1}^{n-1}$ missing edges to be accounted for after tree inversion.

Case 2: Let $m = 2$ and let n be any positive integer, such that $n \geq m$. For these groups and the higher, some generators as well as some edges are missing. We describe one set, and the corresponding follow by reflection about symmetry. When $n = 2$, only one generator is missing, this is $\langle 0p, p0\rangle$. The missing edge set is given by $\{[p\alpha p; 0p], \langle 0p, p0\rangle\}$ for $\alpha = 0, \ldots, p-1$. By reflection about symmetry we discover a corresponding set of edges. When $n = 3$, the following set of edges is missing: $\{[p^2\alpha p; 0p], \langle 0p, p^20\rangle\}$ and $\{[p\alpha p; \langle 0p, p^20\rangle], \langle 0p, p0\rangle\}$ together with their reflections.

The following trend is followed for $n > 3$. The missing edges are given by set:

$$\{[p^3\alpha p; 0p], p^30\}; \{[p^2\alpha p, \langle 0p, p^30\rangle], \langle 0p, p^20\rangle\};$$

and $\{[p\alpha p; \langle 0p, p^20\rangle], \langle 0p, p0\rangle\}$ for $\alpha = 0, \ldots, p-1$ together with their reflections about symmetry.

On the other hand the missing generators are all given by $\langle 0p, p^i0\rangle$ for

$i = 1, \ldots, n-1$.

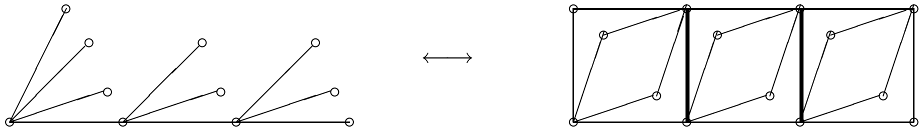
In general for groups of the form $\mathbb{Z}p^n \times \mathbb{Z}_{p^2}$, the missing edges are given by the following sets, together with their reflections about symmetry:

$$\{[p^{n-1}\alpha p; 0p], \langle 0p, p^{n-1}0\rangle\}; \{[p^i\alpha p; \langle 0p, p^{i+1}\rangle], \langle 0p, p^i0\}_{i=1}^{n-1},$$

and for $\alpha = 0, \ldots, p-1$.

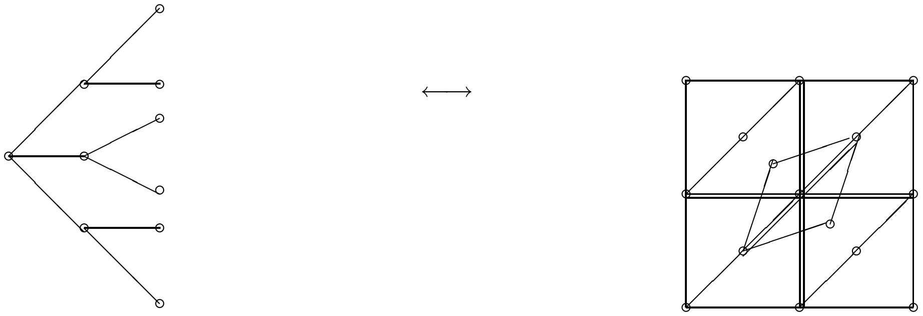
The process carries on until all possible cases have been considered.

Example 3.3.6 Consider the reflection of the tree diagram for $\mathbb{Z}_{3^3} \times \mathbb{Z}_3$. The missing edges are $\{3^20, \langle 01, 3^20\rangle\}$; and $\{30, \langle 01, 30\rangle\}$, while there are no missing generators.



Example 3.3.7 The reflection of a tree diagram for $\mathbb{Z}_4 \times \mathbb{Z}_4$ has the following missing generators and edges: one generator $\langle 02, 20\rangle$, and the edges

$\{20, \langle 02, 20\rangle\}; \{22, \langle 02, 20\rangle\}$.



The other cases can be explained similarly. Δ

We next give a concise overview of Fuzzy Set Theory, and lay out some material necessary for the discussion of the topic of this thesis.

Chapter 4

Fuzzy Group Theory

4.1 Introduction

Let X be a non-empty set. Crisp subsets of X are characterized by a function $\chi_A \in \{0,1\}^X$, for $A \subseteq X$, which is defined as follows:

$$\chi_A(x) = \begin{cases} 1 & \text{if} \quad x \in A \\ \\ 0 & \text{if } x \notin A \end{cases} \tag{4.1}$$

where the relation $\in$ has the property that for each $x \in X$, either $x \in A$ or $x \notin A$. However, if the set X is a representation of some collection of objects in the real world whereby A has no definitive condition on elements belonging to A, then the statement $x \in A$ cannot be declared to be either true or false with absolute certainty. This is what prompted the development of a fuzzy set, a concept introduced by Zadeh in [89]. In his definition, a fuzzy set is simply an element of I^X where $I = [0,1]$, and where if $\mu \in I^X$ then we can think of the real number $\mu(x)$ as being the *degree of membership of x to μ.*

4.2 Fuzzy Set Theory

4.2.1 Preliminaries

In this section we give an account background to fuzzy theory and a list of concepts that will be useful in future discussions.

We will use the following notation interchangeably:

$$x \wedge y = \min(x, y) \quad x \vee y = \max(x, y), \quad x, y \in \mathrm{I} \tag{4.2}$$

$$\bigvee_{x \in S} x = \sup\{S\} \text{ and } S \subseteq [0, 1]. \tag{4.3}$$

Let X be the universe of discourse.

A fuzzy set μ on X is defined as a function $\mu : X \to [0, 1]$. The interval $[0, 1]$ is used as a chain with the usual ordering in which $\wedge$ stands for *infimum* (or intersection) and $\vee$ stands for *supremum* (or union).

The support of μ, denoted as supp (μ), is defined to be the crisp subset of X given by

$$\mathrm{supp}(\mu) = \{x \in X : \mu(x) > 0\}. \tag{4.4}$$

A fuzzy binary relation $\mathcal{R}$ on μ is defined as a fuzzy subset of the direct product $X \times X$ with values in the unit interval $[0, 1]$.

Let $\alpha \in [0, 1]$. By an α-cut of a fuzzy set μ, denoted as μ_α, is meant a subset of X defined by $\mu_\alpha = \{x \in X : \mu(x) \geq \alpha\}$. An α-cut $\mathcal{R}_\alpha$ of a fuzzy binary relation $\mathcal{R}$ on X is a crisp binary relation on X defined by $x\mathcal{R}_\alpha y$ if and only if $\mathcal{R}(x, y) \geq \alpha$.

A composition of fuzzy binary relations $\mathcal{R}$ and $\mathcal{R}'$ is defined as

$$(\mathcal{R} \circ \mathcal{R}')(x, y) = \sup_{z \in X}\{\mathcal{R}(x, z) \wedge \mathcal{R}(z, y)\}. \tag{4.5}$$

The α-cut of the composition of two fuzzy binary relations is the crisp composition of their α-cuts, that is $(\mathcal{R} \circ \mathcal{R}')_\alpha = \mathcal{R}_\alpha \circ \mathcal{R}'_\alpha$.

A fuzzy binary relation $\mathcal{R}$ on a set X is said to be

- *reflexive* if $\mathcal{R}(x, x) = 1$ for every $x \in X$,
- *symmetric* if $\mathcal{R}(x, y) = \mathcal{R}(y, x)$ for all $x, y \in X$,

- *transitive* if $\mathcal{R} \circ \mathcal{R} \subseteq \mathcal{R}$

  [equally said $\mathcal{R}(x,y) \wedge \mathcal{R}(y,z) \leq \mathcal{R}(x,z)$ for all $x, y, z \in X$].

A fuzzy binary relation $\mathcal{R}$ on X is said to be a *similarity relation* on X if it is reflexive, symmetric and transitive.

Note 4.2.1 By virtue of the reflexivity of $\mathcal{R}$, the transitive property is equivalent to

$$\bigvee_{z \in X} \{\mathcal{R}(x,z) \wedge \mathcal{R}(z,y)\} = \mathcal{R}(x,y) \text{ for all } x, y \in X. \tag{4.6}$$

4.3 Fuzzy Subgroups

The concept of a fuzzy group was first proposed by Rosenfeld in 1971. Within a short space of time his paper caught the interests of algebraist worldwide and ever since there has been an explosion of beautiful results out of that enthusiasm.
Let G be a group, and let $\mu : G \to \mathrm{I}$ be a mapping, where I is a unit interval $[0,1]$. Throughout our discussion, unless otherwise stated, G is a finite Abelian group.

4.4 t-norm

A fuzzy subgroup is mostly defined in terms of a t-norm (as t-norms are more general than max and min). We hereby give a brief description of a t-norm.

Definition 4.4.1 *A t-norm is a function $T : [0,1] \times [0,1] \to [0,1]$ satisfying for each $x, y, z \in [0,1]$:*

- $T(0,x) = 0$
- $T(1,x) = x$
- $T(x,y) = T(y,x)$
- *if* $y \leq z$, *then* $T(x,y) \leq T(x,z)$
- $T(x, T(y,z)) = T(T(x,y), z)$

The frequently encountered t-norm, $T(x, y) = \min(x, y)$, was used by Rosenfeld in his original definition of fuzzy subgroup, and will be used in this thesis.

$$\min(x, y) = \begin{cases} x & \text{if } x \leq y, \\ \\ y & \text{if } y < x \end{cases} \tag{4.7}$$

Another frequently used t-norm is

$$T(x, y) = \text{prod}(x, y) = xy.$$

A t-norm T_1 is said to be stronger than a t-norm T_2 if and only if

$$T_1(x, y) \geq T_2(x, y) \text{ for all } x, y \in [0, 1]. \tag{4.8}$$

Definition 4.4.2 *Let G be a group. A function $\mu : G \to [0, 1]$ is a fuzzy subgroup of G with respect to a t-norm T if and only if for each $x, y \in G$*

- $\mu(x, y) \geq T(\mu(x), \mu(y))$
- $\mu(-x) = \mu(x)$
- $\mu(0) = 1,$ *where* 0 *is the identity in* G

Consequently the following results hold:

Theorem 4.4.3 *Let G be a group. A function $\mu : G \to [0, 1]$ is a fuzzy subgroup of G with respect to a t-norm T if and only if $\mu(0) = 1$ and*
$\mu(x - y) \geq T(\mu(x), \mu(y)),$ for all $x, y \in G$.

Proof. [Osman].

Theorem 4.4.4 *Let G_1, G_2 be groups and $G = G_1 \times G_2$ be the direct product group of G_1 and G_2. Let μ_1 be a fuzzy subgroup of G_1 with respect to T, and μ_2 a fuzzy subgroup of G_2 with respect to T. Then $\mu = \mu_1 \times \mu_2$ is a fuzzy subgroup of G with respect to T defined by*

$$\mu(x_1, x_2) = (\mu_1 \times \mu_2)(x_1, x_2) = T(\mu(x_1), \mu(x_2)) \tag{4.9}$$

Proof. [Osman].

Since *min* is the strongest of all t-norms, any fuzzy subgroup with respect to *min* is a fuzzy subgroup with respect to any other t-norm as well.
(Schweizer and Sklar).
Therefore, consistent with group theory notation, we have the following restatement of a fuzzy subgroup:

Definition 4.4.5 *Let $x, y \in G$. μ is said to be a fuzzy subgroup of G if*

1. $\mu(x + y) \geq \mu(x) \wedge \mu(y)$,

2. $\mu(-x) = \mu(x)$, *for all* $x, y \in G$.

In their definition of arbitrary t-norms, Anthony and Sherwood did not include condition (3) as appearing in the following proposition. However, they realized later through their "experience of constructing example" the necessity for its inclusion. The following proposition, they claim, provides additional justification for its inclusion.

Proposition 4.4.6 (Anthony and Sherwood) *Let G be a group and suppose $\mu : G \to [0, 1]$ satisfies*

1. $\mu(x + y) \geq \min(\mu(x), \mu(y))$,

2. $\mu(-x) = \mu(x)$,

3. $\mu(0) > 0$

Then the function θ defined for each $x \in G$, by $\theta(x) = \mu(x)/\mu(0)$ is a fuzzy subgroup of G with respect to min such that $\theta(0) = 1$.

Proof. For any $x \in G$,
We first show that $1 = \theta(0) \geq \theta(x)$.

$$\theta(0) = \mu(0)/\mu(0) = \mu(x - x)/\mu(0) \geq \min(\mu(x), \mu(-x))/\mu(0) \tag{4.10}$$

$$= \min(\mu(x), \mu(x))/\mu(0) = \mu(x)/\mu(0) = \theta(x) \tag{4.11}$$

Thus $\theta(0) = 1$ and $0 \leq \theta(x) \leq 1$ for any $x \in G$.

We next show that $\theta(x + y) \geq \min(\theta(x), \theta(y))$. Now,

$$\begin{aligned}
\theta(x+y) = \mu(x+y)/\mu(0) &\geq \min(\mu(x), \mu(y))/\mu(0) && (4.12)\\
&= \min(\mu(x)/\mu(0), \mu(y)/\mu(0)) && (4.13)\\
&= \min(\theta(x), \theta(y)) && (4.14)
\end{aligned}$$

Finally,

$$\theta(-x) = \mu(-x)/\mu(0) = \mu(x)/\mu(0) = \theta(x) \tag{4.15}$$

Therefore θ is a fuzzy subgroup of G with respect to *min*. □

Definition 4.4.7 *Let μ be a fuzzy subset of S. For $t \in [0, 1]$, the set*

$$\mu_t = \{x \in S : \mu(x) \geq t\} \tag{4.16}$$

is called a level set subset of the fuzzy subset μ.

The following results pertaining to level sets hold:

Theorem 4.4.8 [5]. *Let G be a group and μ be a fuzzy subgroup of G. Then the level subset μ_t, $t \in [0, 1]$, $t \leq \mu(0)$, is a subgroup of G, where 0 is the identity of G.*

Theorem 4.4.9 *Any subgroup H of G can be realized as a level subgroup of some fuzzy subgroup G.*

In their paper [23], Dixit *et al* give a corrected version of theorem of Das [21] in the following way:

Theorem 4.4.10 *Let G be a group, and let μ be a fuzzy subgroup of G. Two level subgroups μ_{t_1} and μ_{t_2} of μ (with $t_1 < t_2$) are equal if and only if there is no $x \in G$ such that $t_1 \leq \mu(x) < t_2$.*

If μ is a fuzzy subgroup of G and Im $\mu = \{t_0, t_1, \ldots, t_n\}$ with $t_0 > t_1 > \cdots > t_n$, then the family of level subgroups forms a *chain*

$$\mu_{t_0} \subseteq \mu_{t_1} \subseteq \cdots \subseteq \mu_{t_n}, \text{ where } \mu(0) = t_0. \tag{4.17}$$

Sebastian and Sundar [77] studied the level sets in detail and produced the following: Let μ be a fuzzy subgroup of G with Im $\mu = \{t_j : j \in J\}$, and let $U = \{\mu_{t_j} : j \in J\}$, where J is an arbitrary index set. Then

1. $\exists$ a unique $j_0 \in J$ such that $t_{j_0} \geq t_j$ for every $j \in J$
2. $\mu_{t_{j_0}} = \wedge_{j \in J} \mu_{t_j}$
3. $G = \cup_{j \in J} \mu_{t_j}$
4. the members of $\mathcal{U}$ form a chain.

The following proposition also forms part of the discussion:

Proposition 4.4.11 [23], [77]. *Let ν be a fuzzy subgroup of G' and let $\{\nu_{t_j} : j \in J\}$ be a collection of all level subgroups of ν, then $\{f^{-1}(\nu_{t_j}) : j \in J\}$ is the collection of all level subgroups of $f^{-1}(\nu)$.*

Proof. Let $\mu = f^{-1}(\nu)$ and $t \in [0, 1]$. We show that $\mu_t = f^{-1}(\nu_t)$ for all $t \in [0, 1]$. Now

$$\begin{aligned} x \in \mu_t &\iff f^{-1}(\nu)(x) \geq t \\ &\iff \nu(f(x)) \geq t \\ &\iff f(x) \in \nu_t \\ &\iff x \in f^{-1}(\nu_t) \end{aligned}$$

Thus, in particular, we have $\mu_{t_j} = f^{-1}(\nu_{t_j})$ for all $j \in J$. We proceed by contradiction method, to establish the result. Suppose μ has a level subgroup
$\mu_t \notin \{f^{-1}(\nu_{t_j}) : j \in J\}$. This means that ν must have a level subgroup ν_t which does not belong to $\{\nu_{t_j}) : j \in J\}$ such that $\mu_t = f^{-1}(\nu_t)$, $t \in [0, 1]$ holds. (Contradiction)
Thus $\{f^{-1}(\nu_{t_j}) : j \in J\}$ is the collection of all level subgroups of $f^{-1}(\nu)$. □

Note 4.4.12 Some of the $f^{-1}(\nu_{t_j})$ may be equal.
In this event, *Thm 3.3* (Sebastian and Sundar, [77]) gives a necessary and sufficient condition for all $f^{-1}(\nu_{t_j})$ to be distinct.

For completeness we state the result and refer the reader to the article for the proof.

Theorem 4.4.13 [77]. *Let ν be a fuzzy subgroup of G' with $Im\ \nu = \{t_j : j \in J\}$, where J is a countable set. Then $f^{-1}(\nu_{t_j})$ are all distinct if and only if $f(G) \cap \nu^*(t_j) \neq \emptyset$, for all $j \in J$, where $\nu^*(t) = \{x \in G : \nu(x) = t\}$.*

4.5 Operations on Fuzzy Subgroups

In this section we define the operations of intersection, union, quotient, sum and product of fuzzy subgroups of G under an equivalence relation. It is evident that equality of fuzzy subgroups implies equivalence of fuzzy subgroups, but the converse need not be true. Not even fuzzy isomorphic fuzzy subgroups need be fuzzy equivalent. (see example 3.8 [59]). Also, inclusion and equivalence of fuzzy subgroups need not imply one another. In [62], Murali and Makamba introduced the study of these operations in detail. For consistency and convenience, we will state their results in the discussion below.

Definition 4.5.1 *Two fuzzy subgroups μ and ν of a group G are said to be* equivalent *if they have the same family of level subgroups. Otherwise the fuzzy subgroups are* non-equivalent.

4.5.1 Intersection of Fuzzy Subgroups

We define the analog of crisp intersection in the context of fuzzy subgroups and prove a proposition based on the intersection.

Definition 4.5.2 *Let μ and ν be two fuzzy subgroups of a group G. Then by their intersection $\mu \wedge \nu$ is meant:*

$$(\mu \wedge \nu)(x) = min(\mu(x), \nu(x)) \ \text{for all} x \in G. \tag{4.18}$$

We now state the following proposition involving intersection:

Proposition 4.5.3 *If μ and ν are fuzzy subgroups of a group G, then their intersection $(\mu \wedge \nu)$ is a fuzzy subgroup.*

Proof. Suppose μ and ν are fuzzy subgroups of a group G. Let $x, y \in G$. We want to show that

$$(\mu \wedge \nu)(x+y) \geq \min((\mu \wedge \nu)(x), (\mu \wedge \nu)(y)$$

and

$$(\mu \wedge \nu)(-x) = (\mu \wedge \nu)(x)$$

Now

$$\begin{aligned}
(\mu \wedge \nu)(x+y) &= \min(\mu(x+y), \nu(x+y)) \\
&\geq \min(\min(\mu(x), \mu(y)), \min(\nu(x), \nu(y)) \\
&\geq \min(\min(\mu(x), \nu(x)), \min(\mu(y), \nu(y) \\
&= \min((\mu \wedge \nu)(x), (\mu \wedge \nu)(y))
\end{aligned}$$

Also,

$$\begin{aligned}
(\mu \wedge \nu)(-x) &= \min(\mu(-x), \nu(-x)) \\
&= \min(\mu(x), \nu(x)) \\
&= (\mu \wedge \nu)(x).
\end{aligned}$$

□

With regards to equivalence, if two fuzzy subgroups are equivalent to each other then their intersection is equivalent to either of the fuzzy subgroups as the following proposition states:

Proposition 4.5.4 [62]. *Let μ and ν be two fuzzy subgroups. If $\mu \sim \nu$ then $\mu \wedge \nu \sim \mu$. As a consequence, $\mu \wedge \nu \sim \nu$.*

4.5.2 Union of Fuzzy Subgroups

In connection with union of fuzzy subgroups, Rosenfeld gave the following statement. We state it as a proposition:

Proposition 4.5.5 *A group cannot be the union of two proper fuzzy subgroups.*

In fact by a group he meant the characteristic function of G which is not a proper fuzzy subgroup.

The above statement was generalized by V. N Dixit *et al* [23] who gave the following formulation: *Is it possible for a proper fuzzy subgroup to be realized as a union of two proper fuzzy subgroups such that none is contained in the other?**

We begin by first stating what is meant by a *proper* fuzzy subgroup.

Definition 4.5.6 *Let G be a group. A fuzzy subgroup μ of G is said to be* proper *if $Im\ \ \mu$ has at least two elements (i.e μ is not constant).*

In preparation for the answer to the question * above, we note the following result due to Dixit *et al*:

Lemma 4.5.7 *Let G be a group and μ a fuzzy subgroup of G. If for $x, y \in G$, $\mu(x) < \mu(y)$, then*

$$\mu(x+y) = \mu(x) = \mu(y+x). \tag{4.19}$$

Proof. Given that μ is a fuzzy subgroup, we need to show that $\mu(x+y) = \mu(x)$ and $\mu(y+x) = \mu(x)$.

Now, μ is a fuzzy subgroup implies that

$$\mu(x+y) \geq \min(\mu(x), \mu(y)) = \mu(x) \ \text{ (by assumption).}$$

Also

$$\mu(x) = \mu(x+y-y) \geq \min(\mu(x+y), \mu(y)) \geq \mu(x+y), \ \text{ since } \ \mu(x) < \mu(y).$$

Hence we have that $\mu(x+y) = \mu(x)$. Similarly, it can be shown that $\mu(y+x) = \mu(x)$, which completes the proof . □

The union of two fuzzy subgroups need not be a fuzzy subgroup as illustrated in the following example, courtesy of Dixit et al, [24]:

Example 4.5.8 Let G be a *Klein's four group.*

$$G = \{e, f, g, fg\}, \ \text{ where } \ f^2 = e = g^2 \ \text{ and } \ fg = gf$$

For $0 \leq i \leq 5$, let $t_i \in [0,1]$ such that $1 = t_0 > t_1 > \cdots > t_5$.
Define fuzzy subsets μ and $\nu : G \to [0,1]$ as follows:

$$\mu(e) = t_1, \mu(f) = t_3 \text{ and } \mu(g) = \mu(fg) = t_4 \tag{4.20}$$

$$\nu(e) = t_0, \nu(f) = t_5, \nu(g) = t_2 \text{ and } \nu(fg) = t_5 \tag{4.21}$$

It can be seen that $\mu, and\ \nu$ are fuzzy subgroups of G. Furthermore, $(\mu \vee \nu)(0) = t_0$, $(\mu \vee \nu)(fg) = t_4$, $(\mu \vee \nu)(f) = t_3$, $(\mu \vee \nu)(g) = t_2$ but $\mu \vee \nu$ is not a fuzzy subgroup of G. Δ

In fact, the union of two *equivalent* fuzzy subgroups is a fuzzy subgroup.

Proposition 4.5.9 [62], [24]. *If $\mu \sim \nu$ then $\mu \vee \nu \sim \mu$. By consequence $\mu \vee \nu \sim \nu$.*

We conclude this section with this statement: With their carefully chosen examples, the authors in [23] demonstrated that a proper fuzzy subgroup can be realized as a union of two proper fuzzy subgroups (such that none is contained in the other) depending on the image set of the fuzzy subgroup under consideration.

4.5.3 Sum of Fuzzy Subgroups

We define what is meant by the sum of two fuzzy subgroups μ and ν.

Definition 4.5.10 *Let μ and ν be the two fuzzy subgroups. By the sum of μ and ν over G is meant*

$$(\mu + \nu)(x) = \ sup\{\mu(x_1) \wedge \nu(x_2) \,|\, x_1 + x_2 = x,\ where x \in G\}, \tag{4.22}$$

and this sum is defined using the extension principle.

In terms of equivalence, we state the following proposition:

Proposition 4.5.11 [62]. *If $\mu \sim \nu$ then $\mu + \nu \sim \mu$. By consequence $\mu + \nu \sim \nu$.*

4.6 Group Theoretic Terms in the Fuzzy Sense

4.6.1 Conjugacy

We first define what is meant by a *fuzzy conjugate.* Even though we are dealing with additive groups, we will continue to adopt a multiplicative notation whenever it is convenient to do so.

Definition 4.6.1 (Mukherjee and Bhattacharya) *Let G be a group and μ_1, μ_2 two fuzzy subgroups of G. μ_1 is said to be* conjugate *to μ_2 if for some $x \in G$ we have that*

$$\mu_1(g) = \mu_2(-x + g + x), \text{ for all } g \in G. \tag{4.23}$$

Hence if μ is a fuzzy subgroup of a group G and $g \in G$, then

$$\mu_g^*(x) = \mu(-g + x + g) \text{ for all } x \in G \tag{4.24}$$

denotes the fuzzy subgroup called the fuzzy conjugate subgroup of G determined by μ and g in G.

The following is a criterion for a p-group to be cyclic:

Theorem 4.6.2 (M. Asaad) *Let G be a group of prime-power order. Then G is cyclic if and only if there exists a fuzzy subgroup μ of G such that for $x, y \in G$*

1. *if $\mu(x) = \mu(y)$ then $\langle x \rangle = \langle y \rangle$*
2. *if $\mu(x) > \mu(y)$ then $\langle x \rangle \subset \langle y \rangle$*

What can be said about the fuzzy subgroups of a cyclic group of prime order? The following result provides the answer.

