

**A STUDY ON EXHAUSTION NUMBERS AND COMPLETE  
DECOMPOSITIONS OF SUBSETS OF SOME FINITE GROUPS**

**SYAFIQ AIMAN BIN NOORHAIZAN**


**A project report submitted in partial fulfilment of  
the requirements for the award of Bachelor of Science  
(Honours) Applied Mathematics With Computing**

**Lee Kong Chian Faculty of Engineering and Science  
Universiti Tunku Abdul Rahman**

**JUNE 2023**

**DECLARATION**

I hereby declare that this project report is based on my original work except for citations and quotations which have been duly acknowledged. I also declare that it has not been previously and concurrently submitted for any other degree or award at UTAR or other institutions.

Signature :  \_\_\_\_\_

Name : SYAFIQ AIMAN BIN NOORHAIZAN

ID No. : 2006309

Date : 8 / 9 / 2023

**APPROVAL FOR SUBMISSION**

I certify that this project report entitled “**A STUDY ON EXHAUSTION NUMBERS AND COMPLETE DECOMPOSITIONS OF SUBSETS OF SOME FINITE GROUPS**” was prepared by **SYAFIQ AIMAN BIN NOORHAIZAN** has met the required standard for submission in partial fulfilment of the requirements for the award of Bachelor of Science (Honours) Applied Mathematics With Computing at Universiti Tunku Abdul Rahman.

Approved by,

Signature : Chen

Supervisor : Chen Huey Voon

Date : 8/9/2023

Signature : \_\_\_\_\_

Co-Supervisor : \_\_\_\_\_

Date : \_\_\_\_\_

The copyright of this report belongs to the author under the terms of the copyright Act 1987 as qualified by Intellectual Property Policy of Universiti Tunku Abdul Rahman. Due acknowledgement shall always be made of the use of any material contained in, or derived from, this report.

© 2023, SYAFIQ AIMAN BIN NOORHAIZAN. All rights reserved.



## TABLE OF CONTENTS

<b>DECLARATION</b>		<b>i</b>
<b>APPROVAL FOR SUBMISSION</b>		<b>ii</b>
<b>TABLE OF CONTENTS</b>		<b>iii</b>
<b>LIST OF TABLES</b>		<b>vi</b>
<b>LIST OF SYMBOLS / ABBREVIATIONS</b>		<b>vii</b>
<b>LIST OF APPENDICES</b>		<b>viii</b>
 <b>CHAPTER</b>		
<b>1</b>	<b>INTRODUCTION</b>	<b>1</b>
	1.1 General Introduction	1
	1.2 Objectives	1
	1.3 Problem Statement	2
	1.4 Work Plan	3
 <b>2</b>	<b>LITERATURE REVIEW</b>	 <b>4</b>
	2.1 Introduction	4
	2.2 Exhaustion Numbers of Subsets of Finite Groups	6
	2.3 Complete Decompositions of Finite Groups	6
	2.4 Programming Language	7
 <b>3</b>	<b>SOME PROPERTIES OF GROUPS AND SUBGROUPS</b>	 <b>8</b>
	3.1 Some Results on Group Theory	8
	3.2 Some Results on Cyclic Groups	9
	3.3 The Groups of Interest	10
 <b>4</b>	<b>EXHAUSTION NUMBERS OF SUBSETS OF FINITE</b>	 <b>12</b>
	<b>GROUPS</b>	<b>12</b>
	4.1 Introduction	12
	4.1.1 Algorithm For Finding the Exhaustion Num- bers of Subsets of a Finite Group	13

4.2	Groups of $2 \times 2$ Diagonal Matrices over $\mathbb{Z}_n$	14
4.3	Groups of $2 \times 2$ Upper Triangular Matrices over $\mathbb{Z}_n$	20
4.4	Groups of General $2 \times 2$ Matrices over $\mathbb{Z}_2$	22
<b>5</b>	<b>COMPLETE DECOMPOSITIONS OF ORDER <math>k</math> OF FINITE GROUPS</b>	<b>24</b>
5.1	Introduction	24
5.2	Groups of $2 \times 2$ matrices over $\mathbb{Z}_2$	25
5.2.1	Complete Decompositions of order 3, 4, 5 of $G_2^d$	25
5.2.2	Complete Decompositions of order 3, 4, 5 of $G_2^t$	26
5.2.3	Complete Decompositions of order $k$ of $G_2$	29
5.3	Groups of $2 \times 2$ matrices over $\mathbb{Z}_3$	29
5.3.1	Complete Decompositions of order 2 of $G_3^d$	29
5.3.2	Complete Decompositions of order 2 of $G_3^t$	30
5.3.3	Complete Decompositions of order 2 of $G_3$	32
<b>6</b>	<b>CONCLUSION AND RECOMMENDATIONS</b>	<b>36</b>
6.1	Conclusion	36
6.2	Recommendations	36