Theorem 4.6.3 (M. Asaad and others) *Let G be a cyclic group of prime order. Then there exists a fuzzy subgroup μ of G such that $\mu(0) = t_0$ and $\mu(x) = t_1$, for all $x \neq 0$ in G and $t_0 > t_1$.*

4.6.2 Normal Fuzzy Subgroups

Definition 4.6.4 *A fuzzy subgroup μ of a group G is said to be* normal *in G if $\mu(x+y) = \mu(y+x)$ for all $x, y \in G$.*

It is appropriate in this context to define another important concept in group theory, the concept of a *normalizer* [1]. In fuzzy subgroups it translates as follows:

Definition 4.6.5 *Let μ be a fuzzy subgroup of a group G. Then the set given by*

$$N(\mu) = \{g \in G : \mu^g = \mu\}$$

is called the normalizer *of μ.*

As a consequence, we have the following propositions:

Proposition 4.6.6 *If μ is a fuzzy subgroup of a group G, then $N(\mu)$ is a subgroup of G.*

Proof. For any $x, y \in N(\mu)$, we want to show that $xy \in N(\mu)$ and $x^{-1} \in N(\mu)$. Let $x, y \in N(\mu)$, then

$$\mu^{xy} = \mu^{yx} = \mu^y = \mu. \tag{4.25}$$

Hence $x, y \in N(\mu)$ implies $xy \in N(\mu)$.

Next, let $u = x^{-1}$, then for any $g \in G$

$$\begin{aligned} \mu^u(g) &= \mu(u^{-1}gu) \\ &= \mu(xgx^{-1}) = \mu((x^{-1}g^{-1}x)^{-1}) \\ &= \mu(x^{-1}g^{-1}x) = \mu^x(g^{-1}) \\ &= \mu(g^{-1}) = \mu(g) \end{aligned}$$

so that $x^{-1} \in N(\mu)$, that is $\mu^{x^{-1}} = \mu$. Thus $N(\mu)$ is a subgroup of G. □

Proposition 4.6.7 [57]. *Let μ be a fuzzy subgroup of a finite group G. Let $H = \{a \in G : \mu(a) = \mu(e)\}$, where e denotes the identity of G. Then H is a subgroup.*

[1] Let G be a group and let H be a subgroup of G. Then $N(H) = \{x \in G : xHx^{-1} = H\}$ is called the normalizer of H.

4.6.3 Commutator

We next explore the concept of *commutator* in the fuzzy sense. In their paper, [Gupta and Sarma, 1996], which was later strengthened by [Sarma, 1999] in terms of more results, the authors studied commutator in the fuzzy sense and its impact on group terms like *solvability* and others. For convenience, we give a summary of their version below.

Definition 4.6.8 *Suppose μ, ν are fuzzy subsets of a group G. A* commutator *of μ, ν is a fuzzy subgroup $[\mu, \nu]$ of G which is generated by the fuzzy subset (μ, ν) of G defined in the following manner:*

$$(\mu,\nu)(x) = \begin{cases} \bigvee\limits_{x=[a,b]} \{\mu(a) \wedge \nu(b)\} & \textit{if} \quad x \ \text{is a commutator of} \ G \\ \\ 0 \quad \text{otherwise} \end{cases} \tag{4.26}$$

We mention the following consequence of the definition, the details of which can be found in [Gupta and Sarma, 1996]:

1. Let μ, ν be the fuzzy subsets of G. If supp $(\mu) = K$ and supp $(\nu) = L$, then supp $([\mu, \nu]) = [K, L]$,

2. If μ, ν are normal fuzzy subgroups of G, then $[\mu, \nu]$ is a normal fuzzy subgroup of G,

3. $[\mu, \nu] = [\nu, \mu]$ for any two fuzzy subsets μ, ν of G.

We hereby state the result based on the definition of commutator and give a proof by induction.

Theorem 4.6.9 *Let μ be a fuzzy subgroup of a given group G. Suppose we define $\mu^{(0)} = \mu$ and $\mu^{(n)} = [\mu^{(n-1)}, \mu^{(n-1)}]$ for $n \geq 1$. Then $\mu^{(n)} \subseteq \mu^{(n-1)}$.*

Proof. Let $a \in G$. We consider two cases, if a is or is not a commutator.

Case 1: (not a commutator) For any $a \in G$ we have $(\mu, \mu)(a) = 0 \leq \mu(a)$.

Case 2. (commutator) For any $a \in G$, by definition of a commutator, we have that

$$(\mu, \mu)(a) \quad = \quad \bigvee_{a=[x,y]} \{\mu(x), \mu(y)\}$$

$$
\begin{aligned}
&= \bigvee_{a=[x,y]} \wedge\{\mu(x^{-1}, \mu(y^{-1}, \mu(x), \mu(y)\} \\
&\leq \bigvee_{a=[x,y]} \mu(x^{-1}y^{-1}xy) \\
&= \mu(x)
\end{aligned}
$$

Therefore, $(\mu, \mu) \leq \mu$, and because μ is a fuzzy subgroup we have

$$\mu^{(1)} = [\mu, \mu] = [(\mu, \mu)] \subseteq \mu = \mu^{(0)}. \tag{4.27}$$

Thus the statement is true for $n = 1$.

Assume the statement is true for $n = k$, that is assume $\mu^{(k)} \subseteq \mu^{(k-1)}$ for some $k \geq 1$. First we must note that if μ, ν are fuzzy subsets of G such that $\mu \subseteq \nu$, then $[\mu, \beta] \subseteq [\nu, \beta]$ for every fuzzy subset β of G.

We need to show that the statement is true for $n = k + 1$. Now

$$\mu^{(k+1)} = [\mu^{(k)}, \mu^{(k)}] \subseteq [\mu^{(k-1)}, \mu^{(k-1)}] = \mu^{(k)} \tag{4.28}$$

Therefore the statement is true for $n = k + 1$. Thus, by mathematical induction principle, the statement is true for all $n \geq 1$. □

4.6.4 Solvability

Definition 4.6.10 *Let G be a group. A fuzzy subgroup μ of G is said to be* solvable *if there exists a finite chain $\{\mu_i\}$ of fuzzy subgroups of G*

$$\{0\} = \mu_0 < \mu_1 < \mu_2 < \cdots < \mu_k = \mu \tag{4.29}$$

such that $\mu_{i-1} \triangleleft \mu_i$ and μ_{i+1}/μ_i is Abelian, $0 \leq i \leq k - 1$. Such a finite chain is called a **solvable series** *for μ.*

Consequently we have the following results due to [Ray, 1993]. For continuity and convenience, we provide the original proof as well.

Theorem 4.6.11 *Suppose H is a subgroup of a group G. The characteristic function χ_H is solvable if and only if H is solvable.*

Proof. ($\Longrightarrow$) Assume φ_H is solvable. By definition (4.6.10) there exists a solvable series

$$\{0\} = \mu_0 < \mu_1 < \mu_2 < \cdots < \mu_k = \chi_H \tag{4.30}$$

such that $\mu_{i-1} \lhd \mu_i$. Now consider the supp (μ_i), N_i, $0 \leq i \leq k-1$. Then the resulting series

$$\{0\} = N_0 \subset N_1 \subset N_2 \subset \cdots \subset N_k = H, \text{ where } N_{i-1} \lhd N_i \tag{4.31}$$

is a solvable series for H. Hence H is solvable.
($\Longleftarrow$) Assume H is solvable. Similarly,

$$\{0\} = \chi_{N_0} < \chi_{N_1} < \chi_{N_2} < \cdots < \chi_{N_k} = \chi_H \tag{4.32}$$

is a solvable series for χ_H. Thus χ_H is solvable. □

Theorem 4.6.12 (Ray) *Suppose μ and ν are fuzzy subgroups of a group G satisfying the following*

- *supp(μ) = supp(ν) = M*
- *$\mu \leq \nu$*
- *$\mu \lhd \mu$.*

If μ is solvable, so is ν.

4.7 Fuzzy Homomorphism and Fuzzy Isomorphism

In this section we describe fuzzy homomorphism in general, and give some results pertaining to the study.
In view of Chakraborty and Khare [17], before we define what a fuzzy homomorphism is, we need a few concepts to understand, namely, *fuzzy map, characteristic map.*[2]
For sets X and Y, and a map $\mu_\theta : X \times Y \to [0, 1]$,

[2] A fuzzy subgroup μ on a group G is called a characteristic fuzzy subgroup of G if $\mu \circ \theta = \mu$.

Definition 4.7.1 *A* fuzzy map $\theta : X \to Y$ *is an ordinary map from* X *to a set of all fuzzy subsets of* Y*, denoted as* $\mathcal{F}(Y)$*, in such a way that the following are satisfied:*

1. $\mu_\theta(x, y_1) = \mu_\theta(x, y_2) \neq 0 \Longrightarrow y_1 = y_2$,
2. *for all* $x \in X, \;\exists$ *unique* $y_x \in Y$ *with* $\mu_\theta(x, y_x) = 1$.

Such a μ_θ is termed the map characterizing fuzzy map.

Now with this information we are ready to define what is meant by a fuzzy homomorphism.

Definition 4.7.2 (Fuzzy homomorphism) *A fuzzy map* $f : G \to G'$ *that maps a group* G *to a group* G' *is said to be a fuzzy homomorphism if for every* $g_1, g_2 \in G$ *and* $g' \in G'$*,*

$$\mu_f(g_1 g_2, g') = \;\; sup_{g'=g_1'g_2'}([\mu_f(g_1, g_1')\dot{\mu}_f(g_2, g_2')])$$

Definition 4.7.3 *Let* f *be a homomorphism from a group* G *to a group* G'*, and let* μ, ν *be fuzzy sets in* G *and* G' *respectively. Then the homomorphic image (direct image)* $f(\mu)$ *and the preimage (inverse image)* $f^{-1}(\nu)$ *are fuzzy sets in* G' *and* G *respectively, defined by*

1.

$$f(\mu)(y) = \begin{cases} sup\{\mu(x) : x \in f^{-1}(y)\} & \text{if } f^{-1}(y) \neq \emptyset, \\ \\ 0 \quad \text{if } f^{-1}(y) = \emptyset \end{cases}$$

2. $f^{-1}(\nu)(x) = \nu(f(x))$ for each $x \in G$.

If for every $S \subseteq X, \;\exists\; s_0 \in S$ such that

$$\mu(s_0) = \;\; \sup\{\mu(s) : s \in S\},$$

then μ is said to have a *sup-property*.

We hereby state the following proposition found in fuzzy literature:

Proposition 4.7.4 *Suppose $f : X \to X'$ is a map, and let U_i and V_i be the families of fuzzy subsets of X and X'. Then for $\mu_i \in U_i$ and $\nu_i \in V_i$, and indexing set I, the following are true:*

1. $f(\bigvee_{i \in I} \mu_i) = \bigvee_{i \in I} f(\mu_i)$

2. $f^{-1}(\bigvee_{i \in I} \nu_i) = \bigvee_{i \in I} f^{-1}(\nu_i)$

3. $ff^{-1}(\nu_i) = \nu_i$ *if f is surjective*

4. $ff^{-1}(\mu_i) = \mu_i$ *if μ is f-invariant*

4.7.1 Fuzzy Homomorphism

The study of the effect of group homomorphisms on fuzzy groups was carried by Rosenfeld [73], Anthony and Sherwood [5], Sidky and Mishref [78], and Akgul [3]. Rosenfeld [73], for instance, proved that if f is a homomorphism on a group G and μ is a fuzzy subgroup of G, then $f(\mu)$ is a fuzzy subgroup of $f(G)$ if and only if μ has a *sup-property*, and that $f^{-1}(\nu)$ is a fuzzy subgroup of G whenever ν is a fuzzy subgroup of $f(G)$.

This idea was later challenged by Anthony and Sherwood when they proved that μ need not have a sup-property in order for $f(\mu)$ to be a fuzzy subgroup.

Sidky and Mishref [78] proved that if $f : G \to G'$ is a group homomorphism, and μ is a fuzzy subgroup of G, then $f(\mu)$ is a fuzzy subgroup of G'.

Akgul proved that $f^{-1}(\nu)$ is a fuzzy subgroup of G whenever ν is a fuzzy subgroup of G'. The above information is provided by S. Sebastian et al [77].

The homomorphic image of a fuzzy subgroup is always a fuzzy subgroup, as the following result states:

Theorem 4.7.5 (Sidky, Mishref) *Let f be a homomorphism from a group G to a group G'. If μ is a fuzzy subgroup of G, then $f(\mu)$ is a fuzzy subgroup of G'.*

The preimage of a fuzzy subgroup is a fuzzy subgroup:

Theorem 4.7.6 (Akgul) *Let ν be a fuzzy subgroup of a group G'. Then $f^{-1}(\nu)$ is a fuzzy subgroup of G.*

Dixit, Kumar and Ajmal [23], have proved that if μ is a fuzzy subgroup of G with $Im\ \mu = \{t_j : j = 1, \ldots, n\}$ such that $t_1 > t_2 > \cdots > t_n$ and if $F : G \to G'$ is a surjective group homomorphism, then the chain

$$f(\mu_{t_1}) \subseteq f(\mu_{t_2}) \subseteq \cdots f(\mu_{t_n})$$

contains all level subgroups of $f(\mu)$.
Sebastian and Sundar [77] removed the restriction on finiteness of $\mid f(\mu) \mid$ and proposed in the following way:

Proposition 4.7.7 *If f is a surjection, μ has a sup-property and $\{\mu_{t_j} : j \in J\}$ is the collection of all level subgroups of μ, then $\{f(\mu_{t_j}) : j \in J\}$ is the collection of all level subgroups of $f(\mu)$.*

It was also obvious that ontoness of f did not guarantee that all $f(\mu_{t_j})$ would be distinct, hence they proposed a necessary and sufficient condition for the distinctness of all $f(\mu_{t_j})$. (*μ must be f-invariant*) [Thm. 4.5].

Proposition 4.7.4 helps simplify significantly the results by M.E. Eroglu [33(1989)]. The author illustrates the application of the proposition to the following cases "[23] (Theorem 2.9, Theorem 2.10)":

Theorem 4.7.8 *Suppose $f : G \to G'$ is a homomorphism of a group G onto a group G', and let $\mathcal{U}_i$ be a family of fuzzy subgroups of G. Then the following hold:*

1. *If $\bigvee\limits_i(\mu_i)$ is a fuzzy subgroup of G, then $\bigvee\limits_i f(\mu_i)$ is a fuzzy subgroup of G'*
2. *If $\bigvee\limits_i f(\mu_i)$ is a fuzzy subgroup of G', then $\bigvee\limits_i(\mu_i)$ is a fuzzy subgroup of G only if μ_i are f-invariant.*

Proof.

1. Assume $\bigvee\limits_i(\mu_i)$ is a fuzzy subgroup of G. By theorem 4.7.5 and Proposition 4.7.4(1), the result follows.

2. Assume $\bigvee_i f(\mu_i)$ is a fuzzy subgroup of G'. Then $f^{-1}(\bigvee_i f(\mu_i))$ is a fuzzy subgroup of G'. By Proposition 4.7.4(2), the result follows.

Theorem 4.7.9 *If f is a homomorphism of a group G onto a group G', and $\mathcal{V}_i$ is a family of fuzzy subgroups of G, then the following are equivalent:*

1. *$\bigvee_i \nu_i$ is a fuzzy subgroup of G'*

2. *$\bigvee_i f^{-1}(\nu_i)$ is a fuzzy subgroup of G*

Proof. (1)$\Longrightarrow$ (2) Use the fact that the homomorphic preimage of a fuzzy subgroup is a fuzzy subgroup, together with Proposition 4.7.4(2).
(2)$\Longrightarrow$ (1) Since the homomorphic image of a fuzzy subgroup is a fuzzy subgroup and by Proposition 4.7.4(1), $f(\bigvee_i f^{-1}(\nu_i)) = \bigvee_i ff^{-1}(\nu_i) = \bigvee_i \nu_i$, the result follows. □

Whilst on fuzzy homomorphism, we state the following result:

Definition 4.7.10 *Let G and G' be groups, and let $f : G \to G'$ be a homomorphism. Let μ be a fuzzy subgroup of G. By the image of μ under f, $f(\mu)$, we mean a fuzzy subset of $f(G)$ defined by*

$$f(\mu)(f(x)) = sup\{\mu(y) : f(y) = f(x)\}. \tag{4.33}$$

Define $f(\mu)(y) = 0$ if $y \notin f(G)$. Then, $f(\mu)$ becomes a fuzzy subgroup of G'.

For proof of the claim, see [50], [51].

4.7.2 Homomorphism and Equivalence

Suppose $f : G \to G'$ is a homomorphism of a group G to G'. Under this homomorphism, if the fuzzy subgroups of G are equivalent, what can be said about their images in G'? The following result addresses this question:

Proposition 4.7.11 *If $f : G \to G'$, and if $\mu \sim \nu$ in G, then $f(\mu) \sim f(\nu)$ in G'.*

Proof. Let $f : G \to G'$ be a homomorphism. Suppose also that $\mu \sim \nu$ in G. Hence $\mu(x) > \mu(y)$ if and only if $\nu(x) > \nu(y)$ and $\mu(x) = 0$ if and only if $\nu(x) = 0$ for all $x, y \in G$. The second part implies that the supports of μ and ν are equal.
Now $f(\operatorname{supp}\mu) = f(\operatorname{supp}\nu)$, since f is a homomorphism. Hence
$\operatorname{supp} f(\mu) = \operatorname{supp} f(\nu)$. We end this by showing that f satisfies the equivalence part. To do this we choose any elements $x', y' \in G'$ in such a way that $f(\mu)(x) > f(\mu)(y)$. We show that $f(\nu)(x) > f(\nu)(y)$. Now for all $y \in G$ such that $f(y) = y'$ there exists an $x \in G$ such that $f(x) = x'$ and $\mu(x) > \mu(y)$. But $\mu \sim \nu$ hence $\nu(x) > \nu(y)$. From this it follows that $f(\nu)(x) > f(\nu)(y)$. Thus $f(\mu) \sim f(\nu)$ in G'. □

It is interesting to consider the behaviour of the preimages as well.

Proposition 4.7.12 *If $f : G \to G'$, and if $\mu \sim \nu$ in G', then $f^{-1}(\mu) \sim f^{-1}(\nu)$ in G.*

Proof. Let $f : G \to G'$ be a homomorphism. Assume that $\mu \sim \nu$ in G'. Then
$\operatorname{supp}\mu = \operatorname{supp}\nu$ in G'. From this we have that, since f is a homomorphism, $f^{-1}(\operatorname{supp}\mu) = f^{-1}(\operatorname{supp}\nu)$ in G. We next show that f^{-1} satisfies the equivalence. For this we pick $x_1, x_2 \in G$ such that $f^{-1}(\mu)(x_1) > f^{-1}(\mu)(x_2)$. Then we have that $\mu(f(x_1)) > \mu(f(x_2))$. Since $\mu \sim \nu$ we have $\nu(f(x_1)) > \nu(f(x_2))$. It follows that $f^{-1}(\nu)(x_1) > f^{-1}(\nu)(x_2)$. Thus $f^{-1}(\mu) \sim f^{-1}(\mu)$ in G. □

We close this chapter by looking at the concept of fuzzy isomorphism.

4.7.3 Fuzzy Isomorphism

The version of fuzzy isomorphism as defined below appeared as a remark in [59].

Definition 4.7.13 *Let G be a group and μ and ν be fuzzy subgroups of G. Then μ is said to be* fuzzy isomorphic *to ν if there exists an isomorphism $f : supp\,\mu \to supp\,\nu$ such that*

$$\mu(x) > \mu(y) \Longleftrightarrow \nu(f(x)) > \nu(f(y))$$

for any $x, y \in supp\,\mu$, and is denoted as $\mu \approx \nu$.

Subsequently there was the following comment:

The notion of equivalence can be viewed as a special case of the notion of fuzzy isomorphism as per the definition above. In comparison with the equivalence to be used in this work, the latter is finer than the usual fuzzy isomorphism as defined above. Thus fuzzy equivalence implies fuzzy isomorphism and not the other way round. (See example 3.8 in [59]).

Consider $G = \mathbb{Z}_2 \times \mathbb{Z}_2$, and let μ and ν be fuzzy subgroups of G such that

$$\mu(x) = \begin{cases} 1 & x = \{e\} \\ \lambda & x \in \mathbb{Z}_2 \times \{0\} \setminus \{e\} \\ \beta & \text{elsewhere} \end{cases} \qquad \nu(x) = \begin{cases} 1 & x = \{e\} \\ \lambda & x \in \{0\} \times \mathbb{Z}_2 \setminus \{e\} \\ \beta & \text{otherwise} \end{cases}$$

If there is a function f in G given by $f : (x, y) \rightarrow (y, x)$ then f is an isomorphism. Thus μ and ν are not equivalent even though they are isomorphic.

Chapter 5

Maximal Chains, Flags and Keychains

5.1 Introduction

In chapter 2 we described what is called in group theory a series of subgroups. In this chapter we introduce a new term synonymous to a series, namely a flag.

We, amongst other things, fix some terminology which will be used later in the classification of fuzzy subgroups. This terminology includes flags, pins, keychains, pinned flag, padidity, index and various other terms as will be described in progress. We will explain how a pinned flag determines a fuzzy subgroup or alternatively how a fuzzy subgroup can be associated with a pinned flag. Finally we will enumerate maximal chains based on the labelling of subgroup generators and ideas of the number of cyclic subgroups of each order. We will brush on the results based on the number of k-pad keychains as will be illustrated.

To begin this work, we give the following definitions that will be followed in the entire description of the topic.

Definition 5.1.1 *A* flag *is a maximal chain of subgroups of the form* $G_0 \subset G_1 \subset G_2 \subset \cdots \subset G_n$ *in which* $G_0 = \{0\}$ *and* $G_n = G$*, and all the* G_i*'s are called the* components *of the flag.*

We will interchangeably refer to $G_0 \subset G_1 \subset G_2 \subset \cdots \subset G_n$ as a *flag* or a maximal chain.

Definition 5.1.2 *Consider a set of real numbers λ_i, with $i = 0, \ldots, n$ in the unit interval I, where the λ_i's are not all necessarily distinct. We call a chain of these real numbers*

$$1 = \lambda_0 \geq \lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n \geq 0 \tag{5.1}$$

a keychain*, and all the λ_i's are called* pins*. A keychain always contains λ_0.*

Notice that 1 occupies the first position, and λ_i occupies the $(i+1)$-th position, for $i = 1, 2, \ldots, n$. Hence the length of a keychain is $n+1$, and so the n-chain has $n+1$ available positions. These positions will play a crucial role in further discussion. (see Definition 5.3.1).

Identical keychains, as can be anticipated, have the same length and contain identical pins. For this reason, two keychains are said to be distinct whenever they are either of different lengths or there is a pin which is found in one keychain but not in the other. (The keychains will be treated more promptly in the sections to follow. For now let us be using them in the context they are given in.)

The combination of these two terms leads us to what we refer as a *pinned flag.*

By a pinned flag on G we mean a flag on G together with a keychain on I. We denote such a pinned flag suggestively as

$$\{0\}^1 \subset G_1^{\lambda_1} \subset G_2^{\lambda_2} \cdots \subset G_n^{\lambda_n} \tag{5.2}$$

A fuzzy subset μ associated with a pinned flag in 5.2 is denoted as follows

$$\mu(x) = \begin{cases} 1 & \text{if } x = 0 \\ \\ \lambda_1 & \text{if } x \in G_1 \setminus \{0\} \\ \\ \lambda_2 & \text{if } x \in G_2 \setminus G_1 \\ \vdots \\ \lambda_n & \text{if } x \in G_n \setminus G_{n-1} \end{cases} \tag{5.3}$$

Proposition 5.1.3 *μ defined by 5.3 is a fuzzy subgroup.*

Proof. For any $a, b \in G$ there exist indices i, j with the property $1 \leq i \leq j \leq n$ such that $a \in G_i \setminus G_{i-1}$ and $b \in G_j \setminus G_{j-1}$. Now a, b are elements of G_j, and hence their sum $a + b$ is also in G_j so that $\mu(a + b) \geq \lambda_j$. But $\lambda_j \geq \lambda_i \wedge \lambda_j$, and by the way i, j have been defined we have that $\mu(a+b) \geq \mu(a) \wedge \mu(b)$. It is easy to show the second part, for if $a \in G$ there is an index i such that $a \in G_i \setminus G_{i-1}$. Now since $-a \in G_i$, we have that $\mu(a) = \lambda_i \geq \mu(-a)$ for some i. Also $\mu(0) \geq \mu(a)$ for all $a \in G$. This completes the proof that μ is a fuzzy subgroup. □

The converse to Proposition 5.1.3 also holds. That is given any fuzzy subgroup μ of G, then μ can be decomposed into a pinned-flag representing μ as in 5.3.

Proposition 5.1.4 [61]. *Let μ be a fuzzy subgroup of G. Then μ can be decomposed into a pinned flag $\{0\}^1 \subset G_1^{\lambda_1} \subset G_2^{\lambda_2} \cdots \subset G_n^{\lambda_n}$ such that 5.3 holds.*

Since λ_n may or may not be equal to 0, it follows that the support of μ is strictly contained in G or is equal to G respectively.
The equivalence relation that will be used in this work for the purpose of enumeration is the one appearing in [59].

Definition 5.1.5 *Let μ and ν be any fuzzy sets on I^X. An equivalence relation on I^X is defined as follows:*
$\mu \sim \nu$ if and only if for all $x, y \in X, \mu(x) > \mu(y)$ if and only if $\nu(x) > \nu(y)$ and $\mu(x) = 0$ if and only if $\nu(x) = 0$. The second condition, namely, $\mu(x) = 0$ if and only if $\nu(x) = 0$ implies that the supports of μ and ν are equal.

If fuzzy subgroups are equivalent what can be said about their pinned flags? Normally, one would expect that their pinned flags have the same length and that their corresponding components are identical. Indeed this is the case as stated in the following Proposition [61]:

Proposition 5.1.6 *Let μ and ν be two fuzzy subgroups. Suppose*
$X_0^1 \subset X_1^{\lambda_1} \subset X_2^{\lambda_2} \cdots \subset X_m^{\lambda_m}$ and $Y_0^1 \subset Y_1^{\beta_1} \subset Y_2^{\beta_2} \cdots \subset Y_n^{\beta_n}$ are the corresponding

pinned flags to μ and ν respectively. Then $\mu \sim \nu$ on G if and only if the following are true

1. *$n = m$*

2. *$X_i = Y_i$, for $i = 0, 1, \ldots, n$ and for distinct λ_is and distinct β_js.*

3. *$\lambda_i > \lambda_j$ if and only if $\beta_i > \beta_j$, for $1 \leq i, j \leq n$.*

Proof. ($\Longrightarrow$) Suppose $\mu \sim \nu$.