## LIST OF TABLES

Table 4.1:	The exhaustion numbers of all 2-subsets of $G_2^d$	15
Table 4.2:	The exhaustion numbers of all 3-subsets of $G_2^d$	15
Table 4.3:	List of exhaustion numbers of all subsets of $G$	16
Table 4.4:	Exhaustion number for diagonal $2 \times 2$ matrices over $\mathbb{Z}_3, G_3^d$	17
Table 4.5:	Exhaustion number for diagonal $2 \times 2$ matrices over $\mathbb{Z}_5$	18
Table 4.6:	Some Largest Non-Exhaustive Subsets of $G_2^t$	21
Table 4.7:	Some Largest Non-Exhaustive Subsets of $G_3^t$	21
Table 4.8:	Some Largest Non-Exhaustive Subsets of $G_2$	22
Table 5.1:	All Partitions of Size 3 of $G_2^d$	26
Table 5.2:	Some Complete Decompositions of Order 3 of $G_2^t$	27
Table 5.3:	Some Complete Decompositions of Order 4 of $G_2^t$	28
Table 5.4:	Some Complete Decompositions of Order 5 of $G_2^t$	28
Table 5.5:	Some Complete Decompositions of Order 3 of $G_2$	29
Table 5.6:	Some Complete Decompositions of Order 2 of $G_3^d$	30
Table 5.7:	Some Complete Decompositions of Order 2 of $G_3^t$	31
Table 5.8:	Some Complete Decompositions of Order 2 of $G_3$	33

**LIST OF SYMBOLS / ABBREVIATIONS**

LNES: largest non-exhaustive subset

$$G_n = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{Z}_n \right\}$$

$$G_n^{tt} = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a, b, c \in \mathbb{Z}_n \right\}$$

$$G_n^d = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} : a, b \in \mathbb{Z}_n \right\}$$

**LIST OF APPENDICES**

APPENDIX A1: List Of Exhaustion Numbers Of Subsets Of Finite Groups

APPENDIX A2: ALL LNES of  $G_2^t$

APPENDIX A3: ALL LNES of  $G_3^t$

APPENDIX A4: ALL LNES of  $G_2$

APPENDIX B1: Complete Decompositions of Order 3 of  $G_2^t$

APPENDIX B2: Complete Decompositions of Order 4 of  $G_2^t$

APPENDIX B3: Complete Decompositions of Order 5 of  $G_2^t$

APPENDIX B4: Complete Decompositions of Order 3 of  $G_2$

APPENDIX B5: Complete Decompositions of Order 2 of  $G_3^d$

APPENDIX B6: Complete Decompositions of Order 2 of  $G_3^t$

APPENDIX B7: Complete Decompositions of Order 2 of  $G_3$

## CHAPTER 1

### INTRODUCTION

#### 1.1 General Introduction

Group theory has been applied to make many discoveries in the field of mathematics and physics since its early history. In the field of mathematics, a famous unsolved geometry problem was refactored in terms of groups, and was later solved using group theory. In physics, group theory has been applied in various fields such as quantum mechanics and crystallography.

Group factorization is the decomposition of an abelian (commutative) group into a sum of its subsets. Group factorization has many applications in mathematics and other fields. In 1983, an unsolved well-known geometry problem proposed by H. Minkowski was reformulated by G.Hajós into an equivalent problem in terms of group factorization. In 1941, Hajós was able to solve this problem by applying group theory. This project will be focused on two special cases of group factorization which are called exhaustion numbers of subsets of finite groups and complete decompositions of finite groups.

One of the main reasons people are interested in exhaustion numbers of subsets of finite groups is because of its applications in cryptography. Group factorization also has applications in secret and public key cryptosystems. Exhaustion numbers and group factorization are important in cryptography to protect the privacy of internet users.

#### 1.2 Objectives

The objectives of this project are:

1. Generalize results for the largest non-exhaustive subsets of

$$G_n = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{Z}_n \right\}$$

and list down the exhaustion numbers of all subsets of

- (a)  $G_n$  for  $b = c = 0$  (diagonal matrices) and  $n = 3, 5$

(b)  $G_n$  for  $c = 0$  (upper triangular matrices) and  $n = 2, 3$

2. Find the complete decompositions of  $G$  and list down all complete decompositions of  $G$  of order 3 for  $n = 2$ .