1. Define a function $f : \mu(X) \to \nu(X)$ by $f(\mu(x)) = \nu(x)$ for $x \in X$, where $\mu(X), \nu(X)$ are subsets of I. We need to show that f is well defined and bijective. To do this let $x, y \in X$. Now $\mu(x) > \mu(y)$ if and only if $\nu(x) > \nu(y)$, since $\mu \sim \nu$. Similarly, $\mu(x) < \mu(y)$ if and only if $\nu(x) < \nu(y)$. Thus $\mu(x) = \mu(y)$ if and only if $\nu(x) = \nu(y)$, that is $f(\mu(x)) = f(\mu(y))$. Hence f is well defined and is one-to-one. Lastly, by the way f has been defined, there exists a $\nu(x) \in \nu(X)$ such that $f(\mu(x)) = \nu(x)$ for all $\mu(x) \in \mu(X)$ and for all $x \in X$. Hence f surjective. Now f is well defined and bijective. Thus $|\mu(X)| = |\nu(X)|$. Therefore, $n = m$.

2. We prove by induction on n. Let $n = 0$, then $Y_0 = X_0$ as each set is the empty subgroup. Assume that $Y_k = X_k$ for $k \geq 0$. We need to show that $Y_{k+1} = X_{k+1}$. To do this we show that $Y_{k+1} \subset X_{k+1}$ and $X_{k+1} \subset Y_{k+1}$. To show the first inclusion, we pick an element $g \in Y_{k+1}$ and show that $g \in X_{k+1}$. Let $g \in Y_{k+1}$. By assumption, if $g \in Y_k$ then $g \in X_k$ a subset of X_{k+1}. If not, that is if $g \notin Y_k$, then there is a β_{k+1} such that $\nu(g) = \beta_{k+1}$. Such a g must be an element of X_{k+1}. To verify our claim, suppose not, that is suppose $g \notin X_{k+1}$. Then we have that $\mu(g) < \lambda_{k+1}$. Now select a $x \in X_{k+1}$ such that $x \notin X_k = Y_k$. Then we have that $\mu(g) < \mu(x)$ which by equivalence implies that $\nu(g) < \nu(x)$. This means that $\beta_{k+1} = \nu(g) < \nu(x) = \alpha$, say, where $\beta_k > \alpha > \beta_{k+1}$. From this we learn that x is in the α-cut of ν, that is $x \in \nu^\alpha \supseteq Y_k = X_k$. This is a contradiction. Hence $Y_{k+1} \subset X_{k+1}$. The reverse inclusion can be shown in a similar manner. Therefore, by the principle of mathematical induction, (2) holds.

3. By equivalence, supp μ = supp ν. Now since $\mu(x) > \mu(y)$ if and only if $\nu(x) > \nu(y)$, and since $X_i = Y_i$, for $i = 0, 1, \ldots, n$ and for distinct $\lambda_i s$ and distinct $\beta_j s$ by 2, then 3 follows.

($\Longleftarrow$) Let μ and ν be two fuzzy subgroups satisfying 1, 2 and 3. We need to show that $\mu \sim \nu$. From 1 and 3, we have supp μ = supp ν (since $\lambda_k = 0$ if and only if $\beta_k = 0$ for $1 \leq k \leq n$, and $m = n$). Let $x, y \in$ suppμ, and suppose that $\mu(x) > \mu(y)$. Then there exist λ_i, λ_j for some $1 \leq i, j \leq n$ for which $\mu(x) = \lambda_i$ and $\mu(y) = \lambda_j$. According to 1, we have that $n = m$ and condition 3 says that $\lambda_i > \lambda_j$ if and only if $\beta_i > \beta_j$, for $1 \leq i, j \leq n$. From these two conditions we conclude that $\nu(x) > \nu(y)$. We have shown that $\mu(x) > \mu(y)$ if and only if $\nu(x) > \nu(y)$. Thus $\mu \sim \nu$. □

The following example illustrates how we classify the fuzzy subgroups of a given group.

Example 5.1.7 Let $G = \mathbb{Z}_{16}$. Define $\mu : G \to I$ as follows:

$$\mu(x) = \begin{cases} 1 & \text{if } x = 0 \\ \frac{1}{2} & \text{if } x \in \mathbb{Z}_2 \setminus \{0\} \\ \frac{1}{4} & \text{if } x \in \mathbb{Z}_4 \setminus \mathbb{Z}_2 \\ \frac{1}{8} & \text{if } x \in \mathbb{Z}_8 \setminus \mathbb{Z}_4 \\ \frac{1}{16} & \text{if } x \in \mathbb{Z}_{16} \setminus \mathbb{Z}_8 \end{cases} \tag{5.4}$$

μ can be represented by

$$\{0\}^1 \subset \mathbb{Z}_2^{\frac{1}{2}} \subset \mathbb{Z}_4^{\frac{1}{4}} \subset \mathbb{Z}_8^{\frac{1}{8}} \subset \mathbb{Z}_{16}^{\frac{1}{16}}, \tag{5.5}$$

where $1, \frac{1}{2}$, etc are the weights in each subgroup.

All fuzzy subgroups ν that are equivalent to μ can be represented by

$$\nu : \{0\}^1 \subset \mathbb{Z}_2^{\lambda} \subset \mathbb{Z}_4^{\beta} \subset \mathbb{Z}_8^{\gamma} \subset \mathbb{Z}_{16}^{\delta} \tag{5.6}$$

such that

$$1 > \lambda > \beta > \gamma > \delta > 0. \tag{5.7}$$

Δ

We simply denote the keychain defined in 5.1 by $1\lambda_1\lambda_2\ldots\lambda_{n-1}\lambda_n$ in the descending order, where the last entry may or may not be zero.
Consider the pinned flag

$$\{0\}^1 \subset G_1^{\lambda_1} \subset G_2^{\lambda_2} \subset G_3^{\lambda_3}, \text{ with } 1 \geq \lambda_1 \geq \lambda_2 \geq \lambda_3 \geq 0. \tag{5.8}$$

Corresponding to the flag there are $15 = 2^4 - 1$ distinct equivalent classes of fuzzy subgroups. The keychains for such fuzzy subgroups arise from all the possibilities in (5.8) and can be written out thus $1111, 111\lambda_1, 1110, 11\lambda_1\lambda_1, 11\lambda_1\lambda_2, \cdots, 1000$. We choose to denote the number of fuzzy subgroups in the form $15 = 2^4 - 1 = \sum\limits_{r=0}^{3} 2^r$, and make an assumption that $1 > \lambda_1 > \lambda_2 > \lambda_3 \geq 0$.
We note that the number of fuzzy subgroups whose support is strictly G_3 is one more than the number of fuzzy subgroups whose support is properly contained in G_3. Hence we can write the number of fuzzy subgroups as

$$15 = 2^4 - 1 = \sum_{r=0}^{3} 2^r = 2^4/2 + 2^4/2 - 1. \tag{5.9}$$

The number of fuzzy subgroups whose support is G_i, for $i = 0, 1, 2, 3$, correspond to the components $(8, 4, 2, 1)$ of the partition of 15.
If a flag is extended by one component, the effect on the resulting number of distinct equivalent classes of fuzzy subgroups can be explained in the following way: Each fuzzy subgroup of G_{i-1} whose pins are all different from zero yields three fuzzy subgroups of G_i. Each of the remaining keychains gives rise to one fuzzy subgroup of G_n by simply attaching 0 to the keychain. This process will be explored fully in chapter 6 when we enumerate fuzzy subgroups of finite Abelian groups of rank two.

5.2 Enumeration of Maximal Chains

5.2.1 The Number of Maximal Chains

The process of enumeration of maximal chains of a lattice diagram is facilitated by the knowledge of subgroups of each order, as explained in chapter 3. In the following, we count the number of maximal chains on the lattice diagram of $\mathbb{Z}_{p^n} \times \mathbb{Z}_{p^m}$ for specific values of $n, m \in \mathbb{Z}^+$. Firstly, we illustrate with the case when $n = m = 1$:

Consider the case $n = m = 1$.

Lemma 5.2.1 *The group $G = \mathbb{Z}_p \times \mathbb{Z}_p$ has $p + 1$ maximal chains.*

Proof. The group $\mathbb{Z}_p \times \mathbb{Z}_p$ is a noncyclic group of order p^2 and is *Abelian.* The group has subgroups of order $1, p, p^2$, where the subgroup of order 1 is the trivial subgroup while that of order p^2 is the whole group. A group of order p cannot have a proper subgroup hence it be a cyclic group whose generator is any element different from the identity. The subgroups of order p are all cyclic and disjoint, with their generators being $(1, 0), (1, 1), \ldots, (1, p - 1), (0, 1)$. The whole group is described by the *linear combination* of the subgroups of order p. Hence the group $\mathbb{Z}_p \times \mathbb{Z}_p$ has maximal chains of the form $0 \subset \langle a \rangle \subset G$. From this it follows that $\mathbb{Z}_p \times \mathbb{Z}_p$ has $p+1$ maximal chains of subgroups. $\square$

Secondly, for other values of $n, m \in \mathbb{Z}^+$, we state the following propositions and prove them.

Lemma 5.2.2 *There are $2p^2 + 3p + 1$ maximal chains in the subgroup lattice of $G = \mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2}$*

Proof. Since $\mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2}$ is a non-cyclic group of order p^4, it has subgroups of order k, where k is a divisor of p^4. Hence each maximal chain of $\mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2}$ is a chain of the form

$$\{0\} \subset \langle a \rangle \subset \langle b \rangle \subset \langle c \rangle \subset G,$$

where a, b, c are cyclic of order p, p^2, p^3 respectively. Now $\langle a \rangle$ is representative of the

subgroup generators of the form $0p$; $p(ip)$, for $i = 0, 1, \ldots, p-1$ whose intersection contains the identity alone. It is easy to see that there are only $p+1$ such generators. The subgroup generators of the form $\langle b \rangle$ fall into different slots as shown on the table below. Again it is not difficult to see that there are $p+1$ such slots each with a membership of $p+1$. It should be noted that in this count one group, namely one generated by $\langle 0p, p0 \rangle$, has been counted more than once. The equation $(p+1)(p+1) - p = p^2 + p + 1$ fixes the over count. This means that $\langle b \rangle$ is comprised of $p^2 + p$ cyclic and one non-cyclic subgroups. The intersection,
$\cap \langle b \rangle_j \setminus \langle 0p, p0 \rangle$, $j = 0, 1, \ldots, p$, is empty. With the exception of the non-cyclic $\langle 0p, p0 \rangle$ which contains all the subgroups $\langle a \rangle$ and is itself contained in all $\langle c \rangle$, the rest of the subgroups in each slot are each contained in only one subgroup of $\langle c \rangle$ respectively. By counting, there are $p+1$ subgroup generators comprising $\langle c \rangle$ which is itself contained in G. Collectively, the result is $(p+1)(p+\mathbf{1}(p+1))$ maximal chains of subgroups as claimed in the proposition.

Alternatively, the maximal chains of the group G can be viewed as extensions of the maximal chains of the previous groups in this manner. The maximal chains of G are extensions of $\mathbb{Z}_{p^2} \times \mathbb{Z}_p$ or $\mathbb{Z}_p \times \mathbb{Z}_p$ or $\mathbb{Z}_p$. Now $\mathbb{Z}_{p^2} \times \mathbb{Z}_p$ contributes $2p+1$ maximal chains to G. These are the chains that go through $\langle 0p, 10 \rangle$. Next we consider the chains that go through $\langle 0p, p0 \rangle$ as such chains are the extensions $\mathbb{Z}_p \times \mathbb{Z}_p$. In this effect we obtain p ways to do this, with the path through $\langle 0p, 10 \rangle$ having been considered. Hence we have $p(p+1)$ such extensions. Finally $\mathbb{Z}_p$ contributes $p(p)$ maximal chains not having been considered before, as can be checked. Thus the total number of maximal chains of G is

$$(2p+1) + p(p+1) + p(p) = 2p^2 + 3p + 1,$$

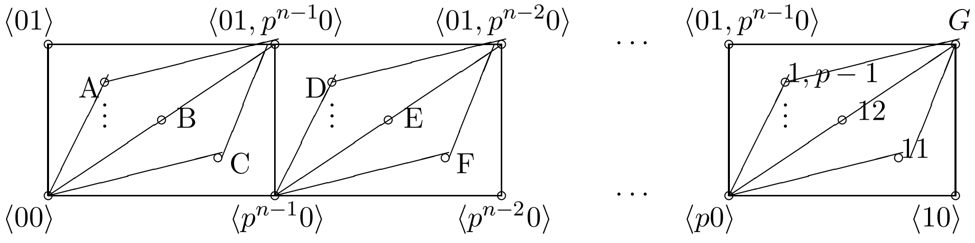
as required. This completes the proof. □

level	**subgroups**	**range**
0	1	
$\langle a\rangle \quad \equiv \quad 0p; \quad p(\alpha p)$	$p+1$	$\alpha = 0, 1, \ldots, p-1$
$\langle b\rangle \quad \equiv \quad 01; \quad \langle 0p, p0\rangle; \quad p\beta$		$\beta = 1, \ldots, p-1$
$\langle b\rangle \quad \equiv \quad \langle 0p, p0\rangle; \quad 1\,(0+\alpha p)$		
$\langle b\rangle \quad \equiv \quad \langle 0p, p0\rangle; \quad 1\,(1+\alpha p)$		
$\vdots$	p^2+p+1	$\alpha = 0, 1, \ldots, p-1$
$\langle b\rangle \quad \equiv \quad \langle 0p, p0\rangle; \quad 1\,((p-1)+\alpha p)$		
$\langle c\rangle \quad \equiv \quad \langle 01, p0\rangle; \quad \langle 0p, p0\rangle; \quad \langle 1\delta, 1(\delta+p)\rangle$	$p+1$	$\delta = 1, \ldots, p-1$

Subgroups of $\mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2}$

Proposition 5.2.3 *Let $G = \mathbb{Z}_{p^n} \times \mathbb{Z}_p$. Then the number of maximal chains of G is $np+1$.*

Proof. We prove by induction on n. When $n = 1$ the result resembles Lemma 5.2.1. Assume that $\mathbb{Z}_{p^k} \times \mathbb{Z}_p$ has $kp+1$ maximal chains. Now $\mathbb{Z}_{p^{k+1}} \times \mathbb{Z}_p$ has two sets of maximal subgroups, they are $\mathbb{Z}_{p^k} \times \mathbb{Z}_p$ and $\mathbb{Z}_{p^{k+1}} \times \mathbb{Z}_p \subset \langle b\rangle \subset \mathbb{Z}_{p^{k+1}} \times \mathbb{Z}_p$, where $\langle b\rangle$ has subgroup generators of the form $(10), (1,1), \ldots, (1, p-1)$ as illustrated in the diagram. Hence $\mathbb{Z}_{p^{k+1}} \times \mathbb{Z}_p \subset \langle b\rangle \subset \mathbb{Z}_{p^{k+1}} \times \mathbb{Z}_p$ contributes p maximal chains. Thus $\mathbb{Z}_{p^{k+1}} \times \mathbb{Z}_p$ has $kp+1+p = (k+1)+p$ maximal chains. This completes the induction.



$\langle 01\rangle$
$\langle 01, p^{n-1}0\rangle$
$\langle 01, p^{n-2}0\rangle$
$\cdots$
$\langle 01, p^{n-1}0\rangle$
G
A
$\vdots$
B
C
D
$\vdots$
E
F
$1, p-1$
$\vdots$
12
11
$\cdots$
$\langle 00\rangle$
$\langle p^{n-1}0\rangle$
$\langle p^{n-2}0\rangle$
$\langle p0\rangle$
$\langle 10\rangle$

where $A = \langle p^{n-1}, p-1\rangle$; $B = \langle p^{n-1}2\rangle$; $C = \langle p^{n-1}1\rangle$; $D = \langle p^{n-2}, p-1\rangle E = \langle p^{n-2}2\rangle; F = \langle p^{n-2}1\rangle$.

Proposition 5.2.4 *$G = \mathbb{Z}_{p^n} \times \mathbb{Z}_{p^2}$ has $[C(n,2) + C(n-1,1)]p^2 + C(n+1,1)p + 1$ maximal chains.*

Proof. We prove by induction on n. Let $C(a,b) = 0$ for $a < b$.
For $n = 2$, G has $2p^2 + 3p + 1$ maximal chains, in agreement with Lemma 5.2.2. These maximal chains are of the form

$$0 \subset \langle a \rangle \subset \langle b \rangle \subset \langle c \rangle \subset G,$$

where $\langle a \rangle, \langle b \rangle, \langle c \rangle$ have the form explained in Table 2.
Assume that $G = \mathbb{Z}_{p^k} \times \mathbb{Z}_{p^2}$ has $[C(k,2)+C(k-1,1)]p^2+C(k+1,1)p+1$ maximal chains, where $k \geq 2$. We need to show that the result is true for $n = k+1$. Every maximal chain of $\mathbb{Z}_{p^{k+1}} \times \mathbb{Z}_{p^2}$ can be considered as an extension of maximal chains of $\mathbb{Z}_{p^k} \times \mathbb{Z}_{p^2}$ or $\mathbb{Z}_{p^k} \times \mathbb{Z}_p$ or $\mathbb{Z}_{p^k}$ as shown in Dig. 1 below. (We have used double lines to mark the diagram that has been extended). We first determine the number of maximal chains of $\mathbb{Z}_{p^{k+1}} \times \mathbb{Z}_{p^2}$ which are extensions of $G = \mathbb{Z}_{p^k} \times \mathbb{Z}_{p^2}$. By assumption there are $[C(k,2) + C(k-1,1)]p^2 + C(k+1,1)p + 1$ such maximal chains. Such chains only go through the generator 1. (For ease of reference we only use digits to represent the nodes in question). We next consider those which are extensions of $\mathbb{Z}_{p^k} \times \mathbb{Z}_p$. Clearly these are the chains that pass through generator 2. Such chains give rise to p chains $\mathbb{Z}_{p^{k+1}} \times \mathbb{Z}_{p^2}$ as the path trough 1 has already been counted. Thus the number of this extension is $p(kp+1)$. Finally we consider the extensions of $\mathbb{Z}_{p^k}$. The extensions through the nodes $3, 4, 5$ have not been considered, and they constitute the extensions of $\mathbb{Z}_{p^k}$. Each of these p nodes gives rise to p maximal chains of $\mathbb{Z}_{p^{k+1}} \times \mathbb{Z}_{p^2}$ with those paths through 1 and 2 having been accounted for already. This exhausts all the possible extensions. Thus the total number of maximal chains of $\mathbb{Z}_{p^{k+1}} \times \mathbb{Z}_{p^2}$ is

$$\begin{aligned} &[C(k,2) + C(k-1,1)]p^2 + C(k+1,1)p + 1 + p(kp+1) + p(p) \\ &= [C(k,2) + C(k-1,1) + k + 1]p^2 + [C(k+1,1) + 1]p + 1 \\ &= [C(k+1,2) + C(k,1)]p^2 + C(k+2,1)p + 1, \text{ as required.} \end{aligned} \tag{5.10}$$

This completes the induction. □

Note that the number of maximal chains in Proposition 5.2.4 can also be counted using the formula $\sum_{\gamma=2}^{n} p(\gamma p+1)+(2p+1)$. The two formulas are identical as shown below:

$[C(n,2)+C(n-1,1)]p^2+C(n+1,1)p+1=\sum_{\gamma=2}^{n} p(\gamma p+1)+(2p+1)$ for all natural numbers n such that $n \geq 2$. To prove this, let $n=2$. Then

$$[C(2,2)+C(1,1)]p^2+C(3,1)p+1=\sum_{\gamma=2}^{2} p(\gamma p+1)+(2p+1).$$

We next assume that the statement is true for $n=k>2$, i.e

$$[C(k,2)+C(k-1,1)]p^2+C(k+1,1)p+1=\sum_{\gamma=2}^{k} p(\gamma p+1)+(2p+1).$$

We show that the statement is true for $n=k+1$. Now,

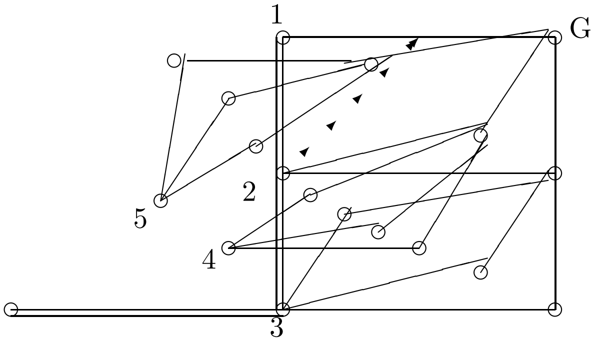
$$\begin{aligned}\sum_{\gamma=2}^{k+1} p(\gamma p+1)+(2p+1) &= \sum_{\gamma=2}^{k} p(\gamma p+1)+(2p+1)+p[(k+1)p+1]\\ &= [C(k,2)+C(k-1,1)]p^2+C(k+1,1)p+1+(k+1)p^2+p\\ &= [C(k+1,2)+C(k,1)]p^2+C(k+2,1)p+1.\end{aligned}$$

By the Principle of Mathematical induction, the statement holds for all $n \in \mathbb{N}$.

We state this result as a corollary:

Corollary 5.2.5 *$G=\mathbb{Z}_{p^n}\times\mathbb{Z}_{p^2}$ has $\sum_{\gamma=2}^{n} p(\gamma p+1)+(2p+1)$ maximal chains, $\gamma \in \mathbb{N}$.*

This can be proved by similar argument as in Proposition 5.2.4.



Dig. 1

For $m = 3$ and any n, we have:

Proposition 5.2.6 *Let $G = \mathbb{Z}_{p^n} \times \mathbb{Z}_{p^3}$ where p is a prime . Then the number of maximal chains of G is $[C(n,3) + 2C(n-1,2) + 2C(n-2,1)]p^3 + [C(n+1,2) + C(n,1)]p^2 + C(n+2,1)p + 1$.*

Proof. The proof follows by the same argument given in Propositions 5.2.3 and 5.2.4 above.

In fact the results appear in the following sequence, with the +1 term in all expressions on the right column not shown

Group	**Number of Maximal Chains**
pnp	$C(n,1)p$
$pnp2$	$[C(n,2) + C(n-1,1)]p^2 + p(n+1)p$
$pnp3$	$[C(n,3) + 2C(n-1,2) + 2C(n-2,1)]p^3 + p(n+1)p2$
$\vdots$	$\vdots$
$pnpm$	$\left\{\sum_{j=0}^{m-1} [C(n-j, m-j)] \cdot * \ T_m\right\} p^m + p(n+1)p(m-1)$
	with $p(n+m-1)p = (n+m-1)p$

Formulae for the number of maximal chains

(By $pnpm$ we mean a group $\mathbb{Z}_{p^n} \times \mathbb{Z}_{p^m}$.)

In the general expression for $pnpm$ as written on the last line of the table, T_m is the $m-$th row of a Catalan's triangle, $p(n+1)p(m-1)$ is the number of maximal chains of $\mathbb{Z}_{p^{n+1}} \times \mathbb{Z}_{p^{m-1}}$, and $.*$ is the usual pointwise multiplication.

Example 5.2.7 To illustrate the general case, consider the case when $m = 4$. According to definition, $n = 4, 5, 6, \ldots$ while T_4, in vector form, is $[1 \;\; 3 \;\; 5 \;\; 5]$. We obtain the following iteration:

$$\begin{aligned} p5p4 &= \{\sum_{j=0}^{3}[C(5-j,4-j)] \cdot * \ T_4\}p^4 + p(5+1)p(4-1) \\ &= \{[C(5,4)+C(4,3)+C(3,2)+C(2,1)].*[1 \ \ 3 \ \ 5 \ \ 5]\}\,p^4 + p6p3 \\ &= \{[C(5,4)+3C(4,3)+5C(3,2)+5C(2,1)]\}\,p^4 + p6p3 \end{aligned}$$

The process is repeated for $p6p3$ to get an expression involving $p7p2$ and so on, to obtain the collective number $42p^4+48p^3+27p^2+8p+1$ of maximal chains of $\mathbb{Z}_{p^5} \times \mathbb{Z}_{p^4}$ as expected (See the table below, in which (n,m) is a short notation for $pnpm$). Δ

$(1,1)$ $[1\ \ 1]$	$(2,2)$ $[2\ \ \ 3\ \ 1]$	$(3,3)$ $[5\ \ 9\ \ 5\ \ 1]$	$(4,4)$ $[14\ \ 28\ \ 20\ \ 7\ \ 1]$	...
$(2,1)$ $[2\ \ 1]$	$(3,2)$ $[5\ \ \ 4\ \ 1]$	$(4,3)$ $[14\ \ 14\ \ 6\ \ 1]$	$(5,4)$ $[42\ \ 48\ \ 27\ \ 8\ \ 1]$	
$(3,1)$ $[3\ \ 1]$	$(4,2)$ $[9\ \ \ 5\ \ 1]$	$(5,3)$ $[28\ \ 20\ \ 7\ \ 1]$	$(6,4)$ $[90\ \ 75\ \ 35\ \ 9\ \ 1]$	...
$(4,1)$ $[4\ \ 1]$	(5,2) $[14\ \ \ 6\ \ 1]$	$(6,3)$ $[48\ \ 27\ \ 8\ \ 1]$	$(7,4)$ $[165\ \ 110\ \ 44\ \ 10\ \ 1]$	
$(5,1)$ $[5\ \ 1]$	(6,2) $[20\ \ \ 7\ \ 1]$	$(7,3)$ $[75\ \ 35\ \ 9\ \ 1]$	$(8,4)$ $[275\ \ 154\ \ 54\ \ 11\ \ 1]$	...
$(6,1)$ $[6\ \ 1]$	(7,2) $[27\ \ \ 8\ \ 1]$	$(8,3)$ $[110\ \ 44\ \ 10\ \ 1]$	$(9,4)$ $[429\ \ 208\ \ 65\ \ 12\ \ 1]$	
$\vdots$	$\vdots$	$\vdots$	$\vdots$	...