### 1.3 Problem Statement

Factorizations of abelian groups have had applications in areas of mathematics such as completion of codes and the Rédei property of groups (Szabó, 2006). Group factorization has also seen several applications in cryptography. Magliveras (2002) introduced a public key cryptosystem in which group factorization is applied. A secure encryption scheme was developed by Cong et al. (2019) which uses a group factorization problem.

Let  $G$  be a finite group which has the operation of addition and  $H$  a subset of  $G$ . If  $G = H + H + \dots + H$  ( $n$  times), then  $H$  is called  $n$ -exhaustive where the sum of two sets (called sumset)  $C + D = \{c + d : c \in C, d \in D\}$ . For convenience, we write  $nH = H + H + \dots + H$  ( $n$  times). If  $H$  is  $n$ -exhaustive, then the exhaustion number of the set  $H$ ,  $e(H)$ , is the minimum integer  $n > 0$ . If there doesn't exist an integer  $n$  such that  $nH = G$ , then  $e(H) = \infty$  and we say  $H$  is not exhaustive. Let  $G$  be an abelian group and let  $A_1, \dots, A_h$  ( $h \geq 2$ ) be a partition of  $G$ . If  $A_1 + \dots + A_h = G$ , then  $A_1, \dots, A_h$  is called a complete decomposition of  $G$  of order  $h$ .

The group of interest in this project is the set of  $2 \times 2$  matrices whose entries are elements of  $\mathbb{Z}_n$  together with the sum operation:

$$G = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b \in \mathbb{Z}_n \right\}.$$

We will also attempt to develop programming techniques to assist in finding the exhaustion numbers of subsets of finite groups and complete decompositions of finite groups. In order to find the results, we will need to go through every case one by one. Doing the calculations manually is impractical since there are too many cases to go through. Therefore, we will use a programming language to assist in listing down the numerical data. The programming language that will be used is Python because of its vast data science libraries.

After listing down all the numerical data, we will look for patterns and try to generalize the result for  $G$  where  $n$  is prime.

#### 1.4 Work Plan

The flow of projects 1 and 2 will follow the gantt charts below:

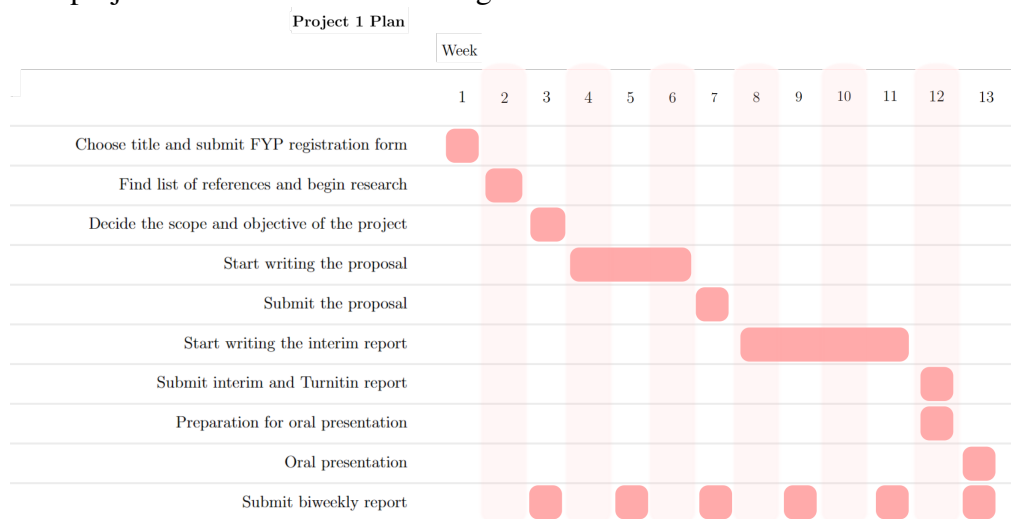


Figure 1.1: Gantt Chart for Project 1

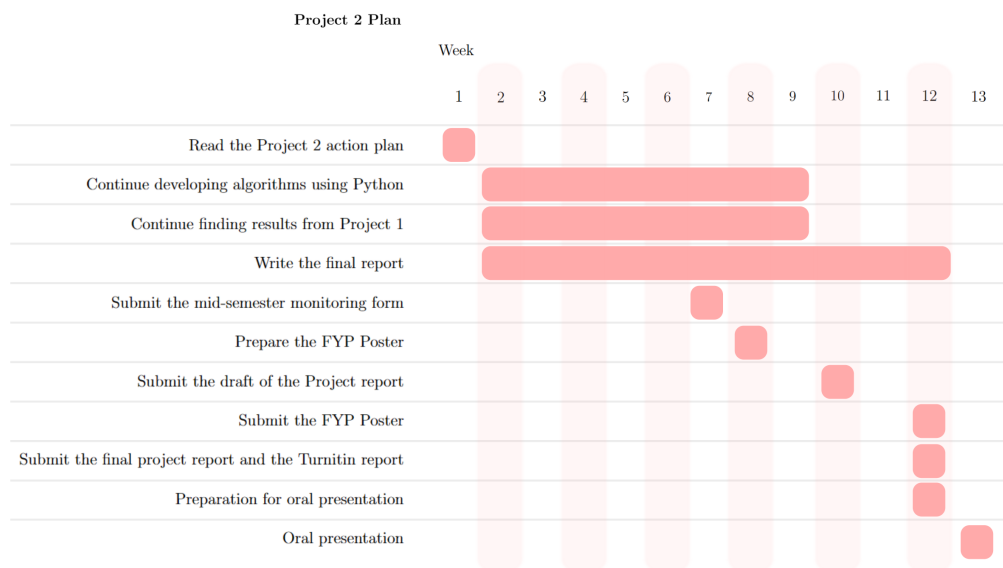


Figure 1.2: Gantt Chart for Project 2



## CHAPTER 2

### LITERATURE REVIEW

#### 2.1 Introduction

One of the earliest contributions in the history of group theory was made by Leonard Euler in 1760. Euler gave a generalization of one of Fermat's theorems: natural numbers which are coprime to  $k$  and are less than or equal to  $k$  is equivalent to an abelian group together with multiplication modulo  $k$  (Miller, 1964). Group theory is important because it has many applications in chemistry, theoretical physics and electrical engineering (Hamermesh, 1989).

In the field of crystallography, the symmetries of crystals are represented by groups with symmetry operations. A symmetry operation of an object is a motion that maps an object onto itself. It turns out that all symmetry operations for a given object obeys the four axioms of a group, that is, the set of all symmetry operations of an object form a group. Therefore any theorems of groups may be applied to the symmetries of objects (Prince, 1984).

An interesting research within the area of group theory is group factorization. Group factorization is the decomposition of a commutative group into a sum of its subsets. Let  $G$  be a finite abelian group and let  $D, C_1, \dots, C_n$  be subsets of  $G$ . If there are unique elements  $c_1, \dots, c_n$  of  $G$  for every  $d$  in  $D$  such that

$$d = c_1 + \dots + c_n, \quad c_1 \in C_1 \dots c_n \in C_n,$$

then we say that  $D = C_1 + \dots + C_n$  is a factorization of  $D$  (Szabo and Sands, 2009). Usually, the cases considered are when  $C_1, \dots, C_n$  are cyclic subgroups of  $G$  and  $D = G$ . A cyclic group  $G$  is a group that contains an element  $a$  such that  $\forall b \in G$ , there exists an integer  $n$  such that  $b = a^n$ . Thus,  $a$  is known as the generator of the group. Now we focus on subsets of a group which also form groups. A subset  $S$  is called a subgroup of  $G$  if  $x, y \in S$ , then  $xy^{-1} \in S$ .

Let  $G$  be an abelian group. A subset  $S \subseteq G$  is called periodic if  $\exists k \in G, k \neq 0$  where  $S + k = S$ . If at least  $C$  or  $D$  is periodic in every factorization  $G = C + D$ , we say that  $G$  has the Hajós property. Hajós (1949) began classifying finite abelian groups having this property. This effort is com-

pleted in 1962, and all groups which has the Hajós property was listed in (Sands, 1962).

Group factorization can be seen as a combination of an algebraic and a combinatorial problem. The results have been applied to many fields including error correcting codes, cryptography, graph theory and more (Szabo and Sands, 2009). One of the first results of group factorization is shown by Cauchy (1813), then later by Davenport (1935). This resulted in the Cauchy-Davenport theorem which states: If  $C, D$  are subsets of an abelian group, then

$$|C + D| \geq |C| + |D| - 1.$$

The well-known unsolved problem in geometry proposed by Minkowski (1896) was rewritten as a group factorization problem by Hajós (1938). After three years, Minkowski's problem was solved by Hajós (1942). After this breakthrough, more attention was given to group factorization.

In the field of cryptography, several applications of group factorization can be found. As the internet continues to take over the world, research and applications in the field of cryptography is becoming more important to protect the privacy and security of its users. Chen and Sin (2021a) did a study on how group coverings of subsets of finite groups can be applied in cryptography. Other researchers who contributed in this field include Magliveras (2002), who used group factorizations to construct public and secret key cryptosystems, and Baba et al. (2011) introduced a cryptosystem based on a group factorization problem.

The concept of a group has been expanded and new studies have been formed in this field. The study that we are interested in is called group factorization. Szabo and Sands (2009) have shown the interesting properties and applications of factoring groups into subsets. Zhou (2017) researched the multiple factorizations of cyclic groups. Zhou showed that for any cyclic group  $G$ , there does not exist distinct subsets  $A, B, C \subseteq G$  such that  $G$  has the group factorizations  $G = AB = AC = BC$ .

The topics that we are interested in are exhaustion numbers of subsets of finite groups and complete decompositions of finite groups. In section 2.2, we will discuss some previous results and research done on the exhaustion numbers

of subsets of some finite groups. In section 2.3, we will discuss some previous results and research done on the complete decompositions of some finite groups. In section 2.4, we discuss the programming language used to find the numerical data for the project.

## 2.2 Exhaustion Numbers of Subsets of Finite Groups

Chin (1999) has found the exhaustion numbers of certain subsets of some cyclic groups. It was found that the exhaustion number of a set  $H$  which is in arithmetic sequence and the common difference  $k$  is coprime to  $n$ , such that  $H \subseteq \mathbb{Z}/n$ ,  $n \geq 2$  with  $|H| = h > 1$ , then  $e(H) = \lceil \frac{n-1}{h-1} \rceil$ .

Furthermore, if  $H$  is in arithmetic sequence but the common difference  $k$  is not coprime to  $n$ , then  $e(H) = \infty$ . Chin (2003) has determined the exhaustion numbers of various subsets of finite abelian groups. Chen et al. (2012) has shown the exhaustion numbers of 2-subsets of dihedral groups. It was shown that if  $S$  is a 2-subset of  $D_{2n}$  for an even integer  $n$  where  $n \geq 6$ , then  $e(S) = \infty$ .

A study was done on subsets of finite groups which were exhaustive and non-exhaustive (Chen and Chin, 2017). Wong et al. (2018) did a study on exhaustion 2-subsets in dihedral groups of order  $2p$ , where  $p$  is an odd prime. The authors classified all possible exhaustion 2-subsets in  $D_{2p}$  by considering a 2-subset  $A = \{a_1, a_2\}$  of  $D_{2p}$  with either  $A \subset \langle k \rangle$ ,  $A \subset \langle k \rangle s$  or  $a_1 \in \langle k \rangle$  and  $a_2 \in \langle k \rangle m$ .

## 2.3 Complete Decompositions of Finite Groups

Chin and Chen (2018) determined the integers  $a$  where there exists a complete decomposition of order  $a$  for  $\mathbb{Z}_k$  ( $k \geq 6$ ). The main results are as follows. Let  $j > 0$  be the smallest integer such that  $2^j \geq k$  where  $k \geq 6$ . For each  $a \in [2, k - j]$ , there exists a complete decomposition for  $\mathbb{Z}_k$  of order  $a$ .

Chen and Sin (2021b) conducted a study on complete decompositions of dihedral groups. The paper shows constructions of the complete decompositions of  $D_{2n}$  of order  $t$ , where  $2 \leq t \leq n$ . The authors constructed complete decompositions of order 2 for  $D_{2n}$ , where  $C \cap D = \emptyset$ ,  $|C| \neq |D|$  and  $C \cup D \subset D_{2n}$ . Let  $n \geq 3$  be an integer. Let  $C = \{1, r, \dots, r^{n-3}, r^{n-2}s, r^{n-1}s\}$  and  $D_j = \{r^{n-2}, r^{n-1}, s, rs, \dots, r^{n-3}s\} \setminus \{rs, r^3s, \dots, r^j s\}$ , where  $C, D_j \subseteq$

$D_{2n}, j \in \{1, 3, \dots, n - 5\}$ ,  $|C| = 5$  and  $|D| = n - \frac{j+1}{2}$ . Then  $(C, D_j)$  is a complete decomposition of order 2 for  $D_{2n}$ .

## 2.4 Programming Language

To find the exhaustion numbers of a group subset, the brute force method will be used. The brute force method is an algorithm to solve problems by going through every possible combination until a solution is found. The programming language used for this project will be Python. Python is a suitable language to be used in this project because of its `itertools` package. The package contains useful functions such as `combinations` which can find all subsets of a list of elements. It also allows us to iterate through a list efficiently (Soklaski, 2021).