The number of maximal chains of $pnpm$, where (n,m) represents $pnpm$ and the vectors represent the polynomials $a_np^n + a_{n-1}p^{n-1} + \ldots + a_0$.

From the Table (**Formulae for the number of maximal chains**) we infer the following propositions which can be proved by mathematical induction as in Proposition 5.2.4:

Proposition 5.2.8 *There are*

$$[C(n,4)+3C(n-1,3)+5C(n-2,2)+5C(n-3,1)]p^4+[C(n+1,3)+2C(n,2)+2C(n-1,1)]p^3+$$

$$[C(n+2,2)+C(n+1,1)]p^2+C(n+3,1)p+1$$

maximal chains of $G = \mathbb{Z}_{p^n} \times \mathbb{Z}_{p^4}$.

Proposition 5.2.9 *$G = \mathbb{Z}_{p^n} \times \mathbb{Z}_{p^5}$ has*

$$[C(n,5)+4C(n-1,4)+9C(n-2,3)+14C(n-3,2)+14C(n-4,1)]p^5+$$

$$[C(n+1,4)+3C(n,3)+5C(n-1,2)+5C(n-2,1)]p^4+[C(n+2,3)+2C(n+1,2)+2C(n,1)]p^3+$$

$$[C(n+3,2)+C(n+2,1)]p^2+C(n+4,1)p+1$$

maximal chains.

The expression for $m = 6$ and any positive integer n follows by rewriting the above theorem with n replaced by $n+1$ and adding the result to

$$[C(n,6)+5C(n-1,5)+14C(n-2,4)+28C(n-3,3)+42C(n-4,2)+42C(n-5,1)]p^6$$

to obtain the number of maximal chains of $G = \mathbb{Z}_{p^n} \times \mathbb{Z}_{p^6}$. The process continues for the general case through the use of Catalan's triangle.

Note 5.2.10 Consider the group $G = \mathbb{Z}_{p^n} \times \mathbb{Z}_{p^3}$. By Proposition 5.2.6 the group G has

$$[C(n,3)+2C(n-1,2)+2C(n-2,1)]p^3+[C(n+1,2)+C(n,1)]p^2+C(n+2,1)p+1$$

maximal chains. Now

$$\begin{aligned} C(n,3)+2C(n-1,2)+2C(n-2,1) &= \frac{n(n-1)(n-2)}{3!}+\frac{2(n-1)(n-2)}{2!}+2(n-2) \\ &= \frac{(n-2)[(n-1)(n+6)+12]}{3!} \\ &= \frac{(n-2)(n+2)(n+3)}{3!} \end{aligned}$$

Also,

$$\begin{aligned} C(n+1,2)+C(n,1)+C(n+2,1)+1 &= \frac{n(n+3)}{2!}+(n+3) \\ &= \frac{(n+2)(n+3)}{2!} \end{aligned}$$

Adding the two results, we have

$$\frac{(n+1)(n+2)(n+3)}{3!} = C(n+3,3).$$

On the basis of this observation and many cases of n and m in $\mathbb{Z}^+$, we make the following proposition which can be proved by mathematical induction:

Proposition 5.2.11 *The sum of the coefficients of the polynomial representing the number of maximal chains of a group $G = \mathbb{Z}_{p^n} \times \mathbb{Z}_{p^m}$, where $n, m \in \mathbb{Z}^+$, is equal to $C(n+m, m)$.*

Let $M(G)$ represent the number of maximal chains of a group G. Then

$$M(G)_n^m = A_m p^m + A_{m-1} p^{m-1} + \ldots + A_2 p^2 + A_1 p + A_0, \tag{5.11}$$

where A_0 is always equal to 1, and A_i, $i = 1, \ldots, m$ is a sum of combinatorial coefficients. In this expression, for instance, A_m has the form

$$a_1 \binom{n}{m} + a_2 \binom{n-1}{m-1} + \cdots + a_m \binom{n-m+1}{1}, \quad a_i \in T_m. \tag{5.12}$$

The determination of the coefficient of the leading term in any polynomial representation of the number of maximal chains of the group G has been a tricky one. We managed to get in control of the results by writing them in the combinatorial style as suggested above. In so doing, we observed that the coefficients a_i, $i = 1, \ldots, m$ in A_m, were entries in a Catalan triangle (read by rows) corresponding to the value of m. For example, $M(G)_n^3$ has the value given in note 5.2.10.

In the Catalan triangle each term is the sum of the entries above and to the left. Thus mathematically (see [79]), a Catalan's triangle $T(n,k)$ is a triangular array described by the equation

$$T(n,k) = \sum_{j=0}^{k} T(n-1, j).$$

For the first few rows, the array looks like:

$$\begin{array}{c}
1 \\
1 \quad 1 \\
1 \quad 2 \quad 2 \\
1 \quad 3 \quad 5 \quad 5 \\
1 \quad 4 \quad 9 \quad 14 \quad 14 \\
1 \quad 5 \quad 14 \quad 28 \quad 42 \quad 42 \\
\vdots
\end{array}$$

As suggested by the formulas, each row of the array corresponds to the value of m and any positive integer n in $\mathbb{Z}_{p^n} \times \mathbb{Z}_{p^m}$.

Using this array, we write

$$M(G)^3_n = \overbrace{[C(n,3) + 2C(n-1,2) + 2C(n-2,1)]}^{m=3} p^3 + \underbrace{[C(n+1,2) + C(n,1)]}_{n+1,m=2} p^2 +$$

$$C(n+2,1)p + 1,$$

the result that appeared in Proposition 5.2.6.

There are various interpretations attached to this array and its versions. The most dominant interpretation is that $T(n,k)$ is the number of standard tableaux of shape (n,k), where $n \geq 0$ and $0 \leq k \leq n$. The same array can be described as a sequence $a(n,m)$ with the same meaning, that is the number of standard tableaux of shape (n,m), where $n \geq 0$ and $0 \leq m \leq n$.

Other sequences can be generated from this array. For instance a sequence formed by the row sums of the array is called a sequence of Catalan Numbers.

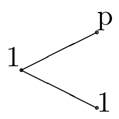
In our subsequent work we shall investigate what is meant by the sequences generated by other diagonals of this array to our lattices.

For now we can mention the resemblance of the conversion of each lattice to a binary tree diagram to the triangle of Narayana Numbers. The interpretation of the sequence $a(n,k)$ of these numbers is that of the number of pairs (P,Q) of lattice paths from $(0,0)$ to $(k, n+1-k)$, each consisting of unit steps East or North, in such a manner that P lies strictly above Q except at the endpoints. [79].

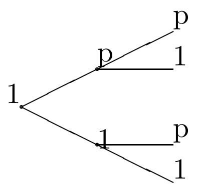
5.2.2 The Conversion of a Subgroup Lattice into a Binary Tree

In chapter three we laid down a method of conversion from a tree diagram to a subgroup lattice diagram of a particular group $G = \mathbb{Z}_{p^n} \times \mathbb{Z}_{p^m}$ for any positive integers n and m. Here we shall describe a method of conversion from a lattice diagram to a binary tree diagram of any group G. Although the method is tedious for bigger groups, but once a binary tree has been obtained it is much easier to count the maximal chains and subchains. We will develop an algorithm to go about this conversion.

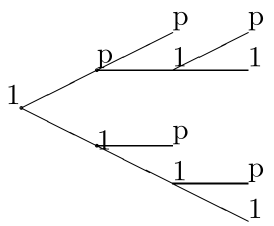
Take a subgroup lattice diagram of any group G. We count the number of paths from $(0, 0)$ to G with movements to the left and downwards prohibited. There are $p + 1$ ways of traversing the diagram from $(0, 0)$ to the next level in the lattice (see Lemma 5.2.1 and example 3.3.4). We represent this by the following diagram



Specifically for $G = \mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2}$, we see that from each of the $p + 1$ nodes there are $p+1$ ways available to travel to the destination G. This translates the above diagram into the form



Now of the $p + 1$ each p takes us to the destination in only one way, whereas there are $p+1$ ways available from the remaining 1, and we have reached G. The diagram has the following look



Now the sum of the products of vertices in each path from the root to the leaves gives the number of maximal chains of G as a polynomial in p.

We can obtain the binary tree diagram for the next higher group, in this case $G = \mathbb{Z}_{p^3} \times \mathbb{Z}_{p^2}$, from the previous tree diagram by certain attachments as will be explained in the program below. For instance $G = \mathbb{Z}_{p^3} \times \mathbb{Z}_{p^2}$ has the looks of figure

4 (at the back).

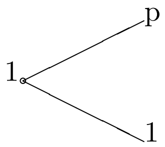
Definition 5.2.12 *Let the symbol ∇ define the extension of a binary tree representation of a subgroup lattice for a smaller group to that of a higher group.*
The height *of a binary tree is the number of levels from a root of the tree to its leaves.*
The binary tree representation for a group $\mathbb{Z}_{p^n} \times \mathbb{Z}_{p^m}$, hereby represented as (n, m) is itself a result of the extension of a binary tree representation of a smaller group in some way as explained below.

The following scheme can be used to produce graphs for G for any positive integers n and m:

$$(n,m) = \begin{cases} (n, m-1)\nabla(n, m-1) & \text{if } n = m \\ \\ (n-1, m)\nabla(n, m-1) & \text{if } n \neq m \end{cases} \tag{5.13}$$

$$(n, 0) = \text{ no extension } , n \geq m, \;\; n \in \mathbb{Z}^+$$

In this scheme (n, m) for $n, m \in \mathbb{Z}^+$, is a binary tree diagram of height $n + m - 1$. This binary tree is a composition of a full binary tree of height m with extensions of height $n - 1$. By extensions we mean the extension of the full binary tree by attaching binary trees of height $n - 1$ to all but the upper node of the full binary tree. The root of every (n, m) is always 1. In the process of extension the root is dropped and its place is taken by a leaf of the extended binary tree diagram.
To construct a binary tree diagram (n, m) for G, we need the following information. For a fixed m and $n \in \mathbb{Z}^+$ with $n \geq m$, we call $\{(n, m)\}$ a class of binary tree diagrams of height $n + m - 1$. The members of this class are called nth members depending on the value of n. The first member of each class occurs when $n = m$. When $m < 1$, we have an empty class, that is there is no possible binary tree diagram. We call $(1, 1)$ a default member whose structure has the appearance



Every class member is an extension of the default member's leaves. To construct the first member of each class, we extend the default member by the second member of the previous class. Thus (n, m) for $n = m$ is the extension of $(1, 1)$ by
$(n, m - 1) \in \{(n, m)\}$.
For each class we have the following array of members

$$\begin{aligned} &(n,1),(n,2),(n,3),\dots \\ (n+1,1),(n&+1,2),(n+1,3),\dots \\ (n+2,1),(n&+2,2),(n+2,3),\dots \\ &\vdots \\ (n+j,i)&\ \ 0 \le j \le i \ge 1 \end{aligned}$$

(n, m), $m = 1$ is a special class in which only the lower node of a default member is extended by $(1, 1)$ to obtain $(n + 1, 1)$.
In terms of sequence and for this special class, for $n = 1, m = 1$ we have
$(n, m) = (1, 1)$ as described above. Define an operation ∇ (an extension of a binary tree diagram) between elements $(n, 1)$ and $(1, 1)$ for any positive integer n such that

$$(n, 1) \ \nabla \ (1, 1) = (n + 1, 1).$$

Let $a_0 = (1, 1)$, the initial element (default member). Then $a_1 = (2, 1) = (1, 1) \ \nabla \ (1, 1)$, an element representing a binary tree diagram formed as a result of the extension of the default member at the lower node by a_0. Similarly, $a_2 = (3, 1) = (2, 1) \ \nabla \ (1, 1)$, an element representing a binary tree diagram formed by a_1 and a_0. Continuing we have

$$a_{n-1} = (n, 1) = (n - 1, 1) \ \nabla \ (1, 1),$$

and so on. Thus we have

$$a_n = (n + 1, 1) = (n, 1) \ \nabla \ (1, 1)$$

so that

$$a_n = a_{n-1} \ \nabla \quad a_0$$

describes the sequence recursively.

Otherwise to construct $(n+1, m)$, where $n+1 > m$, extend the lower node of the default member by (n, m) and the upper node by $(n+1, m-1)$. In all these binary tree diagrams, the upper node is always named p while the lower node is always named 1. It is important to recall, as was described in chapter three, that every nonidentity subgroup of $G = \mathbb{Z}_{p^n} \times \mathbb{Z}_{p^m}$ is contained in $p+1$ subgroups of G. This fact was also evident in the counting of maximal chains of subgroups of G in Chapter 5. Hence we have the nodes p and 1 in the transformation of a subgroup lattice of G into a binary tree diagram, and in the above figure.

If we let $L(G)$ be the subgroup lattice of the group G, $B_{L(G)}$ be a binary tree diagram of height $n+m-1$, $FB_{L(G)}$ be a full binary tree of height m, then $B_{L(G)} = FB_{L(G)} \cup \ \xi$, where ξ is a family of binary tree extensions of height $n-1$.

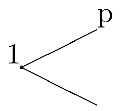
This binary tree diagram is constructed in the following way: Construct a full binary tree diagram of height m and extend its leaves with binary trees of height $n-1$. As a function

$$(n, m) : L(G) \longrightarrow B_{L(G)}$$

such that

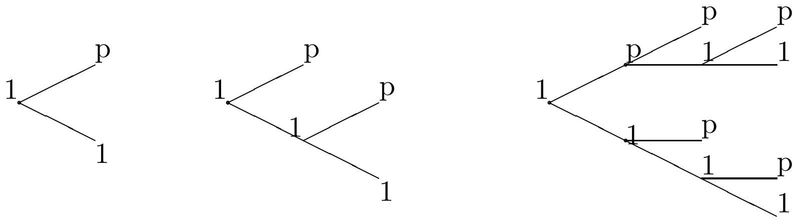
$$\ell \mapsto (F_B, \xi),$$

where ξ is a family of extensions, and $\ell \in L(G)$. To carry out the program of converting a lattice diagram of G into a binary tree diagram of G, we do it in two ways depending on the values of n and m. But in each case we add an extension to the root of the binary tree for $(n, m-1)$ or $(n-1, m)$ which has the form



The p in this extension takes the place of the root of the binary tree for $(n, m-1)$.

Example 5.2.13 Consider the problem of drawing a binary tree diagram for the group $(n, m) = (3, 2)$. Now $n \neq m$, so we first draw one for $(2, 2)$. In this group $n = m$, so we first draw a binary tree for a group $(2, 1)$. In the latter, $n \neq m$, hence a binary tree for a group $(1, 1)$ shall be drawn first, and it looks like this:



We apply the extension on it to obtain $(2, 1)$, affix $(2, 1)$ to be rooted at p of the extension, thereby getting $(2, 2)$. Finally to get $(3, 2)$ we apply extension on $(2, 2)$ followed by affixing $(3, 1)$ at p of the extension. The resulting diagram is figure 4. Δ

Equation 5.13 allows us to perform the following algebra (the coefficient implies duplication):

$$\begin{aligned}(3,3) &= (3,2)\nabla(3,2)\\ &= (2,2)\nabla(3,1)\nabla(3,2)\\ &= 2[(2,1)\nabla(2,1)\nabla(3,1)]\\ &= 2[2(2,1)\nabla(3,1)].\end{aligned}$$

Note 5.2.14 On each binary tree diagram the number of subchains up to each level corresponds to the partition $\lambda = (k, 1, 1 \ldots, 1)$ in $G = \mathbb{Z}_{p^n} \times \mathbb{Z}_{p^m}$, where the sum

$$\sum_{k=1}^{n+m-1} (k, 1, 1 \ldots, 1) = n + m.$$

For instance, in figure 5 we have the following number of subchains:

$$p + 1; \;\; p^2 + 2p + 1; \;\; 3p^2 + 3p + 1; \;\; 6p^2 + 4p + 1; \ldots; \;\; 14p^2 + 6p + 1$$

corresponding to

$\lambda_1 = (6, 1); \lambda_2 = (5, 1, 1); \lambda_3 = (4, 1, 1, 1); \lambda_4 = (3, 1, 1, 1, 1); \ldots; \lambda_6 = (1, 1, 1, 1, 1, 1, 1)$

of $G = \mathbb{Z}_{p^5} \times \mathbb{Z}_{p^2}$.

In the same manner we can consider a problem of converting a binary tree diagram into a subgroup lattice of a group G.

We next give a discussion of keychains. The details can be found in [61].

5.3 Keychains

We define some new concepts and find the cardinality of k-pad chains.

5.3.1 Definition of Key Concepts

Definition 5.3.1 1. *A finite n-chain is a collection of numbers on* $[0, 1]$ *of the form*

$$1 > \lambda_1 > \lambda_2 > \ldots > \lambda_{n-1} > \lambda_n$$

called **pins***.*

2. *An n-chain is called a keychain if* $1 \geq \lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_{n-1} \geq \lambda_n$.

3. *Interlocked pins are called components, with the exception of a 1 standing alone in the first position and* **not** *interlocked with any of the λ's. (A consecutive occurrence of equality signs is said to be in an interlocking position of pins).*

4. *A* **k-pad***, for* $1 \leq k \leq n$*, is a keychain containing k distinct components.*

5. *The number of pins found in the component formed by interlocked positions is called the* **padidity** *of the component. So in example 5.3.2, the padidities are respectively 1, 3, 1 for a 4-pad key chain, while they are 3, 2 for a 2-pad key chain. Now the* index *of a k-pad keychain is the set of padidities of various components of the keychain. In order to avoid unnecessary complications, the padidities of singleton components are ignored.*

Example 5.3.2 Consider the chain $1 > \lambda_1 > \lambda_2 = \lambda_3 = \lambda_4 > \lambda_5$. This is a 3-pad keychain of a 6-chain.

$1 = \lambda_1 = \lambda_2 > \lambda_3 = \lambda_4$ is a 2-pad keychain of a 5-chain. Δ

Note 5.3.3 For any $n \geq 2$, there are only three 1-pad key chains, they are of the form

$$1\,\overbrace{111\cdots1}^{n-1}$$

$$1\,\overbrace{\lambda\lambda\lambda\cdots\lambda}^{n-1}$$

$$1\,\overbrace{000\cdots0}^{n-1}$$

There are only four $(n-1)$-pad keychains for any $n \geq 3$. They are

$$1\lambda_1\lambda_2\lambda_3\cdots\lambda_{n-1} > 0$$

$$11\lambda_2\lambda_3\cdots\lambda_{n-1} > 0$$

$$1\lambda_1\lambda_2\lambda_3\cdots\lambda_{n-2}0$$

$$11\lambda_2\lambda_3\cdots\lambda_{n-2}0$$

The number of keychains of a chain of length n were determined with the use of index as defined in Definition 5.3.1 from the paper by the authors in [60]. For completeness, we give the following discussion:

5.3.2 Enumeration of Keychains

Following Note 5.3.3 above, in this section we determine the number of all keychains of length n. We begin by illustrating the inductive steps necessary for the formal proof of a general case. Detailed proofs of the following propositions can be found by visiting [60].

The notation $card[(n-k)-pad, n:k]$ in the following propositions shall mean the number of $(n-k)-pad$ keychains of length n with index k.

Proposition 5.3.4 *The $card[(n-k)-pad, n:k]$ keychains is $4(n-k)$.*

Proposition 5.3.5 *The $card[(n-k_1-k_2+1)-pad, n:(k_1,k_2)]$ keychains is*

$$\frac{4(n-k_1-k_2+1)!}{(n-k_1-k_2-1)!} \quad \textit{if } k_1 \neq k_2,$$

$$\frac{4(n-k_1-k_2+1)!}{2!(n-k_1-k_2-1)!} \quad \text{if } k_1 = k_2,$$

where $k_i > 1$ *for* $i = 1, 2$.

Proposition 5.3.6 *The* $card[(n-k_1-k_2-k_3+2)-pad, n : (k_1, k_2, k_3)]$ *keychains is*

$$\frac{4(n-k_1-k_2-k_3+2)!}{(n-k_1-k_2-k_3-1)!} \quad \text{if } k_1 \neq k_2 \neq k_3,$$

$$\frac{4(n-k_1-k_2-k_3+2)!}{3!(n-k_1-k_2-k_3-1)!} \quad \text{if } k_1 = k_2 = k_3,$$

where $k_i > 1$ *for* $i = 1, 2, 3$.

Chapter 6

Counting of the Number of Fuzzy Subgroups of Finite Abelian p-Groups of Rank Two

6.1 Introduction

In this chapter we enumerate fuzzy subgroups of G using the technique for counting that was introduced in [59]. We determine the number of fuzzy subgroups through the actions of keychains on flags (or maximal chains). For this purpose, the information in Section 5.2 as well as Definition 5.1.5 will be useful.

6.2 Preliminaries

The equivalence relation we shall use states that $\mu \sim \nu$ if and only if

$$(i)\ \text{for all}\, x, y \in G,\ \ \mu(x) > \mu(y)\ \ \text{ if and only if }\ \ \nu(x) > \nu(y)$$

$$(ii)\ \ \mu(x) = 0\ \ \text{ if and only if } \nu(x) = 0$$

The theory of partitions dates back to the Middle Ages, but the discoveries of great depth took place in the eighteenth century by L. Euler. Euler laid a foundation when he proved many significant partition theorems. From then other great mathematicians started contributing significantly into the development of the theory. The theory enjoys applications in vast mathematical sciences and statistics, especially combinatorics.

There are many definitions of the term partition. For instance in computer sciences the word refers to segments of memory, and so on. For our purpose, we shall view the meaning of the term as described in the following definition.

Definition 6.2.1 *A partition of a positive integer n is a finite non increasing sequence of non-negative integers $\lambda_1, \lambda_2, \ldots, \lambda_k$ with the property that $\sum_{i=1}^{k} \lambda_i = n$. We call the λ_i the parts of the partition.*

We denote the partition $(\lambda_1, \lambda_2, \ldots, \lambda_k)$ by λ, and some authors write $\lambda \mapsto n$ to mean that λ is a partition of n.

Obviously there can be more than one way of writing n into its partitions, or put differently there are various sets of partitions of a positive integer n. The term partition function, as a result, comes into the picture.

Definition 6.2.2 *The partition function, denoted as $p(n)$, is the number of partitions of n.*

Note 6.2.3 Since the empty sequence forms the only partition of zero, it is appropriate to set $p(0) = 1$. Sometimes it is beneficial to represent $\lambda = \lambda_1, \lambda_2, \ldots, \lambda_s$ in the form $\lambda = (1^{\alpha_1}2^{\alpha_2}3^{\alpha_3}\ldots)$, where strictly α_i of λ_j are equal to i. Hence $\sum_{i\geq 1} i\alpha_i = n$.

As noted by Montes et al, [54], the generalization of the concept of a crisp partition to that of a fuzzy partition requires the choice of a family of fuzzy subsets which preserves the conditions characterizing crisp partitions. However, "the usual constraints for the union and intersection of subsets are very limiting and seem to be far from the 'fuzzy spirit'". He further says that the union of subsets in the partition is forced to be 'close to' the universe of discourse, and the intersection of any two subsets in the partition is forced to be 'close to' the empty set.

6.3 Fuzzy Subgroup Enumeration

In this section we enumerate fuzzy subgroups, up to isomorphism, of finite Abelian p-groups of rank two, where p is any prime number. We use the results on maximal chains of subgroups obtained in Section 5.2.1, and then count fuzzy subgroups using inductive argument. We assume throughout our discussion that $\mu(0) = 1$ for any fuzzy subgroup μ of G.

In every keychain the first position is always occupied by 1, while the rest of the pins occupy the remaining positions in partitions of n. Hence we can ignore the 1 in the first position, which always refers to the identity, and group together all the resulting keychains given by a specific partition of n. We apply the keychains to the maximal chains on the lattice diagram of G. We observe that all the keychains with the same specific partition of n yield the same number of fuzzy subgroups of G. For instance for $n = 4$, by a partition $2, 1, 1$ we mean all the keychains of the form $1\lambda\lambda\beta\delta$, $1\lambda\lambda\beta 0$, $1\lambda\beta\beta\delta$, $1\lambda\beta 00$, etc. By counting there are 12 such keychains. Suppose each of the keychains yields $\alpha(p)$ fuzzy subgroups, where $\alpha(p)$ is a polynomial in p, then the collective number of distinct fuzzy subgroups given by all the keychains with this partition will be $12\alpha(p)$ as can be verified from the table below.

The following example illustrates how we obtain the distinct equivalence classes of fuzzy subgroups of G under the equivalence relation stated in Section 6.2.

Example 6.3.1 Let $G = \mathbb{Z}_{p^3} \times \mathbb{Z}_{p^3}$. We model every maximal chain of G by a chain of the form $0 \subset \mathbb{Z}_p \subset \cdots \subset \mathbb{Z}_{p^n}$. For $n = 6$ there are $2^7 - 1$ distinct equivalence classes of fuzzy subgroups on $\mathbb{Z}_{p^6}$ corresponding to the maximal chain $0 \subset \mathbb{Z}_p \subset \cdots \subset \mathbb{Z}_{p^n}$. These are given by the keychain $1 \geq \lambda \geq \beta \geq \delta \geq \gamma \geq \eta \geq \psi \geq 0$.

Fuzzy Subgroups of $\mathbb{Z}_{p^3} \times \mathbb{Z}_{p^3}$

$p(n)$	$\alpha(p)$	keychains
(6)	1	3
$(5,1)$	$p+1$	8
$(4,2)$	p^2+p+1	8
$(3,3)$	p^3+p^2+p+1	4
$(2,2,2)$	p^3+3p^2+2p+1	4
$(3,2,1)$	p^3+2p^2+2p+1	24
$(4,1,1)$	p^2+2p+1	12
$(2,2,1,1)$	$2p^3+4p^2+3p+1$	24
$(3,1,1,1)$	p^3+3p^2+3p+1	16
$(2,1,1,1,1)$	$3p^3+6p^2+4p+1$	20
$(1,1,1,1,1,1)$	$5p^3+9p^2+5p+1$	4

The above table of results gives the number of subchains as a result of the application of the keychains of a given partition to the lattice diagram of $G = \mathbb{Z}_{p^3} \times \mathbb{Z}_{p^3}$. The number of symbols in each keychain that determines the number of fuzzy subgroups of a group G corresponds to the sum $n+m+1$. In this sum 1 refers to the first symbol in each case which is always 1, while $n+m$ is the number of the remaining symbols that may or may not be equal. In this sense it becomes logical to analyze only the $n+m$ symbols according to their characteristics.

The $n+m$ symbols partition the sum $n+m$ in various permutations. We record these symbols in braces according to their multiplicities. For instance $(3,2,1)$ means there are three distinct symbols occurring in multiplicities as recorded in the braces. It is observed that all keychains of a particular partition yield the same number of fuzzy subgroups of a group G. We use counting to find the number of keychains corresponding to a certain partition for a given group G. By counting, the partition $(2,2,1,1)$, for instance, yields the number $\dfrac{4!}{2!\,2!}$. The First symbol may be smaller or equal to 1, while the last symbol may be greater or equal to 0. This yields four choices. Thus we have $4(\dfrac{4!}{2!\,2!})$ keychains of G determined by the partition of type

$(2,2,1,1)$ as evidenced by 24 in the keychains column. A typical keychain with this partition type is $1\lambda\lambda\beta\beta\delta\gamma$ or $111\lambda\beta\beta0$ etc.

Now we flag all the chains of G with keychains of a specified partition and count the resultant number of fuzzy subgroups. It can be noted that all keychains with a partition determined by $(5,1)$ yield only $p+1$ fuzzy subgroups. Such keychains are $111111\lambda, 1\lambda\lambda\lambda\lambda\lambda\beta, 1100000$, etc., eight of them.

For instance, all the keychains of the form $111\lambda\lambda\beta\beta; 111\lambda\lambda00; 1\lambda\lambda\beta\beta\delta\delta; 1\lambda\lambda\beta\beta00$ would yield p^3+3p^2+2p+1 chains of subgroups. It is not difficult to see that these are the only distinct equivalence classes of fuzzy subgroups of this form on $\mathbb{Z}_{p^3}\times\mathbb{Z}_{p^3}$. Other equivalence classes of fuzzy subgroups determined by each partition can be read off from the table.

It should be noted that the sum of the entries in the column labelled *keychains* is $2^{n+1}-1$, in agreement with the results in Chapter 5. Also, the entries in the column labelled $p(n)$ and those of column keychains are related to each other in the following way: The multiplication of the quotient of the sum of distinct pins, as indicated by each partition, and the product of the factorials of the pins' multiplicities by 4 gives rise to the column named keychains.

Thus if $n+m=k_1+k_2+\ldots+k_l$ for any positive integers k_i with k_i's distinct, then by $(k_1,k_2,\ldots,k_\ell)$ is meant a keychain of the form $\lambda_1^{k_1}\lambda_2^{k_2}\ldots\lambda_\ell^{k_\ell}$, where $\lambda_1^{k_1}$ has the usual meaning $\overbrace{\lambda_1\lambda_1\ldots\lambda_1}^{k_1}$. Hence for any partition $(k_1,k_2,\ldots,k_\ell)$ of n, there are

$$4\{\frac{\sharp\lambda_i!}{k_1!\,k_2!\ldots k_\ell!}\} \qquad i=1,2,\ldots,\ell \tag{6.1}$$

corresponding equivalence classes of fuzzy subgroups. If, however, k_i's are repeated say a_i times, then the formula for the number of equivalence classes of fuzzy subgroups becomes

$$4\left\{\frac{\sharp\lambda_i!}{a_1!\,a_2!\,\ldots\,a_l!(k_1!)^{a_1}\,(k_2!)^{a_2}\ldots(k_\ell!)^{a_l}}\right\} \qquad i=1,2,\ldots,\ell \tag{6.2}$$

(We note that λ_1 may be smaller or equal 1, and λ_ℓ may or may not be zero. This gives us four choices of the keychains, which accounts for the 4 in the product in equation 6.1).

For instance, the partition $(2,2,2)$ in the above table tells us there are $4p^3+12p^2+8p+4$ corresponding fuzzy subgroups.

Procedure: (To explain the formulas in column 2 of the table, marked $\alpha(n)$)
All chains of $G=\mathbb{Z}_{p^3}\times\mathbb{Z}_{p^3}$ are of the form

$$\{0\}=G_0\subset G_1\subset G_2\subset\ldots\subset G_5\subset G_6=G$$

where $\{0\}$ is a trivial subgroup; G is a whole group, while $G_i,\ \ i=1,2,\ldots,5$ comprise $p+1,\ \ p^2+p+1,\ \ p^3+p^2+p+1,\ \ p^2+p+1,\ \ p+1$ subgroup generators of G, respectively. In counting the number of fuzzy subgroups of G, we apply keychains of length 7 to the subgroup lattice of G. As has been explained earlier, there are 2^7-1 such keychains, with partitions as given by column 1 of the table. These keychains are described by

$$1=\lambda_0\geq\lambda_1\geq\lambda_2\geq\ldots\geq\lambda_5\geq\lambda_6\geq 0$$

Let μ be a fuzzy subset and let $x\in G$. Now we say μ is a fuzzy subset associated with the pinned flag

$$\{0\}^1\subset G_1^{\lambda_1}\subset G_2^{\lambda_2}\subset\ldots\subset G^{\lambda_6}$$

and is denoted in the manner shown in equation 5.3.
A partition of type $(4,1,1)$ refers to keychains of the kind
$11111\lambda\beta,\ \ 1\lambda\beta\delta\delta\delta\delta,\ \ 1\lambda\beta\beta\beta\beta 0,$ etc. The result of the application of these keychains is p^2+2p+1 fuzzy subgroups of G for each keychain. Below is a representation of these fuzzy subgroups of G:

$$\mu_1(x)=\begin{cases}1 & x\in G_4\\ \lambda & x\in G_5\setminus G_4\\ \beta & \text{otherwise}\end{cases}\quad \mu_2(x)=\begin{cases}1 & x\in\{0\}\\ \lambda & x\in G_1\setminus\{0\}\\ \beta & x\in G_2\setminus G_1\\ \delta & \text{elsewhere}\end{cases}\quad \mu_3(x)=\begin{cases}1 & x\in\{0\}\\ \lambda & x\in G_1\setminus\{0\}\\ \beta & x\in G_5\setminus G_1\\ 0 & \text{otherwise}\end{cases}$$

$p^2+p+1(p+1)$ $\qquad$ $(p+1)(p+1)$ $\qquad$ $(p+1)(p+1)$

It is clear that a keychain determined by a partition of type $(1,1,1,1,1,1)$ yields fuzzy subgroups equal to the number of maximal chains of G, which is

$5p^3 + 9p^2 + 5p + 1$, and there are four such keychains.
Other fuzzy subgroups of G can be determined in a similar manner.

Thus the total number as described by the table gives the number of distinct fuzzy subgroups of $G = \mathbb{Z}_{p^3} \times \mathbb{Z}_{p^3}$, which is

$$176p^3 + 384p^2 + 320p + 127$$

as will be proved later in this chapter. Δ

Note 6.3.2 All the groups with the property that $n + m = k$, where $k \in \mathbb{Z}^+$, are related to each other. In fact the fuzzy subgroups of one can be used as a check in the enumeration of fuzzy subgroups of a higher group. Thus if $\mathbb{Z}_{p^{n_1}} \times \mathbb{Z}_{p^{m_1}}$ and $\mathbb{Z}_{p^{n_2}} \times \mathbb{Z}_{p^{m_2}}$ are the groups such that $n_1 > n_2$ and $m_1 < m_2$, then the polynomial representation for the number of subgroups of $\mathbb{Z}_{p^{n_2}} \times \mathbb{Z}_{p^{m_2}}$ is nested in that of $\mathbb{Z}_{p^{n_1}} \times \mathbb{Z}_{p^{m_1}}$. For instance, consider $\lambda = (3, 2, 2, 1, 1, 1,)$, for the groups $\mathbb{Z}_{p^7} \times \mathbb{Z}_{p^3}$ and $\mathbb{Z}_{p^8} \times \mathbb{Z}_{p^2}$, we observe that the polynomial for the latter is nested in the polynomial for the former as explained in the following:

In $\mathbb{Z}_{p^7} \times \mathbb{Z}_{p^3}$, the $p^3 + p^2 + p + 1$ subgroups in level 3 give rise to the number of chains in the following way:

$$p^3$$

$$p^2(4p + 1)$$

$$p[p^2 + p(3p + 1) + 1\{p^2 + (p + 1)(2p + 1)\}]$$

$$1[p^2(3p + 1) + (p + 1)\{p^2 + (p + 1)(2p + 1)\}],$$

while in $\mathbb{Z}_{p^8} \times \mathbb{Z}_{p^2}$, they yield the following number of chains:

$$p^2$$

$$p[p + 1(3p + 1)]$$

$$1[p^2 + p(3p + 1) + 1(p^2 + (p + 1)(2p + 1)]$$

as can be read from Table 5, row (32^21^3), up to columns p7p3 and p8p2 respectively. (By pnpm we mean $\mathbb{Z}_{p^n} \times \mathbb{Z}_{p^m}$)

Table 5 illustrates this observation for the case $n + m = 10$, by giving coefficients for the leading term in each case.
For instance, row 43^2 of Table 5 means there are the following number of fuzzy subgroups for each group:

$$\mathbb{Z}_{p^9} \times \mathbb{Z}_p \text{ has } 2p + 1$$

$$\mathbb{Z}_{p^8} \times \mathbb{Z}_{p^2} \text{ has } 3p^2 + 2p + 1$$

$$\mathbb{Z}_{p^7} \times \mathbb{Z}_{p^3} \text{ has } 4p^3 + 3p^2 + 2p + 1$$

$$\mathbb{Z}_{p^6} \times \mathbb{Z}_{p^4} \text{ has } 3p^4 + 4p^3 + 3p^2 + 2p + 1$$

$$\mathbb{Z}_{p^5} \times \mathbb{Z}_{p^5} \text{ has } p^5 + 3p^4 + 4p^3 + 3p^2 + 2p + 1$$

Example 6.3.3 If we let k_i, for $i = 1, \ldots, 10$ represent the number of parts in $p(10)$, then Table 5 shows that the group $\mathbb{Z}_{p^7} \times \mathbb{Z}_{p^3}$ has the following number of subgroups for each k_i:

$$\begin{aligned}
i &= 1 \rightarrow 3 \\
i &= 2 \rightarrow 20p^3 + 28p^2 + 36p + 36 \\
i &= 3 \rightarrow 300p^3 + 336p^2 + 288p + 144 \\
i &= 4 \rightarrow 1680p^3 + 1568p^2 + 1008p + 336 \\
i &= 5 \rightarrow 4900p^3 + 3920p^2 + 2016p + 504 \\
i &= 6 \rightarrow 8400p^3 + 5880p^2 + 2520p + 504 \\
i &= 7 \rightarrow 8820p^3 + 5488p^2 + 2016p + 336 \\
i &= 8 \rightarrow 5600p^3 + 3136p^2 + 1008p + 144 \\
i &= 9 \rightarrow 1980p^3 + 1008p^2 + 288p + 36 \\
i &= 10 \rightarrow 300p^3 + 140p^2 + 36p + 4
\end{aligned}$$

This number is easily seen to be equal to

$$256(125)p^3 + 512(42)p^2 + 1024(9)p + 2048 - 1$$

as suggested by Theorem 6.4.1 below. Δ

We are now in a position to give formal proofs for the results on fuzzy subgroups with the application of the theory learned in Chapter 5 .

6.3.1 Fuzzy Subgroups of $\mathbb{Z}_{p^n} \times \mathbb{Z}_p$

Lemma 6.3.4 *$G = \mathbb{Z}_p \times \mathbb{Z}_p$ has $4p + 7$ distinct fuzzy subgroups.*

Proof. Each of the maximal chains of $\mathbb{Z}_p \times \mathbb{Z}_p$ has only three levels. By Lemma 5.2.1 and by example 6.3.1, the three symbols will give rise to 7 keychains. Of the 7, three will yield identical fuzzy subgroups. These are keychains of the form $1 \geq \lambda_1 = \lambda_2 \geq 0$. The remaining four will each give rise to different fuzzy subgroups. Thus according to Lemma 5.2.1, there will be $4(p+1)+3$ fuzzy subgroups as claimed in the proposition. □

We notice that for $n = 3$, for instance, there are

$$4(3p + 1) + 12(2p + 1) + 12(p + 1) + 3 = 48p + 31$$

fuzzy subgroups of $\mathbb{Z}_{p^n} \times \mathbb{Z}_p$. Hence we make the following remark:

Remark: The number of fuzzy subgroups of $G = \mathbb{Z}_{p^n} \times \mathbb{Z}_p$ for any positive integer n can be read off from the following triangle. The triangle looks like that of Pascal's except that the last entry 1 is missing from all the rows. This triangle is called a *beheaded Pascal triangle read by beheaded rows* "Wouter Meeussen" A074909.
Please note that naturally the initial 1 is missing from this triangle but was added by Sloane [79] at the suggestion of Paul Barry.

$$\begin{array}{c} 1 \\ 1 \quad 2 \\ 1 \quad 3 \quad 3 \\ 1 \quad 4 \quad 6 \quad 4 \\ 1 \quad 5 \quad 10 \quad 10 \quad 5 \\ \vdots \end{array}$$

For each row, let a_i be the entry number and let r be the row number while $n \in \mathbb{Z}^+$. Hence $G = \mathbb{Z}_{p^n} \times \mathbb{Z}_p$ has

$$\sum_{r=1,i=1}^{n} 4a_i(rp + 1) + 3 \text{ fuzzy subgroups.} \tag{6.3}$$

[It is important to note that the entries of the sequence A074909 forming the triangle above, which happen to coincide with those of our work, were found in another context different from ours.]

In terms of the notation involving triangles, an alternative formula for the number of fuzzy subgroups of $\mathbb{Z}_{p^n} \times \mathbb{Z}_p$ is:

$$pnp \text{ has } 4\left\{\sum_{k=1}^{n}(kp+1).* \;\; T'_n\right\} + 3 \text{ fuzzy subgroups,} \tag{6.4}$$

where T'_n is the reversed n-th row of a beheaded Pascal's triangle.

We are interested in the combinatorial formula and the relation of fuzzy subgroups with the maximal chains.

Hence we state the following result, and prove it by induction:

Theorem 6.3.5 *There are* $2^{n+1}C(n,1)p+2^{n+2}-1$ *fuzzy subgroups of* $G = \mathbb{Z}_{p^n} \times \mathbb{Z}_p$.

Proof. (By induction on n). When $n = 1$, the formula yields $4p+7$ fuzzy subgroups in agreement with Lemma 6.3.4. We assume that the result is valid for a positive integer k, that is $G = \mathbb{Z}_{p^k} \times \mathbb{Z}_p$ contains $2^{k+1}C(k,1)p + 2^{k+2} - 1$ fuzzy subgroups. $\mathbb{Z}_{p^k} \times \mathbb{Z}_p$ has $k+2$ levels with $(k+2)$-th level consisting of the whole group, whereas $\mathbb{Z}_{p^{k+1}} \times \mathbb{Z}_p$ has $p+1$ subgroups in the $(k+2)$-th level with whole group $\mathbb{Z}_{p^{k+1}} \times \mathbb{Z}_p$ being in the $(k+3)$-th level.

We first identify $\mathbb{Z}_{p^k} \times \{e\}$ by $\mathbb{Z}_{p^k}$, and consider $\mathbb{Z}_{p^{k+1}} \times \mathbb{Z}_p$ as an extension of $\mathbb{Z}_{p^k} \times \mathbb{Z}_p$ or $\mathbb{Z}_{p^k}$. Next we determine the number of fuzzy subgroups of $\mathbb{Z}_{p^{k+1}} \times \mathbb{Z}_p$ which are extensions of fuzzy subgroups of $\mathbb{Z}_{p^k} \times \mathbb{Z}_p$. By assumption, there are $2^kC(k,1)p + 2^{k+1}$ fuzzy subgroups whose support is exactly $\mathbb{Z}_{p^k} \times \mathbb{Z}_p$, and there are $2^kC(k,1)p + 2^{k+1} - 1$ fuzzy subgroups whose support is strictly contained in $\mathbb{Z}_{p^k} \times \mathbb{Z}_p$. Let S_1 and S_2 denote the former and latter case respectively. Each fuzzy subgroup in set S_1 yields three fuzzy subgroups of $\mathbb{Z}_{p^{k+1}} \times \mathbb{Z}_p$. The extensions of their keychains are given by $(\lambda_0, \lambda_1, \ldots, \lambda_{k+1}, \lambda_{k+1})$, $(\lambda_0, \lambda_1, \ldots, \lambda_{k+1}, \lambda_{k+2})$, where $0 < \lambda_{k+2} < \lambda_{k+1}$ and $(\lambda_0, \lambda_1, \ldots, \lambda_{k+1}, 0)$. Each fuzzy subgroup in set S_2 yields only one fuzzy subgroup of $\mathbb{Z}_{p^{k+1}} \times \mathbb{Z}_p$ as can be easily seen. The number of extensions is thus $4[2^kC(k,1)p + 2^{k+1}] - 1$.

Lastly we consider the extensions of $\mathbb{Z}_{p^k}$. The group $\mathbb{Z}_{p^k}$ has $2^{k+1}-1$ fuzzy subgroups.

Let S_3 denote the set of fuzzy subgroups whose support is exactly $\mathbb{Z}_{p^k}$. The case of those fuzzy subgroups whose support is strictly contained in $\mathbb{Z}_{p^k}$ has already been accounted for in the previous case. The order of S_3 is 2^k. Each fuzzy subgroup in set S_3 yields four fuzzy subgroups of $\mathbb{Z}_{p^{k+1}} \times \mathbb{Z}_p$, with their keychains extended thus $(\lambda_0, \lambda_1, \ldots, \lambda_k, \lambda_{k+1}, \lambda_{k+2})$, where $0 \leq \lambda_{k+2} < \lambda_{k+1} \leq \lambda_k$. Hence S_3 results in $4(2^k p)$ number of extensions. Thus the total number of fuzzy subgroups of $\mathbb{Z}_{p^{k+1}} \times \mathbb{Z}_p$ is

$$\begin{aligned} 4[2^k C(k,1)p + 2^{k+1}] - 1 + 4(2^k p) &= 2^{k+3} + p(k+1)2^{k+2} - 1 \\ &= 2^{k+2} C(k+1,1)p + 2^{k+3} - 1. \end{aligned}$$

This completes the induction. □

6.3.2 Fuzzy Subgroups of $\mathbb{Z}_{p^n} \times \mathbb{Z}_{p^2}$

We next prove the result for the case $m = 2$, hereunder stated

Theorem 6.3.6 *The group $G = \mathbb{Z}_{p^n} \times \mathbb{Z}_{p^2}$ has*

$$2^{n+1}[C(n,2) + 2C(n-1,1)]p^2 + 2^{n+2}C(n+1,1)p + 2^{n+3} - 1 \tag{6.5}$$

fuzzy subgroups.

Proof. (We prove by induction on n). For $n = 1$, the formula gives $16p + 15$ in agreement with the number obtained by taking $n = 2$ in Theorem 6.3.5. We next assume that the formula holds for the case $n = k > 1$. We need to show that the formula is valid for $n = k + 1$. To do this, we count all possible extensions of fuzzy subgroups in disjoint sets S_1, S_2 and S_3 which will exhaust all fuzzy subgroups of G with $n = k + 2$.

Now, the number of S_1-extensions from $\mathbb{Z}_{p^k} \times \mathbb{Z}_{p^2}$ to $\mathbb{Z}_{p^{k+1}} \times \mathbb{Z}_{p^2}$ is

$$4(2^k[C(k,2) + 2C(k-1,1)]p^2 + 2^{k+1}C(k+1,1)p + 2^{k+2}) - 1 \tag{6.6}$$

The number of S_2-extensions from $\mathbb{Z}_{p^k} \times \mathbb{Z}_p$ to $\mathbb{Z}_{p^{k+1}} \times \mathbb{Z}_{p^2}$ are found by referring to the previous theorem for the number of fuzzy subgroups of $\mathbb{Z}_{p^k} \times \mathbb{Z}_p$ together with four keychain extensions that end with pins of the form $\lambda\lambda\beta, \lambda\lambda 0, \lambda\beta\delta$ and $\lambda\beta 0$, where $0 < \delta < \beta < \lambda$, yielding

$$4(2^kC(k,1)p + 2^{k+1})p \tag{6.7}$$

With the exception of the maximal chain through $\mathbb{Z}_{p^k} \times \mathbb{Z}_{p^2}$ which has already been counted under S_1, there are p flags which extend from $\mathbb{Z}_{p^k} \times \mathbb{Z}_p$ to $\mathbb{Z}_{p^{k+1}} \times \mathbb{Z}_{p^2}$, hence the factor p in the above expression.

The set S_3 yields p cases corresponding to level $k+1$. Each of these cases yields $8(2^k)p$ fuzzy subgroups. To justify this number, we pick only one of the p cases for illustration, namely the number of all possible extensions from $\mathbb{Z}_{p^k}$ to $\mathbb{Z}_{p^{k+1}} \times \mathbb{Z}_{p^2}$. There are eight keychain extensions ending with

$$\lambda\lambda\beta\beta, \lambda\lambda 00, \lambda\lambda\beta\delta, \lambda\lambda\beta 0, \lambda\beta\beta\delta, \lambda\beta\beta 0, \lambda\beta\delta\gamma, \quad \text{and} \quad \lambda\beta\delta 0,$$

where $0 < \gamma < \delta < \beta < \lambda$, accounting for the 8 in the product. Only one maximal chain connects $\{0\}$ to $\mathbb{Z}_{p^k}$ and it yields $2^{k+1}-1$ fuzzy subgroups on that particular flag. There are, however, only 2^k keychains ending with non-zero pins that will contribute to fuzzy subgroups, not counted already, of $\mathbb{Z}_{p^{k+1}} \times \mathbb{Z}_{p^2}$. Finally, there are p flags from $\mathbb{Z}_{p^k}$ to $\mathbb{Z}_{p^{k+1}} \times \mathbb{Z}_{p^2}$ which have not been counted before, hence the factor p in the product. Thus S_3 has $p(8(2^k)p) = 8(2^k)p^2$ fuzzy subgroups. Therefore the total number of fuzzy subgroups in all three cases S_1, S_2, S_3 is

$$2^{k+2}[C(k+1,2) + 2C(k,1)]p^2 + 2^{k+3}C(k+2,1)p + 2^{k+4} - 1 \tag{6.8}$$

□

We next consider the effect of increment of m,and for any n.

6.4 Fuzzy Subgroups of $\mathbb{Z}_{p^n} \times \mathbb{Z}_{p^m}$ for $3 \leq m \leq 5$

We state the following results that pertain to the value of any positive integer n and $3 \leq m \leq 5$. The results can be proved with similar argument as in Theorem 6.3.6:

Theorem 6.4.1 *There are*

$$2^{n+1}[C(n,3) + 4C(n-1,2) + 6C(n-2,1)]p^3 +$$
$$2^{n+2}[C(n+1,2) + 2C(n,1)]p^2 + 2^{n+3}C(n+2,1)p + 2^{n+4} - 1$$

fuzzy subgroups of group $G = \mathbb{Z}_{p^n} \times \mathbb{Z}_{p^3}$.

Theorem 6.4.2 *The group $G = \mathbb{Z}_{p^n} \times \mathbb{Z}_{p^4}$ has*

$$\begin{aligned} 2^{n+1}[C(n,4) + 6C(n-1,3) + 16C(n-2,2) + 22C(n-3,1)]p^4 + \\ 2^{n+2}[C(n+1,3) + 4C(n,2) + 6C(n-1,1)]p^3 + \\ 2^{n+3}[C(n+2,2) + 2C(n+1,1)]p^2 + 2^{n+4}C(n+3,1)p + 2^{n+5} - 1 \end{aligned}$$

fuzzy subgroups.

Theorem 6.4.3 *$G = \mathbb{Z}_{p^n} \times \mathbb{Z}_{p^5}$ has*

$$\begin{aligned} 2^{n+1}[C(n,5) + 8C(n-1,4) + 30C(n-2,3) + 68C(n-3,2) + 90C(n-4,1)]p^5 + \\ 2^{n+2}[C(n+1,4) + 6C(n,3) + 16C(n-1,2) + 22C(n-2,1)]p^4 + \\ 2^{n+3}[C(n+2,3) + 4C(n+1,2) + 6C(n,1)]p^3 + \\ 2^{n+4}[C(n+3,2) + 2C(n+2,1)]p^2 + 2^{n+5}C(n+4,1)p + 2^{n+6} - 1 \end{aligned}$$

fuzzy subgroups.

Based on the observation of the results and on the amount of data pertaining to this work, which has been checked by means of a computer program, we conjecture that the **general formula** for the number of fuzzy subgroups of $\mathbb{Z}_{p^n} \times \mathbb{Z}_{p^m}$ should be

$$\left\{ \sum_{j=0}^{m-1} 2^{n+1}[C(n-j, m-j)] \cdot * \ T_m \right\} p^m + p(n+1)p(m-1),$$
$$\text{with } p(n+1)p(0-1) = 2^{n+m+1} - 1 \qquad (6.9)$$

where T_m is the $m-$th row of a Schroeder's triangle (see Sloane [79], A033877), $p(n+1)p(m-1)$ is the number of fuzzy subgroups of $\mathbb{Z}_{p^{n+1}} \times \mathbb{Z}_{p^{m-1}}$, and $.*$ is the usual pointwise multiplication. The array (A033877) is described mathematically in the following way:

$$T(n,k) = \begin{cases} 0 \quad \text{if } k < n \\ \\ T(n,k-1) + T(n-1,k-1) + T(n-1,k) \quad \text{otherwise} \end{cases} \qquad (6.10)$$

and

$$T(1,*) = 1.$$

For the first few rows, the array reads as follows:

$$\begin{array}{c}
1 \\
1 \quad 2 \\
1 \quad 4 \quad 6 \\
1 \quad 6 \quad 16 \quad 22 \\
1 \quad 8 \quad 30 \quad 68 \quad 90 \\
1 \quad 10 \quad 48 \quad 146 \quad 304 \quad 394 \\
1 \quad 12 \quad 70 \quad 264 \quad 714 \quad 1412 \quad 1806 \\
\vdots
\end{array}$$

This array is associated with several sequences, [79]. For instance a sequence obtained by considering the last entry to the right in each row, namely $1, 2, 6, 22, 90, 394, \ldots$ is generally called the Large Schroeder Numbers. Also summing the entries in each row (row sums) generates a sequence which grows rapidly in the values of its terms. This sequence is commonly called Schroeder's second problem (generalized parenthesis) or sometimes called Super-Catalan numbers or little Schroeder numbers. There are various other interpretations of these types of numbers. H. Bottomley gave a graphical illustration of the initial terms ([79], A033877). The other sequence associated with this array is called *Royal paths in a lattice* and consists of the terms $1, 4, 16, 68, 304, 1412, \ldots$. Numerous works have been done around this array by Schroeder himself and various other mathematicians. All this can be found by visiting the site [79].