## CHAPTER 3

### SOME PROPERTIES OF GROUPS AND SUBGROUPS

#### 3.1 Some Results on Group Theory

The algebraic object known as a group serves as one of the foundations for abstract algebra. A group  $G$  is a set and a binary operation for any two elements in the set  $C, D$ , denoted as  $C * D$ , which combines any two elements from the set to produce a third element of the set. A group must satisfy these properties:

1. Closed  $C * D \in G, \forall C, D \in G$ ;
2. Associative law  $C * (D * E) = (C * D) * E, \forall C, D, E \in G$ ;
3. Existence of an identity element  $\exists \alpha \in G$  where  $C * \alpha = C, \forall C \in G$ ;
4. Existence of inverses  $\forall C \in G, \exists C^{-1} \in G$  where  $C * C^{-1} = \alpha$ .

A group  $G$  is called an abelian group if  $\forall C, D \in G, C * D = D * C$ . An interesting property of a group  $G$  is the called the order of  $G$ . The order of a group is the number of elements in its set. In this project, we focus on groups with finite elements, which are called finite groups (Herstein, 1975). For example, consider the group  $G$  consisting of  $\mathbb{Z} = \{\dots - 2, -1, 0, 1, 2 \dots\}$ , the set of all integers, together with the sum operation. It can be seen that:

1.  $C + D$  is an integer  $\forall C, D \in G$  (closed);
2.  $C + (D + E) = (C + D) + E \forall C, D, E \in G$  (associative law);
3.  $C + 0 = C \forall C \in G$  where 0 is the identity element (existence of identity element);
4. There exists an element  $D$  for every element  $C$  such that  $C + D = 0$  where  $D = -C \forall C, D \in G$  (existence of inverse element).

Next, consider the set  $S$  of all integers together with multiplication. Since integers does not have a multiplicative inverse which is also an integer, the set  $S$  and the multiplication operation do not form a group.

**Theorem 3.1** A subgroup of  $G$  is a subset  $D$  of  $G$  together with the binary operation of  $G$ . A nonempty subset  $D$  is a subgroup of  $G$  if and only if:

1. for any two elements  $X, Y$  in  $D$ ,  $X * Y$  is in  $D$ ;
2. for any element  $X$  in  $D$ ,  $X^{-1}$  is in  $D$ .

*proof* ( $\Rightarrow$ ) If  $D$  is a subgroup of  $G$ , then obviously (1) and (2) hold. ( $\Leftarrow$ ) Suppose that  $D$  is a subset of  $G$  such that (1) and (2) hold. To show that  $D$  is a subgroup, we need to show that  $\alpha$  is in  $D$ , and all the elements of  $D$  obeys the associative law. Because the associative law holds for  $G$ , then it will clearly hold for  $D$ , which is a subset of  $G$ . If  $X$  is in  $D$ , then by (2),  $X^{-1}$  is in  $D$ , and by (1),  $XX^{-1} = \alpha$  is in  $D$ . This completes the proof (Lal, 2017).

### 3.2 Some Results on Cyclic Groups

Let  $G$  be a group under addition.  $G$  is called a cyclic group if there exists an element  $g \in G$  such that  $G = \{ng : n \in \mathbb{Z}\}$ . Then  $g$  is called a generator of  $G$  and  $G$  is a group generated by  $g$ , denoted by  $G = \langle g \rangle$ . The order of a group is the number of elements in the group. The order of an element  $g \in G$  is the smallest positive integer  $n$  such that  $ng = 0$ . If such  $n$  doesn't exist, then the element is said to be of infinite order.

**Example 3.1.** The groups  $\mathbb{Z}$  and  $\mathbb{Z}_n$  are cyclic groups.  $\mathbb{Z}$  is a group generated by 1 and has infinite order. The group  $\mathbb{Z}_n$  is a cyclic group of order  $n$ . For example,  $\mathbb{Z}_5$  is generated by 1:

$$1 \equiv 1 \pmod{5}$$

$$1 + 1 \equiv 2 \pmod{5}$$

$$1 + 1 + 1 \equiv 3 \pmod{5}$$

$$1 + 1 + 1 + 1 \equiv 4 \pmod{5}$$

$$1 + 1 + 1 + 1 + 1 \equiv 0 \pmod{5}$$

**Theorem 3.2.** Let  $(S, *)$  be an infinite cyclic group generated by  $a$ . Then,  $\langle a^k \rangle = \langle a^l \rangle$  if and only if  $k = \pm l$ . Particularly,  $\langle a^k \rangle = G$  if and only if  $k = \pm 1$