6.5 Conclusion

The subgroup lattices of finite Abelian groups of rank two are $n \times m$ 2-dimensional diagrams with $n + m + 1$ levels of subgroups (see examples at the back). Each subgroup lattice of a group G is a result of the 180^0 orientation of a tree diagram of cyclic subgroups of G and merging the two, which explains the point of symmetry.

The number of subgroups at each level on the subgroup lattice occur in increasing polynomials of p with coefficients of 1 up to the point of symmetry. The number of maximal chains and fuzzy subgroups of G is a polynomial in prime p whose coefficients are of the form $A_i, \ \ i = 0, \ldots, m$, where A_i can be expressed as a sum of the binomial coefficients. The coefficients of A_m, the leading coefficient, for maximal chains and subgroups of G come from the Catalan triangle and Schroeder triangle read by rows respectively. The coefficients of the other A_i's follow by recursion for each group.

The subgroup lattices of G can be converted into binary tree diagrams which do not depend on the value of p, thus facilitating counting of chains to a great extent.

Chapter 7

Graphs, Generators and Relations

7.1 Introduction

From its initiation, the theory of groups has provided an interesting and powerful abstract approach to the study of the symmetries of various configurations. As a result there is a prolific interaction between groups and graphs. The first paper on graph theory is reported to have been written by Euler in 1736. Contrary to being perceived as a dead field some centuries ago, graph theory has come out as a powerful component of mathematics over the past decades.

It is the above stated interaction as well as the perception of our lattices as graphs that led us to the consideration of the treatment as outlined in this and the following chapter.

As has become a tradition, we introduce and lay out a collection of ground work to the topic by a number of experts in the field. Most of the notation used in this chapter, although it has become conventional, has been borrowed from various authors including Harary [38], Rosen [72] to name a few.

7.2 Graph Terminology

The terminology introduced hereunder will be useful in solving many different problems. Problems that come to light include determining whether a graph is *planar* (i.e can be drawn in the plane so that no two of its *edges* cross) or not, and deciding whether there is a one-to-one correspondence between the *vertices* of two graphs that produces an *isomorphism* between the edges of the graphs.

Definition 7.2.1 *A graph G is generally an ordered pair (V, E), where V is a finite set of vertices, and E is a set of unordered pairs of distinct elements of V called edges.*

In simple terms we view a graph G as a finite set of dots (called vertices) that are connected by links (called edges).
In fact we will notice in the subsequent sections that a third item, namely a function, is necessary in the definition of a graph. Hence we will write $G = (V, E, \alpha)$, where α is a function on V, E.

Definition 7.2.2 *Let G be an undirected graph. Two vertices v_1 and v_2 in G are said to be adjacent if $\{v_1, v_2\}$ is an edge of G. The edge $\{v_1, v_2\}$ is said to be incident with the vertices v_1 and v_2, and v_1, v_2 are called the endpoints of $\{v_1, v_2\}$.*

It is often necessary to keep track of how many edges are incident to a vertex (valency of a vertex). The valency of a vertex, $\delta(v)$, in an undirected graph is the number of edges incident with it.
A vertex of valency 0 is called *isolated*. A vertex is *pendant* if and only if it has valency 1.
When we add the valencies of all the vertices in $G = (V, E)$, each edge contributes 2 to the sum; that is, if $G = (V, E)$, then

$$\Sigma\delta(v) = 2|E|, \;\; v \in V. \text{ (Handshaking Theorem.)}$$

Note 7.2.3 The number of odd valency in any undirected graph is always even.

In directed graphs, when $\{v_1, v_2\}$ is an edge of the graph G, v_1 is said to be adjacent to v_2 while v_2 is said to be adjacent from v_1. Thus v_1 and v_2 are called the initial and terminal vertex of (v_1, v_2) respectively. Hence we speak of the in-valency (or out-valency) of a vertex v denoted by $\delta^-(v)$ (respectively $\delta^+(v)$) to mean the number of edges with v as their terminal (or initial) vertex.

Note 7.2.4 If $G = (V, E)$ is a directed graph, then

$$\Sigma\delta^-(v) = \Sigma\delta^+(v) = \mid E \mid, \ \ v \in V.$$

Examples of simple graphs include *complete graph*, *cycle*, *wheel*, *n-Cube*.

Sometimes a graph has the property that its vertex set can be partitioned into two disjoint nonempty subsets such that every edge in the graph connects a vertex in one of these subsets to a vertex in the other. Such a simple graph is called *bipartite.* $k_{m,n}$, for example, is a complete bipartite graph whose vertex set is partitioned into two subsets of m and n respectively.

Sometimes only part of a graph is needed to solve a problem. When edges and vertices are removed from a graph, without removing endpoints of any remaining edges, a smaller graph called a subgraph of the original graph is obtained. Thus a subgraph of a graph $G = (V, E)$ is a graph $H = (W, F)$, where $W \subseteq V$ and $F \subseteq E$.

Two or more graphs can be combined in various ways to form a new graph (the *union* of the graphs) that contains all the edges and vertices of these graphs. Thus if $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ then

$$G_1 \cup G_2 = (V_1 \cup V_2, E_1 \cup E_2).$$

A simple graph is called *regular* if every vertex of the graph has the same valency.

7.3 Isomorphic Graphs

There are several ways to represent graphs. Sometimes two graphs have exactly the same form in the sense that there is a one-to-one correspondence between their vertex sets that preserves edges. Such graphs are said to be *isomorphic.* The study of whether graphs are isomorphic is an important problem in graph theory.

The useful representation of the graph and a tool to deciding isomorphism is the *adjacency matrix.*

However, powerful as this tool is, we have found our graphs too complex for this representation. Our graphs result in huge matrices that are not easy to manipulate. The theory remains valid as we will discuss.

Definition 7.3.1 *Suppose $G = (V, E)$ is a simple graph with n vertices, and suppose that vertices of G are listed as $v_1, v_2, \ldots, v_n$. Then the* adjacency *matrix A of G with respect to this listing is the nxn zero-one matrix whose (i, j)-th entry, a_{ij} is*

$$a_{ij} = \begin{cases} 1 & \text{if } \{v_i, v_j\} \text{ is an edge of } G \\ \\ 0 & \text{otherwise} \end{cases} \tag{7.1}$$

There is no unique adjacency matrix for any given graph. For instance, there are $n!$ different adjacency matrices for a graph with n vertices since there are $n!$ different orderings of n vertices.

Another common way to represent graphs is to use incidence matrix which is an $n \times n$ matrix $M = [m_{ij}]$ with entries defined by

$$m_{ij} = \begin{cases} 1 & \text{when } e_j \text{ is incident with } v_i \\ \\ 0 & \text{otherwise} \end{cases} \tag{7.2}$$

Definition 7.3.2 *The simple graphs $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ are isomorphic if there is a one-to-one correspondence f from V_1 to V_2 with the property that a and b are adjacent in G_1 if and only if $f(a)$ and $f(b)$ are adjacent in G_2, for all $a, b \in V_1$.*

Since there are $n!$ possible one-to-one correspondences between the vertex sets of two simple graphs with n vertices, it is often difficult to test whether two simple graphs are isomorphic. There are three criteria, technically called *invariants*, for deciding isomorphism. They are, **same number of vertices**, or **same number of edges**, or **same valencies of vertices**. It is relatively simple to show that two simple graphs are not isomorphic. This is done by showing that they do not share a property called an *invariant* with respect to isomorphism.

Remark: If these invariants are not the same in two simple graphs, the graphs cannot be isomorphic. We noticed this fact in group theory, where we said that if two finite Abelian p-groups do not have the same invariants then they are not isomorphic. However, when these invariants are the same, it does not necessarily mean the two graphs are isomorphic.

7.4 Connectivity

Another important area of graph theory is the concept of *connectivity.* There is an in depth study of the concept and many results discovered around this topic. Perhaps the most outstanding result is a classical result of Menger which deals with the number of disjoint paths connecting a given pair of vertices in a graph. Since then there have been variations of this result, with several of them discovered in areas of mathematics other than graph theory itself. We begin by defining what is meant by a connected graph.

Definition 7.4.1 *A graph G is said to be connected if every pair of vertices are joined by a path.*

7.5 Background of Generators and Relations

The idea of graphical representation of a group by a set of generators and relations was invented by Cayley in the nineteenth century to provide a method to visualize a graph. The idea connects two important branches of mathematics, groups and graphs.

The theory of *generators and relations* offers a convenient way to define a group with certain prescribed properties.

The following is a procedure as set out in [30]:

- Start with a set of elements that should generate the group, as well as a set of equations, the *relations*, that specify the conditions these generators should satisfy;

- Select the largest of such possible groups. This will uniquely determine the group up to isomorphism.

To illustrate the procedure we cite the following example:

Example 7.5.1 We say that $\mathbb{Z}_{2^2} \times \mathbb{Z}_2$ is generated by the elements f and g that satisfy the conditions $f^4 = g^2 = e$ and $fg = gf$. Any other relation between f and g can be derived from these equations. This shows that $\mathbb{Z}_{2^2} \times \mathbb{Z}_2$ is uniquely described. Δ

7.5.1 Definition

In his book, Gallian [30] defines the generators and relations in the following manner:

Definition 7.5.2 *Suppose G is a group generated by a certain set $A = \{a_1, a_2, \cdots, a_n\}$ and let F be the* free *group on A. Let $W = \{w_1, w_2, \cdots, w_r\}$ be a subset of F and let N be the smallest normal subgroup of F containing W. Then G is said to be given by the generators $a_1, a_2, \ldots, a_n$ and the relations $w_1 = w_2 = \cdots = w_r = e$ if there exists an isomorphism, say α, defined by*

$$\alpha : F/N \rightarrow G \;\; \textit{such that} \;\; a_iN \rightarrow a_i \tag{7.3}$$

Some suggestive notation is

$$G = \langle a_1, a_2, \cdots, a_n \mid w_1 = w_2 = \cdots = w_r = e \rangle. \tag{7.4}$$

Remark: The group of integers, $\mathbb{Z}$, is the only nontrivial Abelian group that is free (on one letter), (i.e $\mathbb{Z} \approx \langle a \rangle$).

Gallian [30] goes further to illustrate the advantages and disadvantages of this procedure.

7.5.2 Advantages and Disadvantages

Every idea has its pros and cons. However, we concentrate on the positive.
The advantages of using generators and relations to define groups include among other things the following:

- groups defined by the method of generators and relations come out in a natural way;
- it is often convenient to construct examples as well as counterexamples.

Brilliant as the idea sounds, there are often disadvantages attached to it. The method of generators and relations to describe a group has the following disadvantages:

1. it is not always easy to decide whether the group so defined is finite or not, and even whether a particular element is the identity or not.
2. the entirely different sets of generators and relations can define the same group, hence making it difficult to decide whether two given generated groups are isomorphic or not.

7.6 Cayley Digraphs

With much said about generators and relations, we move onto the graphs of groups called the *Cayley digraphs*.
We recall that a directed graph, or shortly *digraph*, is a finite set of points called vertices and a set of arrows (or directed edges) connecting some of the vertices.
But what exactly is meant by a Cayley digraph of a group? The following definition is author's perspective in [30], in addressing this question:

Definition 7.6.1 *Suppose G is a finite group and S is a set of generators of G. A digraph Cay(S:G), pronounced as the Cayley digraph of G with generating set S, is a graph satisfying the following properties:*

1. *Each element of G is a vertex of Cayley(S:G)*
2. *For a and b in G there is an arrow from a to b if and only if $as = b$ for some $s \in S$.*

There are several proposals on how to tell from the graph which particular generator connects two vertices. For instance Cayley proposed that a colour be assigned to each generator and that the arrow from a to as be coloured with the same colour assigned to s.

Instead of colours, most authors, including the author of this thesis, prefer the use of different line styles.

7.7 Applications

The application of directed graphs is found in the study of Hamiltonian circuits and paths, courtesy of the Irish mathematician Sir William Hamilton who invented a puzzle called "Around the world" found in many books. For more information on this puzzle one is referred to the literature on graph theory.

Briefly, the study addresses the problem of starting at some vertex on the graph and moving along the arrows of the digraph in such a way that each vertex is visited exactly once before returning to the starting vertex.

Our main concern is the application into the investigation of the existence of Hamiltonian circuits and paths in Cayley digraphs of groups of the form $\mathbb{Z}_{p^n} \times \mathbb{Z}_{p^m}$ for some positive integers m and n. The application to the groups of the form $\mathbb{Z}_m \times \mathbb{Z}_n$ for some positive integers m and n was carried out by Gallian [30].

The following results appear in his text.

Theorem 7.7.1 [30]. *$Cay(\{(1,0),(0,1)\} : \mathbb{Z}_m \times \mathbb{Z}_n)$ does not have a Hamiltonian circuit when $gcd(m,n) = 1$.*

Theorem 7.7.2 [30]. *$Cay(\{1,0),(0,1)\}:\mathbb{Z}_m\times\mathbb{Z}_n)$ has a Hamiltonian circuit when n divides m.*

However, Abelian groups have Hamiltonian paths as stated by the following theorem:

Theorem 7.7.3 [30]. *Let G be a finite Abelian group, and let S be a nonempty generating set for G. Then Cay(S:G) has a Hamiltonian path.*

Another sufficient condition for the existence of Hamilton circuits is stated in the following theorem

Theorem 7.7.4 [72]. *Suppose G is a connected simple graph with at least three vertices. Then G has a Hamilton circuit if the valency of each vertex is at least $\frac{1}{2}n$, where n is the number of vertices in G.*

Theorem 7.7.5 [72]. *Suppose G is a simple graph containing n vertices and m edges satisfying*

$$m \geq \frac{1}{2}(n-1)(n-2)+2.$$

Then G has a Hamilton circuit.

The number of paths between two vertices in a graph can be determined using its adjacency matrix. The following theorem explains how to get the number of different paths of some length from the adjacency matrix of a graph.

Theorem 7.7.6 [72]. *Suppose G is a graph (directed or undirected) whose adjacency matrix A is given according to the ordering $v_1, v_2, \ldots, v_n$ of its vertices. Then the number of different paths of length r from a vertex v_i to some vertex v_j is the (i,j)th entry of the matrix A^r.*

7.8 Symmetric Graphs

[Harary [38]] The symmetry of graphs as a study was invented by Foster [Geometrical circuits of electrical networks, 1932] where he computed a table of symmetric cubic graphs.

In this section we highlight the terminology necessary for the understanding of the concept of symmetry. We begin by defining what is meant by similar vertices and similar edges.

Definition 7.8.1 *Let G be a graph. Two vertices u and v of G are said to be* similar *if there exists an automorphism $\phi : G \to G$ such that $\phi(u) = v$.*
Similarly, two edges $\{u_1, v_1\}$ and $\{u_2, v_2\}$ are said to be similar if there exists an automorphism ϕ of G such that $\phi(\{u_1, v_1\}) = \{u_2, v_2\}$.

The graphs in our consideration have no *isolated* vertices. In terms of symmetry, we speak of the following:

Definition 7.8.2 *A graph G in which every pair of vertices are similar is said to be* point-symmetric*.*
A graph in which every pair of edges are similar is said to be line-symmetric*.*
A graph G which is both point-symmetric and line-symmetric is said to be symmetric*.*

There are interesting results in connection with this study; we will mention some of them.

Proposition 7.8.3 [38]. *Let G be a graph, and let u and v be the vertices of G. If ϕ is an automorphism of G, then $G - u \approx G - v$.*

The result is due to the fact that if ϕ is an automorphism of G, then it can be shown that $G - u$ is isomorphic to $G - \phi(u)$. The converse to the proposition above, however, is not valid.
We next define what is meant by a *line-regular* graph.

Definition 7.8.4 *The valency (δ) of an edge $\{u, v\}$ is the unordered pair ω_1, ω_2, where $\omega_1 = \delta(u)$ and $\omega_2 = \delta(v)$. Now a graph is said to be* line-regular *if all edges have the same valency.*

The following result combines bipartite, line-symmetric and point-symmetric graphs.

Theorem 7.8.5 [38]. *Every line-symmetric graph with no isolated vertices is point-symmetric or bipartite.*

Proof. Let there be a line-symmetric graph G without any isolated vertices. Note that for any edge there are at least k automorphisms mapping the given edge onto the edges of G. For the edge $\{u, v\}$ and the automorphisms $\phi_1, \phi_2, \ldots, \phi_k$, consider the sets $V_1 = \{\phi_1(u), \phi_2(u), \cdots, \phi_k(u)\}$ and $V_2 = \{\phi_1(v), \phi_2(v), \cdots, \phi_k(v)\}$. Now $V_1 \cup V_2 = V$ because G has no isolated points.
The proof is completed by showing that if $V_1 \cap V_2 = \emptyset$, then G is bipartite; and if $V_1 \cap V_2 \neq \emptyset$, then G is point-symmetric. □

We end this section by stating the results pertaining to the line-symmetric graphs as given by the author, for continuity purposes.
Let G be a line-symmetric graph.

1. If the valency of every edge of G is (ω_1, ω_2) where $\omega_1 \neq \omega_2$, then G is bipartite.

2. If G has an odd number of vertices, and the valency of every edge is (ω_1, ω_2) where $\omega_1 = \omega_2$, then G is point-symmetric.

3. If G has an even number of vertices, and G is regular of valency $\omega \geq v/2$, then G is point-symmetric. (v is the number of vertices).

7.9 Terminology for Trees

A graph G with no cycles is said to be *acyclic*. This allows us to define a tree in the following manner:

Definition 7.9.1 *A* tree *is a connected acyclic graph.*

In numerous applications of trees a particular vertex of a tree is designated as the *root*. A tree together with its root produces a directed graph called a *rooted tree*. For a rooted tree T, the concepts of *parent, child, siblings* etc. have a natural meaning. For instance, the parent of a vertex v other than the root is a unique vertex u such that there is a directed edge from u to v. A vertex of a tree is called a *leaf* if it has no children, while vertices that have children are called *internal vertices*. The leaves are all those vertices in T that are pendant.

Definition 7.9.2 *A rooted tree is called an m-ary tree if every internal vertex has no more than m children. The tree is called a full m-ary tree if every internal vertex has exactly m children.*

The following are the well-known properties of trees, and we hereby state them in the form of theorems (without proof), which they are.
The following Theorem 7.9.3 lists the properties of these graphs, all of which are equivalent.

Theorem 7.9.3 [38]. *Let $H = (V, E)$ be a graph of order $n > 2$. The following properties, each of which characterizes a tree, are equivalent.*

1. *H is connected and has no cycles*

2. *H has $n - 1$ edges and has no cycles*

3. *H is connected and contains exactly $n - 1$ edges*

4. *H is connected, and if any edge is removed, the remaining graph is not connected*

5. *H has no cycles, and if an edge is added to H, exactly one cycle is created*

6. *Every pair of vertices of H is connected by a unique chain.*

Theorem 7.9.4 [72]. *A full m-ary tree with i internal vertices contains $n = mi + 1$ vertices.*

Theorem 7.9.5 [72]. *A full m-ary tree with*

1. *n vertices has $i = \frac{n-1}{m}$ internal vertices and $\ell = \frac{(m-1)n+1}{m}$ leaves.*

2. *i internal vertices has $n = mi + 1$ vertices and $l = (m - 1)i + 1$ leaves.*

3. *ℓ leaves has $n = \frac{m\ell-1}{m-1}$ vertices and $i = \frac{\ell-1}{m-1}$ internal vertices.*

Whilst on the terminology for trees, it is important to define the following terms that are met frequently in the discussion.

Definition 7.9.6 *The* level *of a vertex v in a rooted tree is the length of the unique path from the root to the vertex v. The* height *of a rooted tree is length of the longest path from the root to any vertex. A tree is called a* labeled tree *if each of its vertices is assigned a label.*

Theorem 7.9.7 [38]. *In a tree, any pair of vertices is connected by a unique path.*

Based on this information we analyze the graphs of finite Abelian groups of rank two (in the next chapter).

Chapter 8

Graph Theoretical Analysis of Finite Abelian Groups of Rank Two

8.1 Introduction

In this chapter we give a brief examination of the subgroup lattices of finite Abelian groups of rank two from a graph theoretic point of view. We apply some graph description available in the literature and see how well they suit our subgroup lattices. We notice that the description as explained in example 8.1.1 becomes too cumbersome for our complex subgroup lattices. We count from the subgroup lattices some practical structures including leaves, edges, valencies, and others. We do this in a view to characterizing the subgroup lattices as graphs, that is, what type of graphs they turn out to be.

8.1.1 Graph Description

As a build up, we go through some important terminology for graphs.
In Section 7.2 we should have described a graph G as an ordered triple (V, E, φ) in which

- $V = V(G)$ is a nonempty set of vertices of G,

- $E = E(G)$, with $E(G) \cap V(G) = \emptyset$, is a set of edges,

- φ_G is an incidence function which associates with each edge of G a not necessarily distinct unordered pair of vertices of G.

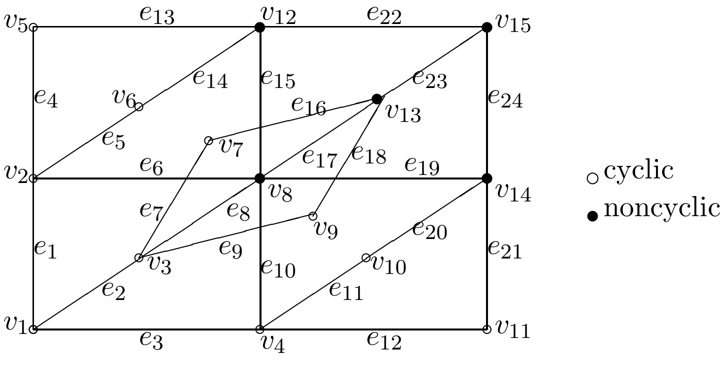
Thus, if e is an edge and u and v are vertices such that $\varphi_G(e) = uv$, then e is said to join u and v, whence u and v are called the *endpoints* of e.
When the context is clear, we shall drop the subscripts and also write for instance V to mean $V(G)$, and so on.

Example 8.1.1 Consider a graph $G = (V, E, \varphi)$ where,

$$V = \{v_i \in G : i = 1, \cdots, 15\}, E = \{e_i \in G : i = 1, \cdots, 24\} \tag{8.1}$$

and φ_G is defined by

$$\begin{aligned}
\varphi_G(e_1) &= v_1v_2, \ \ \varphi_G(e_2) = v_1v_3, \ \ \varphi_G(e_3) = v_1v_4, \ \ \varphi_G(e_4) = v_2v_5, \\
\varphi_G(e_5) &= v_2v_6, \ \ \varphi_G(e_6) = v_2v_8, \ \ \varphi_G(e_7) = v_3v_7, \ \ \varphi_G(e_8) = v_3v_8, \\
\varphi_G(e_9) &= v_3v_9, \ \ \varphi_G(e_{10}) = v_4v_8, \ \ \varphi_G(e_{11}) = v_4v_{10}, \ \ \varphi_G(e_{12}) = v_4v_{11}, \\
\varphi_G(e_{13}) &= v_5v_{12}, \ \ \varphi_G(e_{14}) = v_6v_{12}, \ \ \varphi_G(e_{15}) = v_8v_{12}, \ \ \varphi_G(e_{16}) = v_7v_{13}, \\
\varphi_G(e_{17}) &= v_8v_{13}, \ \ \varphi_G(e_{18}) = v_9v_{13}, \ \ \varphi_G(e_{19}) = v_8v_{14}, \ \ \varphi_G(e_{20}) = v_{10}v_{14}, \\
\varphi_G(e_{21}) &= v_{11}v_{14}, \ \ \varphi_G(e_{22}) = v_{12}4v_{15}, \ \ \varphi_G(e_{23}) = v_{13}v_{15}, \\
\varphi_G(e_{24}) &= v_{14}v_{15} \qquad (8.2)
\end{aligned}$$



There is no unique way of drawing a graph. One is always interested in whether or not two given points are joined by a line, so the manner of connection is immaterial. As observed in Section 7.2, two edges in a diagram of a graph may intersect at a point which is not a vertex, hence we discussed planarity.

It is interesting to note how many diagrams would be possible for the kind of description in equation 8.2. Example 8.1.1 is a typical group we call $\mathbb{Z}_{2^2} \times \mathbb{Z}_{2^2}$, as the figure shows.

(*It can be noted that while this kind of description is suitable for small graphs, it becomes tedious as complexity of graphs increases.*)

The graphs of concern to us have both their vertex sets and edge sets finite, hence they are called finite graphs. Two graphs G and H are said to be isomorphic if there are bijections

$$\theta : V(G) \to V(H) \text{ and } \phi : E(G) \to E(H) \tag{8.3}$$

in such a way that

$$\varphi_G(e) = uv \text{ if and only if } \varphi_H(\theta(e)) = \theta(u)\theta(v), \tag{8.4}$$

where the pair of maps (θ, ϕ) is referred to as isomorphism between G and H.

8.1.2 Labeling of Vertices

The vertices of the graphs are labeled following the order of the subgroups generated by the points at each level. We achieve this by carefully identifying the generators uniquely for each level.

The orders of subgroups in any level of G are of the form p^i, $i = 0, 1, 2, \cdots, n + m$, yielding $n + m + 1$ number of subgroups in any maximal chain of G.

As was noted in the previous chapters, in any lattice diagram the order of a generator on the right is always greater than that of a generator on its left. But for the purpose of the discussion in graph theory, we shall always regard the vertex on the right as a child of the vertex on the left. The labelling of vertices of the graphs of $G = \mathbb{Z}_{p^n} \times \mathbb{Z}_{p^m}$ was discussed in detail in chapter 3.

We are next interested in the number of leaves, internal vertices and vertices of the graphs of G.

8.2 The Acyclic Graphs of $G = \mathbb{Z}_{p^n} \times \mathbb{Z}_{p^m}$

All the acyclic graphs of G are $p+1$-ary with their rooted subgraphs full p-ary, where p is a prime number. The structure of acyclic graphs for each of positive integers n and m was described in chapter three. In each graph of G we note that if we cut out the *main branch*, the resulting graph is a full p-ary acyclic graph of height $m+1$. In this section we count the number of vertices of each graph from the knowledge of the number of leaves and the number of internal vertices.

The number of leaves of an acyclic graph of G for values of $m = 1, 2$ were counted and the following results were obtained. The formulas for the results can be proved by mathematical induction. Specific values were counted and are given by Tables 9 and 10. We use Theorems 7.9.4 and 7.9.5 to count the number of vertices.

Proposition 8.2.1 *The acyclic graph $G = \mathbb{Z}_{p^n} \times \mathbb{Z}_p$ has $n(p-1)+2$ leaves.*

Proof. Note that this number can be written in the form $p + (n-1)p - (n-2)$, where the first term of the expression refers to the number of leaves of G when the main branch is cut. The corresponding number of vertices in each case is $p+1$ and $\frac{(n-1)p^2-(n-2)p-1}{p-1}$, respectively. Therefore the total gives the number of vertices of G. □

Proposition 8.2.2 *The number of leaves of an acyclic graph $G = \mathbb{Z}_{p^n} \times \mathbb{Z}_{p^2}$ is $(n-1)p^2 + (3-n)p$.*

Proof. Again this number can be written as $p^2 + (n-2)p^2 - (n-3)p$ with the first term being the number of leaves when the main branch is cut. Correspondingly we have p^2+p+1 and $\frac{p^2[(n-2)p-(n-3)]}{p-1}$ vertices, the total of which gives the number of vertices of G as can be checked. □

We are next interested in the number of vertices, edges and valencies of vertices in the simple graphs of G.

8.3 The Simple Graphs of $G = \mathbb{Z}_{p^n} \times \mathbb{Z}_{p^m}$

Beginning with an acyclic graph of G and performing the orientation as explained in chapter three, we end up with a simple graph of G. In this section we are analyzing the graphs of G in terms of valencies of vertices, the number of edges and the total number of vertices. We begin by counting the number of valencies of vertices and consequently the number of edges.

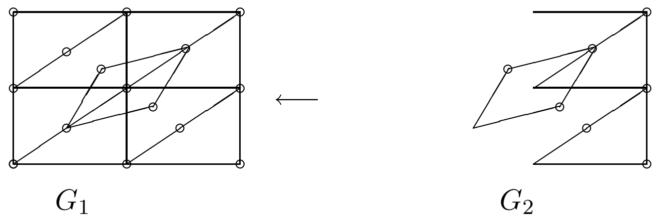
8.3.1 The Sum of Valencies of Vertices of G

Consider $G = \mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2}$. In chapters 5 and 6 we saw that the group has five levels. Each level has the number of vertices as follows:

$$1;\ p+1;\ p^2+p+1;\ p+1;\ 1$$

respectively. Thus G has p^2+3p+5 vertices. Of these vertices two have valencies of $p+1$, and these are the trivial and the big group. The other $p+1$ from each part about symmetry each have $p+2$ valency. Hence we have an additional $2[(p+1)(p+2)]$ valencies. Of the remaining p^2+p+1 vertices, one has a valency of $2(p+1)$, while the rest each have a valency of 2. Adding up, we have that G has $4p^2+12p+8$ valencies of vertices.
Now by the Handshaking Theorem (p97), G has $2p^2+6p+4$ edges.

We next consider the case when $n = 3$ and m fixed at 2, (See figure 3). The graph of G is a union of the graphs G_1 and G_2, where G_2 is an extension of G_1 to G. We give an illustration of an extension from $G_1 = \mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2}$ to $G = \mathbb{Z}_{p^3} \times \mathbb{Z}_{p^2}$, illustration for the case $p = 2$.



The group G now has six levels each with the number of vertices:

$$1;\ p+1;\ p^2+p+1;\ p^2+p+1;\ p+1;\ 1.$$

In this case, it is enough to count the valencies of the levels with 1; $p+1$; p^2+p+1 vertices and use symmetry to arrive at the result. Now 1 vertex has valency of $p+1$, and the $p+1$ each have valency of $p+2$. Of the p^2+p+1 remaining, p^2 have valencies of two each, p have valencies of $p+2$ and the rest have $2(p+1)$, one in this case. Thus, by symmetry, G has a total of $8p^2+16p+10$, an increment of $4p^2+4p+2$ from the number in the previous group.
Continuing in this manner, and by applying the necessary extension, the next case of G for a fixed value of m suggests G has $12p^2+20p+12$. Again, by the Handshaking Theorem, the graphs have $4p^2+8p+5$ and $6p^2+10p+6$ edges respectively.

8.3.2 The Number of Vertices and Edges in the Graphs of G

We are interested in the number of vertices and edges of a simple graph of G. In view of the above description, we state the following propositions without proof as they can be verified from specific subgroup lattices for each case.

Proposition 8.3.1 *Let V be the vertices, and E the edges of a graph of $G=\mathbb{Z}_{p^n}\times\mathbb{Z}_p$. Then*

$$|V| = n(p+1)+2,$$

and

$$|E| = n(2(p+1)-1)+1.$$

Proposition 8.3.2 *Let V be the vertices, and E the edges of a graph of $G=\mathbb{Z}_{p^n}\times\mathbb{Z}_{p^2}$. Then*

$$|V| = 2n(p+1)+(n-1)[p(p-1)-1]+2 = (n-1)p^2+(n+1)p+(n+3)$$

and

$$|E| = 4n(p+1)-(n-1)-(2n-1)+2(n-1)(p^2-p) = 2(n-1)p^2+2(n+1)p+(n+2).$$

8.3.3 The Number of Paths in G

Let the vertices u and v be represented by $\{0\}$ and G in any graph of G. We want to count the number of all distinct paths from u to v on the graph of G. Two paths P_1 and P_2 are said to be distinct if and only if they do not contain the same set of edges. In this counting we impose a restriction in the sense that movements to the left and downwards are prohibited. Hence we only consider those steps that are upwards and to the right. It is important to note that from this restriction there is no shortest path, all paths have the same length.

The distinct paths from u to v are what were referred to in Chapter 5 as maximal chains of G. The number of distinct paths are all described by the polynomials in p, commonly referred to in the literature as Hall polynomials [28], [48].

8.4 Conclusion and Discussion

The process of drawing graphs for the group $G = \mathbb{Z}_{p^n} \times \mathbb{Z}_{p^m}$ produces simple graphs since there is a single edge between any two distinct vertices. The graphs of G are generally undirected graphs, but they enjoy digraph properties during the counting of paths. The description as explained in example 8.1.1 is too cumbersome for our complex subgroup lattices. The number of distinct paths from $u = \{0\}$ to $v = G$ in any graph of G, under the restriction that movements to the left and downwards are prohibited, produces results coinciding with the number of maximal chains of G. In every graph of G there is a path between every pair of distinct vertices hence the graphs are connected. When $m = 1$ and for any positive integer n in G, all the graphs are planar, otherwise the graphs are non-planar.

The graphs of G are not regular for any values of n and m as the graphs always have vertices of different valencies. To our expectation and the nature of the group G, the graphs of G are symmetric.

In view of the entire results, it is interesting to imagine, following this groundwork, how the results for finite Abelian p-groups of rank three and above would look like. The point of symmetry of rank-two finite Abelian p-groups was evident, which leaves to speculation where the symmetry would be for finite Abelian p-groups of rank three. The question of the structure of the direct product of groups G_1 and G_2, where $G_1 = \mathbb{Z}_{p^n} \times \mathbb{Z}_{p^m}$ and $G_2 = \mathbb{Z}_{q^k} \times \mathbb{Z}_{q^l}$ for some positive integers k, l, m, n and for some prime numbers p, q, where $(p, q) = 1$ is a matter of interest and would be considered in subsequent works following this project.

TABLES AND FIGURES

TABLES

Level	Number of subgroups	Generators
0	1	00
1	$p + [1]$	$(p^5 \alpha p^2), \ \ \alpha = 0, 1, \ldots, p-1$
2	$p^2 + [p]$	$(p^4 \lambda p), \ \ \lambda = 0, 1, \ldots, p^2-1$
3	$p^3 + [p^2]$	$(p^3 j), \ \ j = 0, 1, \ldots, p^3-1$
4	p^3	$(p^2 j)$
5	p^3	$(p^1 j)$
6	p^3	$(p^0 j)$

Table 1

Labelling of a tree diagram for $G = \mathbb{Z}_{p^6} \times \mathbb{Z}_{p^3}$.

Level	Subgroups	Range
0	1	
$\langle a \rangle \quad \equiv \quad 0p; \quad p(\alpha p)$	$p + 1$	$\alpha = 0, 1, \ldots, p-1$
$\langle b \rangle \quad \equiv \quad 01; \quad \langle 0p, p0 \rangle; \quad p\beta$		$\beta = 1, \cdots, p-1$
$\langle b \rangle \quad \equiv \quad \langle 0p, p0 \rangle; \quad 1\,(0 + \alpha p)$		
$\langle b \rangle \quad \equiv \quad \langle 0p, p0 \rangle; \quad 1\,(1 + \alpha p)$		
$\vdots$	$p^2 + p + 1$	$\alpha = 0, 1, \ldots, p-1$
$\langle b \rangle \quad \equiv \quad \langle 0p, p0 \rangle; \quad 1\,((p-1) + \alpha p)$		
$\langle c \rangle \quad \equiv \quad \langle 01, p0 \rangle; \quad \langle 0p, p0 \rangle; \quad [1\delta, 1(\delta + p)]$	$p + 1$	$\delta = 1, \ldots, p-1$

Table 2

Table showing labelling of vertices for the subgroup lattice of $G = \mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2}$.

Group/p(n)	$(7,1)$	$(6,2)$	$(5,3)$	$(4,4)$
α_8	1	1	1	1
α_7	$p+1$	$p+1$	$p+1$	$p+1$
$\alpha_{6,2}$	$p+1$	p^2+p+1	p^2+p+1	p^2+p+1
$\alpha_{5,3}$	$p+1$	p^2+p+1	p^3+p^2+p+1	p^3+p^2+p+1
$\alpha_{4,4}$	$p+1$	p^2+p+1	p^3+p^2+p+1	$p^4+p^3+p^2+p+1$
α_6	$2p+1$	p^2+2p+1	p^2+2p+1	p^2+2p+1
$\alpha_{5,2}$	$2p+1$	$2p^2+2p+1$	p^3+2p^2+2p+1	p^3+2p^2+2p+1
$\alpha_{4,3}$	$2p+1$	$2p^2+2p+1$	$2p^3+2p^2+2p+1$	$p^4+2p^3+2p^2+2p+1$
$\alpha_{4,2,2}$	$2p+1$	$3p^2+2p+1$	$2p^3+3p^2+2p+1$	$p^4+2p^3+3p^2+2p+1$
$\alpha_{3,3,2}$	$2p+1$	$3p^2+2p+1$	$3p^3+3p^2+2p+1$	$p^4+3p^3+3p^2+2p+1$
α_5	$3p+1$	$3p^2+3p+1$	p^3+3p^2+3p+1	p^3+3p^2+3p+1
$\alpha_{4,2}$	$3p+1$	$4p^2+3p+1$	$3p^3+4p^2+3p+1$	$p^4+3p^3+4p^2+3p+1$
$\alpha_{3,3}$	$3p+1$	$4p^2+3p+1$	$4p^3+4p^2+3p+1$	$2p^4+4p^3+4p^2+3p+1$
$\alpha_{3,2,2}$	$3p+1$	$5p^2+3p+1$	$5p^3+5p^2+3p+1$	$2p^4+5p^3+5p^2+3p+1$
$\alpha_{2,2,2,2}$	$3p+1$	$6p^2+3p+1$	$6p^3+6p^2+3p+1$	$3p^4+6p^3+6p^2+3p+1$
α_4	$4p+1$	$6p^2+4p+1$	$4p^3+6p^2+4p+1$	$p^4+4p^3+6p^2+4p+1$
$\alpha_{3,2}$	$4p+1$	$7p^2+4p+1$	$7p^3+7p^2+4p+1$	$3p^4+7p^3+7p^2+4p+1$
$\alpha_{2,2,2}$	$4p+1$	$8p^2+4p+1$	$9p^3+8p^2+4p+1$	$4p^4+9p^3+8p^2+4p+1$
α_3	$5p+1$	$10p^{2}5+3p+1$	$10p^3+10p^2+5p+1$	$4p^4+10p^3+10p^2+5p+1$
$\alpha_{2,2}$	$5p+1$	$11p^2+5p+1$	$13p^3+11p^2+5p+1$	$6p^4+13p^3+11p^2+5p+1$
α_2	$\underline{6p+1}$	$15p^2+\underline{6p+1}$	$19p^3+\underline{15p^2+6p+1}$	$9p^4+\underline{19p^3+15p^2+6p+1}$
α_0	$7p+1$	$20p^2+7p+1$	$28p^3+20p^2+7p+1$	$14p^4+28p^3+20p^2+7p+1$

Table 3

Polynomial representation of fuzzy subgroups. Column 1 lists partition of type $\lambda=(\lambda_1,\lambda_2,\ldots,\lambda_k)$, where $\lambda_1+\ldots+\lambda_k=8$. (1's have been dropped). Remaining columns give the number of fuzzy subgroups of (n,m) for each λ, where $(n,m)\equiv\mathbb{Z}_{p^n}\times\mathbb{Z}_{p^m}$, and $n+m=8$.

Partition	**Number of fuzzy subgroups**
α_{10}	1
α_9	$p+1$
$\alpha_{8,2}$	p^2+p+1
α_8	p^2+2p+1
$\alpha_{7,3}$	p^3+p^2+p+1
$\alpha_{7,2}$	$p^3+p^2+(p+1)(p+1)$
α_7	$p^3+p^2+(p+1)(2p+1)$
$\alpha_{6,4}$	$p^4+p^3+p^2+p+1$
$\alpha_{6,3}$	$p^4+p^3+(p^2+p+1)(p+1)$
$\alpha_{6,2,2}$	$p^4+p^3+(p^2+p)(p+1)+(p^2+p+1)$
$\alpha_{6,2}$	$p^4+p^3+(p^2+p)(2p+1)+(p^2+2p+1)$
α_6	$p^4+p^3+(p^2+p)(3p+1)+(p+1)(2p+1)$
$\alpha_{5,5}$	$p^5+p^4+p^3+p^2+p+1$
$\alpha_{5,4}$	$p^5+p^4+(p^3+p^2+p+1)(p+1)$
$\alpha_{5,3,2}$	$p^5+p^4+(p^3+p^2)(p+1)+(p+1)(p^2+p+1)$
$\alpha_{5,3}$	$p^5+p^4+(p^3+p^2)(2p+1)+(p+1)(p^2+2p+1)$
$\alpha_{5,2,2}$	$p^5+p^4+(p^3+p^2)(2p+1)+(p+1)[p^2+(p+1)(p+1)]$
$\alpha_{5,2}$	$p^5+p^4+(p^3+p^2)(3p+1)+(p+1)[p^2+(p+1)(2p+1)]$
α_5	$p^5+p^4+(p^3+p^2)(4p+1)+(p+1)[p(3p+1)+(p+1)(2p+1)]$
$\vdots$	$\vdots$

Table 4

Addresses the process of splitting of paths during the counting of fuzzy subgroups as prescribed by each partition. Illustration for the case $n+m=10$ for $(n,m)=(7,3)$.

$p(10)$	$p9p$	$p8p2$	$p7p3$	$p6p4$	p5p5
10	0	0	0	0	0
91	1	0	0	0	0
82	1	1	0	0	0
73	1	1	1	0	0
64	1	1	1	1	0
5^2	1	1	1	1	1
81^2	2	1	0	0	0
721	2	2	1	0	0
631	2	2	2	1	0
62^2	2	2	2	1	0
541	2	2	2	2	1
532	2	3	3	2	1
4^22	2	3	3	3	1
43^2	2	3	4	3	1
71^3	3	3	1	0	0
621^2	3	4	3	1	0
531^2	3	4	4	3	1
52^21	3	5	5	3	1
4^21^2	3	4	4	4	2
4321	3	5	6	4	2
42^3	3	6	7	6	2
3^31	3	5	7	6	2
3^22^2	3	6	8	7	3
61^4	4	6	4	1	0
521^3	4	7	7	4	1
431^3	4	7	8	7	3
42^21^2	4	8	10	8	3

Table 5

$p(10)$	$p9p$	$p8p2$	$p7p3$	$p6p4$	p5p5
$3^2 21^2$	4	8	11	10	4
$32^3 1$	4	9	13	12	5
2^5	4	10	15	15	6
51^5	5	10	10	5	1
421^4	5	11	14	11	4
$3^2 1^4$	5	11	15	16	6
$32^2 1^3$	5	12	18	17	7
$2^4 1^2$	5	13	21	21	9
41^6	6	15	20	15	5
321^5	6	16	25	24	10
$2^3 1^4$	6	17	29	30	13
31^7	7	21	35	34	14
$2^2 1^6$	7	22	40	43	19
21^8	8	28	55	62	28
1^{10}	9	35	75	90	42

Table 5 **cont.**

Table showing the coefficient of the leading term for each group such that $n + m = 10$, and for each partition of type λ.

Partition	**Number of fuzzy subgroups**
$[7,3]$	p^3+p^2+p+1
$[6,4]$	$p^4+p^3+p^2+p+1$
$[5,5]$	$p^5+p^4+p^3+p^2+p+1$
$[7,2,1]$	p^3+2p^2+2p+1
$[6,3,1]$	$p^4+2p^3+2p^2+2p+1$
$[5,4,1]$	$p^5+2p^4+2p^3+2p^2+2p+1$
$[7,1,1,1]$	p^3+3p^2+3p+1
$[6,2,2]$	$p^4+2p^3+3p^2+2p+1$
$[5,3,2]$	$p^5+2p^4+3p^3+3p^2+2p+1$
$[4,4,2]$	$p^5+3p^4+3p^3+3p^2+2p+1$
$[4,3,3]$	$p^5+3p^4+4p^3+3p^2+2p+1$
$[6,2,1,1]$	$p^4+3p^3+4p^2+3p+1$
$[5,3,1,1]$	$p^5+4p^4+4p^3+4p^2+3p+1$
$[4,4,1,1]$	$2p^5+4p^4+4p^3+4p^2+3p+1$
$[5,2,2,1]$	$p^5+3p^4+5p^3+5p^2+3p+1$
$[4,3,2,1]$	$2p^5+5p^4+6p^3+5p^2+3p+1$
$[3,3,3,1]$	$2p^5+5p^4+6p^3+5p^2+3p+1$
$[6,1,1,1,1]$	$p^4+4p^3+6p^2+4p+1$
$[4,2,2,2]$	$2p^5+6p^4+7p^3+6p^2+3p+1$
$[3,3,2,2]$	$3p^5+7p^4+8p^3+6p^2+3p+1$
$[5,2,1,1,1]$	$p^5+4p^4+7p^3+7p^2+4p+1$
$[4,3,1,1,1]$	$3p^5+7p^4+10p^3+7p^2+4p+1$
$[4,2,2,1,1]$	$3p^5+8p^4+10p^3+8p^2+4p+1$
$[3,3,2,1,1]$	$4p^5+10p^4+11p^3+8p^2+4p+1$

Table 6

Polynomial representations of fuzzy subgroups, grouping together those with the same coefficient of a power of p, p^2 in this case.

n	**vertices**	**edges**	**coefficients**
2	$8+5+2$	$11+9+4=24$	[1,3,5]
3	$11+7+4$	$16+13+8=37$	[2,4,6]
4	$14+9+6$	$21+17+12=50$	[3,5,7]
5	$17+11+8$	$26+21+16$	[4,6,8]
$\vdots$	$\vdots$	$\vdots$	$\vdots$
n			[n-1,n+1,n+3]

Table 7

Systematic counting of vertices and edges, illustration for the graph of

$$\mathbb{Z}_{p^n} \times \mathbb{Z}_{p^2}, \quad p = 2$$

$\mathbb{Z}_p \times \{0\}$	$\mathbb{Z}_{p^2} \times \mathbb{Z}_p$	$\mathbb{Z}_{p^3} \times \mathbb{Z}_{p^2}$	$\mathbb{Z}_{p^4} \times \mathbb{Z}_{p^3}$	$\mathbb{Z}_{p^5} \times \mathbb{Z}_{p^4}$	$\dots$
1	$1(\mathbb{Z}_p \times \mathbb{Z}_p)$	$1(\mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2})$	$1(\mathbb{Z}_{p^3} \times \mathbb{Z}_{p^3})$	$1(\mathbb{Z}_{p^4} \times \mathbb{Z}_{p^4})$	$\dots$
$\vdots$	$1(\mathbb{Z}_p \times \{0\})$	$p(\mathbb{Z}_{p^2} \times \mathbb{Z}_p)$	$p(\mathbb{Z}_{p^3} \times \mathbb{Z}_{p^2})$	$p(\mathbb{Z}_{p^4} \times \mathbb{Z}_{p^3})$	$\dots$
$\vdots$	$\vdots$	$p(\mathbb{Z}_{p^2} \times \{0\})$	$p(\mathbb{Z}_{p^3} \times \mathbb{Z}_p)$	$p(\mathbb{Z}_{p^4} \times \mathbb{Z}_{p^2}$	$\dots$
$\vdots$	$\vdots$	$\vdots$	$p^2(\mathbb{Z}_{p^3} \times \{0\})$	$p(\mathbb{Z}_{p^4} \times \mathbb{Z}_p)$	$\dots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$p^3(\mathbb{Z}_{p^4} \times \{0\}$	$\dots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

Table 8

Illustration of inductive reasoning during the counting of chains.

Group/p	2	3	5	7	11	13	17	...
$(1,1)$	3	4	6	8	12	14	18	...
$(2,1)$	4	6	10	14	22	26	34	...
$(3,1)$	5	8	14	20	32	38	50	...
$(4,1)$	6	10	18	26	42	50	66	...
$(5,1)$	7	12	22	32	52	62	82	...
$(6,1)$	8	14	26	38	62	74	98	...
$\vdots$								$\vdots$

Table 9

Group/p	2	3	5	7	...
$(2,2)$	6	12	30	56	...
$(3,2)$	8	18	50	98	...
$(4,2)$	10	24	70	140	...
$(5,2)$	12	30	90	182	...
$(6,2)$	14	36	110	224	...
$\vdots$					$\vdots$

Table 10

The number of leaves in an acyclic graph of $(n,m) \equiv \mathbb{Z}_{p^n} \times \mathbb{Z}_{p^m}$.

FIGURES

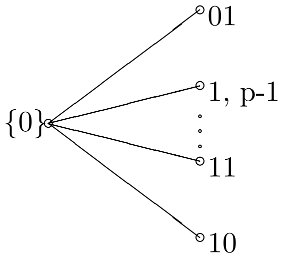


figure 1

Tree diagram for $G = \mathbb{Z}_p \times \mathbb{Z}_p$

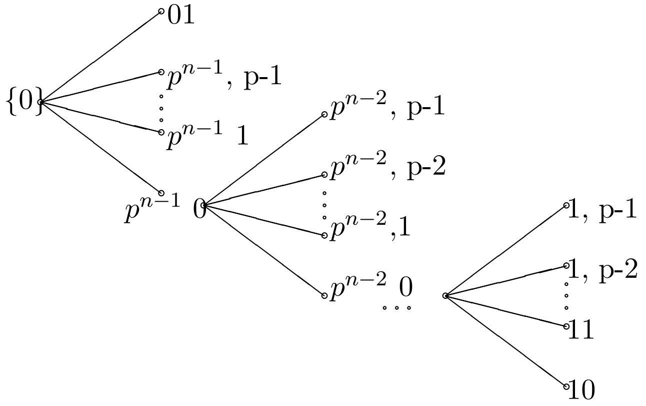


figure 2

Cyclic tree diagram for $G = \mathbb{Z}_{p^n} \times \mathbb{Z}_p$

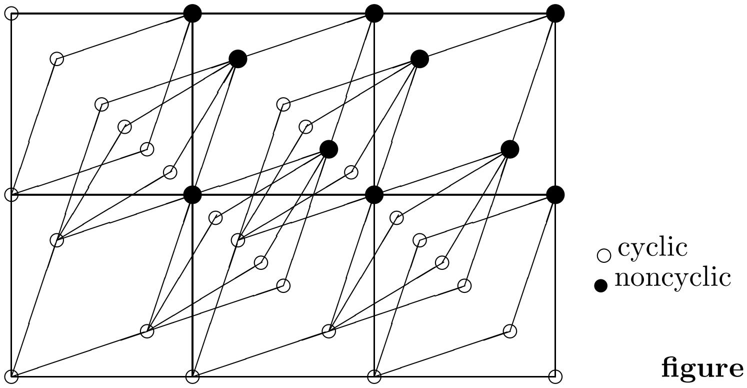


figure 3

Lattice diagram for $G = \mathbb{Z}_{p^3} \times \mathbb{Z}_{p^2}$, illustration for $p = 3$

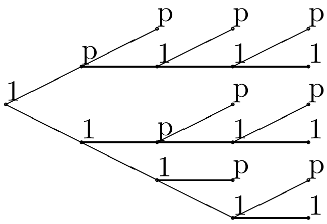


figure 4

Binary Tree representation for subgroup lattice of $G = \mathbb{Z}_{p^3} \times \mathbb{Z}_{p^2}$

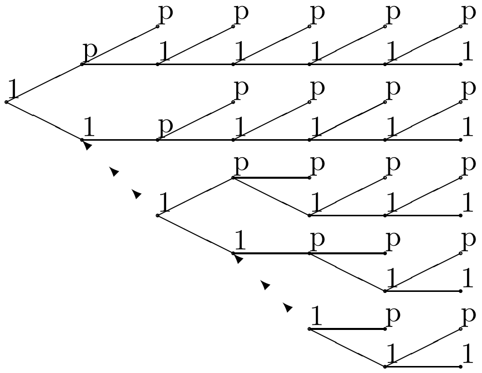
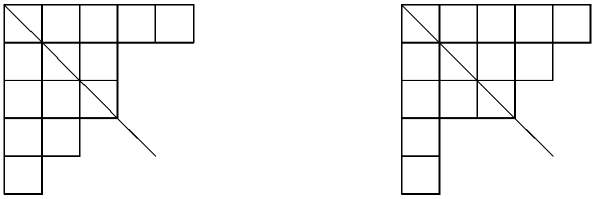


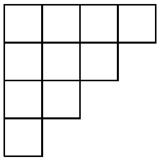
figure 5

Binary Tree representing lattice diagram for $G = \mathbb{Z}_{p^n} \times \mathbb{Z}_p$



$\lambda = (5,3,3,2,1)$ $\lambda' = (5,4,3,1,1)$ **figure 6**

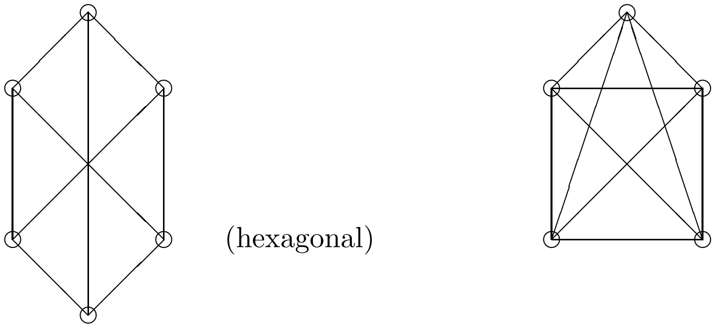
Young diagram representation for partition of type λ and its conjugate, λ'



$\lambda = \lambda' = (4,3,2,1)$

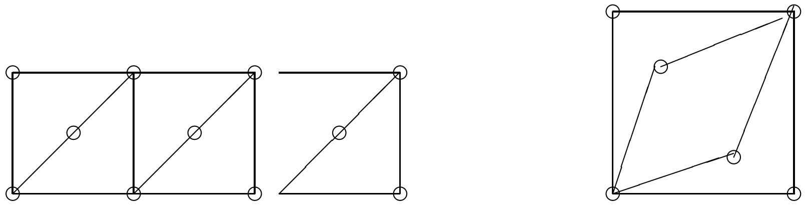
figure 7

Illustration - by a Young diagram - of a partition of type λ which is self-conjugate.