*Proof.* It is obvious that  $\langle a^k \rangle = \langle a^{-k} \rangle$ . Suppose that  $\langle a^l \rangle = \langle a^k \rangle$ . Then there exist  $m, n \in \mathbb{Z}$  such that  $a^k = (a^l)^m$  and  $a^l = (a^k)^n$ . Since  $a$  is

of infinite order,  $k = lm$  and  $l = kn$ . This shows that  $mn = 1$ , and therefore  $k = \pm l$

**Theorem 3.3.** For any divisor  $d$  of the order of a cyclic group, there exists a unique subgroup of order  $d$ .

*Proof.* Let  $(G, *)$  be a cyclic group of order  $k$  generated by  $g$ . Let  $d|k$ . Then  $\langle g^{\frac{k}{d}} \rangle$  is the unique subgroup of order  $d$ .

**Theorem 3.4.** Let  $G$  be a finite cyclic group generated by  $g$ , where the order of  $g$  is  $m$ . Then the powers  $\{g^0, g^1, \dots, g^{m-1}\}$  are unique.

*Proof.* Since  $g$  has order  $m$ ,  $g, g^2, \dots, g^{m-1}$  are not equal to 1. Assume that  $g^k = g^l$  where  $0 \leq k < l < m$ . Then  $l - k < m$  and  $g^{l-k} = 1$ , a contradiction.  $\therefore$  the powers  $\{g^0, g^1, \dots, g^{m-1}\}$  are unique.

**Theorem 3.5** Let  $G$  be a group, and let  $g \in G$  have order  $k$ . Then  $g^l = 1$  if and only if  $k$  divides  $l$ .

*Proof.* If  $k$  divides  $l$ , then  $l = kq$  for some  $q$  and  $g^l = (g^k)^q = 1$ .

Conversely, suppose that  $g^l = 1$ , by the division algorithm:

$$l = m = kq + r \text{ where } 0 \leq r < k.$$

Hence,

$$g^l = g^{kq+r} = (g^k)^q g^r \text{ so } g^r = 1.$$

Since  $k$  is the smallest positive of power of  $g$  where  $g^k = 1$ , and  $r < k$ , this is only true if  $r = 0$ . Therefore,  $l = kq$ , which implies that  $k$  divides  $l$ .

### 3.3 The Groups of Interest

In this project, we are interested in certain groups of matrices. The first group,  $G_n^d$ , is a group over addition of all  $2 \times 2$  diagonal matrices over  $\mathbb{Z}_n$ , that is,  $G = (S, +)$  where

$$S = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} : a, b \in \mathbb{Z}_n \right\}$$

For example, if  $n = 2$ , then

$$S = \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}$$

The second group is  $G_n^t$ , a group over addition of all  $2 \times 2$  upper triangular matrices over  $\mathbb{Z}_n$ , that is,  $G = (T, +)$  where

$$T = \left\{ \begin{pmatrix} a & b \\ c & 0 \end{pmatrix} : a, b, c \in \mathbb{Z}_n \right\}$$

Finally the third group is  $G_n$ , a group over addition of all  $2 \times 2$  matrices over  $\mathbb{Z}_n$ , that is,  $G = (U, +)$  where

$$U = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{Z}_n \right\}$$



## CHAPTER 4

### EXHAUSTION NUMBERS OF SUBSETS OF FINITE GROUPS

#### 4.1 Introduction

**Definition 4.1** Let  $G$  be a finite group which has the operation of addition and  $H$  a subset of  $G$ . If  $G = H + H + \cdots + H$  ( $n$  times), then  $H$  is called  $n$ -exhaustive where the sum of two sets (called sumset)  $C + D = \{c + d : c \in C, d \in D\}$ . For convenience, we write  $nH = H + H + \cdots + H$  ( $n$  times). If  $H$  is  $n$ -exhaustive, then the exhaustion number of the set  $H$ ,  $e(H)$ , is the minimum integer  $n > 0$ . If there doesn't exist an integer  $n$  such that  $nH = G$ , then  $e(H) = \infty$  and we say  $H$  is not exhaustive.

**Example 4.1** Let

$$\begin{aligned} G &= \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} : a, b \in \mathbb{Z}_2 \right\} \\ &= \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\} \end{aligned}$$

and

$$A = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \right\}.$$

To find the exhaustion number of  $A$ , we start by finding the sumsets of  $A$  until  $nA = G$  is found:

$$\begin{aligned} A &= \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \right\}; \\ A + A &= \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}; \\ A + A + A &= \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \right\} = A. \end{aligned}$$

We notice that  $A + A + A = A$ , if we keep adding up  $A$ , the sequence of sumsets

will repeat itself. Therefore, the exhaustion number of  $A$ ,  $e(A) = \infty$ . We can easily use this argument to show that the exhaustion numbers of all 2-subsets of  $G$  is  $\infty$ .