(hexagonal) (pentagonal)

figure 8



(Euler path no Euler circuit)

(Euler circuit)

figure 9

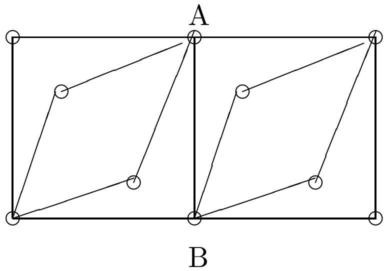


figure 10

(Euler path)

(In **figure 10**, all of the vertices, except *A* (valency 5) and *B* (valency 5) have even valencies. Therefore, according to Euler's theorem, the graph has no Euler circuit. But the graph, however, has an Euler path.)

$$\mathbf{G} = \mathbb{Z}_{\mathbf{3^3}} \times \mathbb{Z}_{\mathbf{3^3}}$$

$$\mathbf{G} = \mathbb{Z}_{\mathbf{2^6}} \times \mathbb{Z}_{\mathbf{2^4}}$$

$$\mathbf{G = \mathbb{Z}_{3^4} \times \mathbb{Z}_{3^4}}$$

$$\mathbf{G} = \mathbb{Z}_{\mathbf{2^5}} \times \mathbb{Z}_{\mathbf{2^5}}$$

APPENDIX I

A partition of a nonempty set X is a family of nonempty subsets $\{S_i : i \in I\}$ satisfying the following:

1. if $i \neq j$, then $S_i \cap S_j = \emptyset$,

2. $X = \cup S_i$.

Suppose G and H are groups with operations $*$ and $\bullet$ respectively. Then for all $a, b \in G$, a mapping $\phi : G \to H$ is called a homomorphism if

$$\phi(a * b) = \phi(a) \bullet \phi(b).$$

Proposition 8.4.1 [30]. *Let G be an additive group whose subgroups are H_1 and H_2, and suppose G satisfies the conditions*

1. $H_1 \cap H_2 = \{0\}$

2. $H_1 H_2 = G$, *where* $H_1 H_2 = \{h_1 h_2 : h_1 \in H_1, h_2 \in H_2\}$

then G is said to be isomorphic to the direct sum $H_1 \oplus H_2$. In fact G is said to be the internal direct sum of H_1 and H_2 denoted as

$$G = H_1 \oplus H_2. \tag{8.5}$$

To prove this proposition, let us state the 1st isomorphism theorem first.

Theorem 8.4.2 (1st Isomorphism Theorem) *If $f : G \to H$ is a homomorphism of groups, then f induces an isomorphism $G/ker\, f \cong im\, f$.*

We are now ready to prove the proposition.
Define the function

$$f : H_1 \oplus H_2 \to G$$

by

$$f(h_1, h_2) = h_1 + h_2.$$

Now f is a homomorphism, for if h_1 and h_1^* are in H_1, and if h_2 and h_2^* are in H_2, then

$$\begin{aligned} f((h_1, h_2) + (h_1^*, h_2^*)) &= f(h_1 + h_1^*, h_2 + h_2^*) \\ &= h_1 + h_1^* + h_2 + h_2^* \\ &= (h_1 + h_2) + (h_1^* + h_2^*) \\ &= f(h_1, h_2) + f(h_1^*, h_2^*). \end{aligned}$$

The other properties of a homomorphism follow immediately.

We proceed to show that the $ker\, f = \{0\}$. This follows from the definition of a kernel

$$ker\, f = \{(h_1, h_2) : f(h_1, h_2) = 0\}$$

From this we deduce that $h_1 + h_2 = 0$ and so $h_1 = -h_2 \in H_1 \cap H_2$, hence $kerf = 0$. Lastly we show that $im\, f = G$. By definition,

$$im\, f = \{h_1 + h_2 : h_1 \in H_1, h_2 \in H_2\} = H_1 + H_2 = G.$$

By the 1st isomorphism theorem, the result follows.

(Zassenhaus Lemma) Let A, A^*, B, B^* be four subgroups of a group G with A normal in A^* and B normal in B^*. Then

$$A(A^* \cap B) \lhd A(A^* \cap B^*),$$

$$B(A \cap B^*) \lhd B(A^* \cap B^*),$$

and there is an isomorphism

$$\frac{A(A^* \cap B^*)}{A(A^* \cap B)} \approx \frac{B(A^* \cap B^*)}{B(A \cap B^*)}. \tag{8.6}$$

The finite Abelian groups of rank two form a symmetric matrix as shown below:

$$\begin{bmatrix} (11) & (12) & (13) & (14) & (15) & \dots & (1m) \\ (21) & (22) & (23) & (24) & (25) & \dots & (2m) \\ (31) & (32) & (33) & (34) & (35) & \dots & (3m) \\ (41) & (42) & (43) & (44) & (45) & \dots & (4m) \\ \vdots & & & & \vdots & & \vdots \\ (n1) & (n2) & (n3) & (n4) & (n5) & \dots & (nm) \end{bmatrix}$$

$$(n, m) \text{ is read } \mathbb{Z}_{p^n} \times \mathbb{Z}_{p^m}$$

It becomes logical to consider only either the lower or upper triangular matrix as there is no distinction between $\mathbb{Z}_{p^n} \times \mathbb{Z}_{p^m}$ and $\mathbb{Z}_{p^m} \times \mathbb{Z}_{p^n}$.

Every finite group has at least one composition series.

Since any finite Abelian group G of order $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ is a product of cyclic groups of prime-power orders, it follows that G has at least one composition series in which all factors are cyclic of prime order.

All maximal chains in a finite Abelian group have the same length.

Thus one can say that a group G is solvable if and only if its composition factors are all of prime order.

A group G is said to be *nilpotent* if G has a normal series $G = G_1 \geq G_2 \geq \cdots \geq G_n = 1$ in such a way that each G_i is normal in G and G_{i-1}/G_i is in the center of the group G/G_i for $2 \leq i \leq n$. It is instructive to note that a nilpotent group is always solvable, whereas a solvable group need not be nilpotent. Thus it can be said that G is nilpotent if G has prime-power order.

APPENDIX II

In the crisp case, $\chi_A(x)$ gives the degree of membership of x to A. In the fuzzy subset case, the degrees of membership range over the full unit interval $[0,1]$. Thus a fuzzy subset A, denoted by μ_A, is a function

$$\mu_A : X \to I,$$

with the number $\mu_A(x)$ in $[0,1]$, interpreted as the degree to which x belongs to A, where $\mu(x)=1$ means that x belongs to A absolutely, and $\mu_A(x)=0$ means x does not belong to A absolutely.

A fuzzy set μ_A is said to be normal if $\mu_A(x)=1$ for at least one x in X.

Union, intersection and complementation of fuzzy sets are defined by taking *max, min* and $'$ pointwise for the degree of membership. If A, B are two fuzzy subsets of X, then $A \cap B, A \cup B, A'$ are given by

$$\mu_{A\cap B}(x) = \mu_A(x) \wedge \mu_B(x)$$
$$\mu_{A\cup B}(x) = \mu_A(x) \vee \mu_B(x)$$
$$\mu_{A'}(x) = 1 - \mu_A(x)$$

The set of all fuzzy sets of X is denoted by I^X, so

$$I^X = \{\mu : \mu \to I\}.$$

A fuzzy point is a fuzzy subset of the form x^λ, where

$$x^\lambda(y) = \begin{cases} \lambda & \text{if} \quad y = x \\ \\ 0 & \text{if} \quad y \neq x \end{cases}$$

and

$$0 < \lambda \leq 1, \;\; x, y \;\; \in X.$$

For two fuzzy sets μ and ν of X,

$$\mu = \nu \Longleftrightarrow \mu(x) = \nu(x) \;\text{ for all }\; x \in X$$

$$\mu \subseteq \nu \;\text{ or }\; \mu \leq \nu \Longleftrightarrow \mu(x) \leq \nu(x) \;\text{ for all }\; x \in X$$

$$\mu < \nu \Longleftrightarrow \mu(x) \leq \nu(x) \text{ for all } x \in X, \text{ and for at least one } x \in X, \ \mu(x) < \nu(x).$$

In this sense, a fuzzy point x^β is strictly contained in another fuzzy point x^λ provided $0 < \beta < \lambda = 1$.

If $\{\mu_j\}_{j\in J}$ is a collection of fuzzy sets of X then the union of μ_j' s is defined as

$$(\bigvee_{j\in J} \mu_j)(x) = \sup_{j\in J}(\mu_j(x)),$$

and the intersection is defined as

$$(\bigwedge_{j\in J} \mu_j)(x) = \inf_{j\in J}(\mu_j(x)).$$

A fuzzy subset μ of a group G is a fuzzy subgroup of the group G if and only if

$$\mu(xy^{-1}) \geq \min\{\mu(x), \mu(y)\} \text{ for every } x, y \in G.$$

Let μ be a fuzzy subset of a group G. Then μ is a fuzzy subgroup of G if and only if ${G_\mu}^t$ is subgroup (called level subgroup) of the group G for every $t \in [0, \mu(e)]$, where e is the identity element of the group G.

A fuzzy subgroup μ of a group G is said to be a fuzzy normal subgroup of G if

$$\mu(xy) = \mu(yx) \text{ for every } x, y \in G.$$

Let μ be a fuzzy normal subgroup of a group G. For $t \in [0, 1]$, the set

$$\mu_t = \{(x, y) \in G \times G : \mu(xy^{-1}) \geq t\}$$

is called the $t-$ level relation of μ. For the fuzzy normal subgroup μ of G and for $t \in [0, 1]$, μ_t is a congruence relation on the group G.

Let G be a cyclic group of prime order. Then there exists a fuzzy subgroup A of G such that $A(e) = t_0$ and $A(x) = t_1$ for all $x \neq e$ in G and $t_0 > t_1$.

Let μ be a fuzzy subgroup of a group G and ν be a fuzzy subset of the group. If μ and ν are conjugate fuzzy subsets of the group G then μ is a fuzzy subgroup of the group G.

Bibliography

[1] Abu Osman, M. T, *On the Direct Product of Fuzzy Subgroups,* Fuzzy Sets and Systems **12** (1984), 87–91.

[2] Ajmal, N., *Homomorphisms of Fuzzy Subgroups, Correspondence Theorem and Fuzzy Quotient Groups*, Fuzzy Sets and Systems **61** (1994), 329–339

[3] Akgul, M., *Some Properties of Fuzzy Groups,* J.Math.Anal.Appl. **133** (1988), 93–100.

[4] Alkhamees, Y.; *Fuzzy Cyclic Subgroups and Fuzzy Cyclic p-Subgroups.* Journal of Fuzzy Math. **3(4)** (1995), 911–919.

[5] Anthony, J. M; Sherwood, H, *Fuzzy Groups Redefined.* J.Math.Anal.Appl. **7** (1982), 297–305.

[6] Asaad, M.; Abou-Zaid, S. , *Characterization of Fuzzy Subgroups*, Fuzzy Sets and Systems **77** (1996), 247–251.

[7] Asaad, M.; Abou-Zaid, S. , *Groups and Fuzzy Subgroups II*, Fuzzy Sets and Systems **56** (1993), 375–377.

[8] Bezdek, J. C; Harris, J. D, *Fuzzy Partitions and Relations: An Axiomatic Basis for Clustering*, Fuzzy Sets and Systems **1** (1978), 111–127.

[9] Bhakat, S.; Das, P., *On the Definition of a Fuzzy Subgroup*, Fuzzy Sets and Systems **51** (1992), 235–241.

[10] Bhakat, S.; Das, P., *Fuzzy Partially Ordered Fuzzy Subgroups*, Fuzzy Sets and Systems **67** (1994), 191–198.

[11] Bodjanova, S., *Comparison of Fuzzy Partitions Based on their α-cuts*, Fuzzy Sets and Systems **105** (1999), 99–112.

[12] Bondy, J. A.; Murty, U. S. R., *Graph Theory with Applications*, Library of Congress Cataloging in Publication Data . North-Holland (1982).

[13] Buchmann, Johannes; Jacobson, Michael J., Jr.; Teske, Edlyn , *On some computational problems in Finite Abelian Groups*, Math. Comp. 66 (1997), no. 220, 1663–1687.

[14] Burn, R. P, *Groups, A Path to Geometry* Great Britain, University Press, Cambridge (1991).

[15] Butler, L., *Generalized Flags in Finite Abelian p-Groups.* Discrete Appl. Math., **34** (1991), 67–81.

[16] Butler, M. L., *Subgroup Lattices and Symmetric Functions.* Mem. AMS, **112** (1994), no. 539.

[17] Chakraborty, A. B; Khare, S. S, *Fuzzy Homomorphisms and f-Fuzzy Subgroups Generated by a Fuzzy Subset*, Fuzzy Sets and Systems **74** (1995), 259–268.

[18] Cohn, P. M, *Algebra, Second Edition, Volume 2* University College, London (1989).

[19] Combe, D.; Nelson, A. M.; Palmer, W. D. *Magic Labellings of Graphs over Finite Abelian Groups,* Australas. J. Combin. 29 (2004), 259–271.

[20] Dai, Qiong; Zou, Xiao Xiang; Luo, Zhu Kai, *An Algorithm for Decomposing a Finite Abelian Group into a Direct Product of p-groups*, Natur. Sci. J. Xiangtan Univ. 21 (1999), no. 1, 19–22.

[21] Das, P. S., *Fuzzy Groups and Level Subgroups*, J. Math. Anal. Appl. 84: 264–269 (1981).

[22] Diderrich, George T.; Mann, Henry B. *Combinatorial Problems in Finite Abelian Groups.* Survey of combinatorial theory (Proc. Internat. Sympos.,

Colorado State Univ., Fort Collins, Colo., 1971), pp. 95–100. North-Holland, Amsterdam, 1973.

[23] Dixit, V. N; Kumar, R; Ajmal, N., *Level Subgroups and Union of Fuzzy Subgroups.* Fuzzy Sets and Systems **37** (1990), 359–371.

[24] Dixit,V. N; Bhambri,S.K;Kumar Pratibha, *Union of Fuzzy Subgroups.* Fuzzy Sets and Systems **78** (1996), 121–123.

[25] Feit, W.; Thompson *Solvability of Groups of Odd Order.* Pacific Journal of Mathematics **13** (1963), 775–1029.

[26] Fuchs, L., *Abelian Groups*, Addison-Wesley Publishing Company (1967).

[27] Fulman, Jason *Hall polynomials and the fixed space of an automorphism of a finite Abelian p-group.* Arch. Math. (Basel) 73 (1999), no. 1, 1–10. (Reviewer: Michael Szalay)

[28] Fulton,William, *Young Tableaux with Applications to Representation Theory and Geometry.* London Mathematical Society, University of Michigan (1999.

[29] Fraleigh, J. B., *A First Course in Abstract Algebra* Addison-Wesley, London, (1982).

[30] Gallian, J. A., *Contemporary Abstract Algebra* 3rd ed., Heath and Company, Lexington, (1994).

[31] Gao, W. D., *A Combinatorial Problem on Finite Abelian Groups.* J. Number Theory **58** (1996), no. 1, 100–103.

[32] Griggs, J. R, *Spanning Subset Sums for Finite Abelian Groups. Combinatorics, graph theory, algorithms and applications* Discrete Math. **229** (2001), no.1-3, 89–99.

[33] Grishko Yu. V, Protasov I.V, *Symmetric Colorings of Finite Abelian Groups*, nauk Ukr.Mat.Prirodozn.Tekh.Nauki, 2000, no.1,32-33.

[34] Gupta,K. C; Gupta,R. K, *Fuzzy Equivalence Relation Redefined.* Fuzzy Sets and Systems **79** (1996), 227–233.

[35] Hall, Marshall, Jr, *The Theory of Groups*, The Macmillan Company, New York (1969).

[36] Hall, P., *A Contribution to the Theory of Groups of Prime-Power Order.*, Proc. London Math. Soc. (2)36 (1933), 29–95.

[37] Hamermesh, Morton, *Group Theory and its Application to Physical Problems*, Addison-Wesley Publishing Company (1964).

[38] Harry, Frank, *Graph Theory* University of Michigan, Addison-Wesley Publishing Company (1969).

[39] Heden, Olof, *Partitions of Finite Abelian Groups.* European J. Combin. **7** (1986), no. 1, 11–25.

[40] Herstein, I. N, *Topics in Algebra, Second Edition* University of Chicago (1975).

[41] Higgins, P. J, *A First Course in Abstract Algebra* London (1975).

[42] Hungerford, Thomas, W., *Algebra* University of Washington, Addison-Wesley Publishing Company (1974).

[43] Jae Kim, *On groups and fuzzy subgroups*, Fuzzy Sets and Systems **67** (1994), 347–348

[44] Jin Fang, *Fuzzy homomorphisms and fuzzy isomorphisms (short communication*, Fuzzy Sets and Systems **63** (1994), 237–242

[45] Kumar, R., *Homomorphisms and Fuzzy(fuzzy normal)Subgroups*, Fuzzy Sets and Systems 44(1991), 165–168.

[46] Kurosh, A.G., *The Theory of Groups*, Chelsea Publishing Company, New York (1955).

[47] Liu, C. L., *Introduction to Combinatorial Mathematics* McGraw Hill, New York (1968).

[48] Macdonald, I. G. *Symmetric Functions and Hall Polynomials*, 2nd ed. Oxford, England: Oxford University Press, pp. 383 and 387, 1995.

[49] MacLane, Saunders; Garrett, Birkhoff, *Algebra, Second Edition*, Macmillan Publishing Co., inc., New York (1979).

[50] Makamba, B. B, *Direct Products and Isomorphism of Fuzzy Subgroups*, Inform. Sci. **65** (1992), 33–43.

[51] Makamba, B. B, Murali, V., *Normality and Congruence in Fuzzy Subgroups*, Inform. Sci. **59** (1992), 121–129.

[52] Malik, D. S; Mordeson, J. N; Nair,P. S, *Fuzzy Generators and Fuzzy Direct Sums of Abelian Groups.* Fuzzy Sets and Systems **50** (1992), 193–199.

[53] Mashinchi, Salili Sh.; *On Fuzzy Isomorphism Theorems* Journal of Fuzzy Math. **4** (1996), 39–49.

[54] Montes, Susana; Couso, Ines; Gil, Pedro , *One-to-one correspondences between ϵ-partitions, $1-\epsilon$-equivalences and $\epsilon-$pseudometrics.* Fuzzy Sets and Systems **vol 124** (2001), 87–95

[55] Mordeson, John N., *Invariants of Fuzzy Subgroups* Fuzzy Sets and Systems **63** (1994), 81–85.

[56] Morsi, N. N., *Note on "Normal fuzzy subgroups and fuzzy normal series of finite groups"* Fuzzy Sets and Systems **87** (1997), 255–256

[57] Mukherjee, Bhattacharya P., *Fuzzy Groups: some group theoretic analogs* Inform. Sci. **39** (1986), 247–268.

[58] Murali, V., *Fuzzy equivalence relations.* Fuzzy Sets and Systems, **30** (1989), no.2, 155–163.

[59] Murali, V. and Makamba, B. B, *On an Equivalence of Fuzzy Subgroups I*, Fuzzy Sets and Systems **123** (2001) 259–264.

[60] Murali, V. and Makamba, B. B, *On an Equivalence of Fuzzy Subgroups II*, *To appear in Fuzzy Sets and Systems(2000)*, 15 pages.

[61] Murali, V.; Makamba, B. B., *Finite Fuzzy Sets,* International Journal of General Systems, Vol. **34** (2005), no.1, 61–75.

[62] Murali, V.; Makamba, B. B., *Operations on Equivalent Fuzzy Subgroups,* The Journal of Fuzzy Mathematics, Vol. **13** , no.2,(2005) 1–16.

[63] Ngcibi, S. L, *Masters Thesis.*, Rhodes University Library, (2002), 1–77.

[64] Ngcibi, S. L.; Murali, V.; Makamba, B. B, *Fuzzy Subgroups of Rank Two Abelian p-Group*– Submitted to the Press.

[65] Ovchinnikov, S., *On the image of a fuzzy subgroup*, Fuzzy Sets and Systems **81** (1996), 235–236

[66] Ray, A. K., *On product of fuzzy subgroups* Fuzzy Sets and Systems **105** (1999), 181–183

[67] Ray, S., *Isomorphic Fuzzy Groups.* Fuzzy Sets and Systems **50** (1992), 201–207.

[68] Ray, S., *Solvable Fuzzy Groups.* Information Sciences **75** (1993), 47–61.

[69] Redei, L., *Algebra, Volume 1* Mathematical Institute, University of Szeged, Hungary (1967).

[70] Regonati, Francesco,On the numbers of subgroups of given order of finite Abelian p-groups. (Italian) Istit. Lombardo Accad. Sci. Lett. Rend. A 122 (1988), 369–380 (1989).

[71] Riordan, John, *An Introduction to Combinatorial Analysis.* Third Edition, John Wiley and Sons, Inc., New York (1958).

[72] Rosen, Kenneth, A., *Discrete Mathematics and its Applications.* Third Edition, McGraw-Hill International Editions (1995).

[73] Rosenfeld, A., Fuzzy Groups, *J. Math. Anal. Appl.*35: 512-517(1971).

[74] Rotman, Joseph J., *The Theory of Groups - An Introduction.* 2nd Edition (1976)

[75] Saxena, P. K., *Fuzzy subgroups as union of two fuzzy subgroups*, Fuzzy Sets and Systems **57** (1993), 209–218

[76] Schenkman, Eugene, *Group Theory* , Addison-Wesley Publishing Company (1965).

[77] Sebastian, S.; Sundar S. Babu, *Fuzzy Groups and Group Homomorphisms.* Fuzzy Sets and Systems **81** (1996), 397–401.

[78] Sidky, F. I; Mishref, M. A, *Divisible and Pure Subgroups.* Fuzzy Sets and Systems **34** (1990), 377–382.

[79] Sloane, N. J. A, *On-Line Encyclopaedia of Integer Sequences* , Published electronically at **http://www.research.att.com/∼njas/sequences**.

[80] Stanley R. P., *Enumerative Combinatorics*, Cambridge, Vol. 2, 1999; see page 178.

[81] Stehling, Thomas *On Computing the Number of Subgroups of a Finite Abelian Group.* Combinatorica **12** (1992), no. 4, 475–479.

[82] Takegahara, Yugen, *The Number of Homomorphisms from a Finite Abelian Group to a Finite Group. Group Theory and Combinatorial Mathematics* No. 991 (1997), 171–179

[83] Vogt, Frank *Subgroup Lattices of Finite Abelian Groups: structure and cardinality.* Lattice Theory and its Applications (Darmstadt, 1991), 241–259,

[84] Voigt, Bernd, *The Partition Problem for Finite Abelian Groups.* J. Combin. Theory Ser. A **28** (1980), no. 3, 257–271.

[85] Wigner, Eugene P., *Group Theory and its Applications to the Quantum Mechanics of Atomis Spectra*, Addison-Wesley Publishing Company (1959).

[86] Willans,C.P.,*On Formulae for the Nth Prime Number*, Mathematical Gazette Volume 48 (1964), 413– 415.

[87] Xu, Ju Yong, *Enumeration of Equivalence Classes of Subsets of a Finite Abelian Group*, Appl. Math. J. Chinese Univ. Ser. A **17**(2002), 237–242.

[88] Yasuda, Kan,*On the automorphism group of the subgroup lattice of a finite Abelian p-group*; some generalizations. Combinatorial representation theory and related topics (Japanese) (Kyoto, 2002) . Sūrikaisekikenkyūsho Kōkyūroku No. 1310 (2003), 169–177.

[89] Zadeh, L. A *Fuzzy Sets.* Information and Control **8** (1965), 338–353.

[90] Zhang, Y., Zou, K. , *A note on an equivalence relation on fuzzy subgroups (short communication)* Fuzzy Sets and Systems **95** (1998), 243–247