Next, consider the subset

$$B = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}.$$

Note that the sumsets of  $B$ ,

$$B + B = \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \right\} = G.$$

Therefore  $e(B) = 2$ .

#### **4.1.1 Algorithm For Finding the Exhaustion Numbers of Subsets of a Finite Group**

To find the exhaustion numbers of a subset  $a$ , the brute force method is used. The brute force method is an algorithm to solve problems by going through every possible combination until a solution is found. The programming language used for this project is Python. Python is a suitable language to be used in this project because of its `itertools` package. The package contains useful functions such as `combinations` which can find all subsets of a list of elements. It also allows us to iterate through a list efficiently. The algorithm is summarized below:

**Algorithm: Find the exhaustion number of a subset of a finite group.**

1. Get all matrices for the underlying set  $S$  of the group of interest.
2. List down all 2-subsets and 3-subsets of the set.
3. Initialize an empty list of sumsets.
4. For each subset  $A$ , find the sumset  $A + A + \cdots + A = nA$  where  $n = 1, 2, \dots$
5. If  $nA = S$ , the exhaustion number of  $A$ ,  $e(A) = n$ , move to the next subset.
6. Else if  $nA$  is already in the list of sumsets, then the exhaustion number of  $A$ ,  $e(A) = \infty$ .
7. Else, for each  $n$ , append  $nA$  to the list of sumsets.

**4.2 Groups of  $2 \times 2$  Diagonal Matrices over  $\mathbb{Z}_n$** 

We list down the exhaustion numbers of all subsets of  $G_2^d$  where

$$\begin{aligned}
 G_2^d &= \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} : a, b \in \mathbb{Z}_2 \right\} \\
 &= \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}
 \end{aligned}$$

Table 4.1: The exhaustion numbers of all 2-subsets of  $G_2^d$ 

Subset, $A$	$e(A)$
$\left\{ \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \right\}$	$\infty$
$\left\{ \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}$	$\infty$
$\left\{ \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\}$	$\infty$
$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}$	$\infty$
$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\}$	$\infty$
$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\}$	$\infty$

Table 4.2: The exhaustion numbers of all 3-subsets of  $G_2^d$ 

Subset, $A$	$e(A)$
$\left\{ \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}$	2
$\left\{ \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\}$	2
$\left\{ \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\}$	2
$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\}$	2

We find that all six 2–subsets of  $G_2^d$  has exhaustion number  $\infty$  and all four 3–subsets of  $G_2^d$  has exhaustion number 2. We summarize the results in the following table:

Table 4.3: List of exhaustion numbers of all subsets of  $G$

Size of subset	Exhaustion number	Number of subsets
2	$\infty$	6 (All)
3	2	4 (All)

We repeat this process using cyclic group over  $\mathbb{Z}_3$  where

$$\begin{aligned}
 G_3^d &= \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} : a, b \in \mathbb{Z}_3 \right\} \\
 &= \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \right. \\
 &\quad \left. \begin{pmatrix} 0 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \right\}
 \end{aligned}$$

Table 4.4: Exhaustion number for diagonal  $2 \times 2$  matrices  
over  $\mathbb{Z}_3, G_3^d$

Size of subset	Exhaustion number	Number of subsets
2	$\infty$	36 (All)
3	4	72
	$\infty$	12
4	2	54
	3	72
5	2	126 (All)
6	2	84 (All)
7	2	36 (All)
8	2	9 (All)

Notice that the largest subset where the exhaustion number is  $\infty$  is the 3–subset.

The following is a list of the twelve 3–subsets which are not exhaustive:

1.  $\left\{ \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix} \right\}$
2.  $\left\{ \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}$
3.  $\left\{ \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 2 \end{pmatrix} \right\}$
4.  $\left\{ \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \right\}$
5.  $\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\}$
6.  $\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \right\}$

$$\begin{aligned}
7. & \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \right\} \\
8. & \left\{ \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \right\} \\
9. & \left\{ \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \right\} \\
10. & \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \right\} \\
11. & \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \right\} \\
12. & \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 2 \end{pmatrix} \right\}
\end{aligned}$$

We observe the sum of all elements from each of the subsets is the zero matrix. For example, taking the first subset:

$$\begin{aligned}
\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} + \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix} &= \begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix} \pmod{3} \\
&= \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \pmod{3}
\end{aligned}$$

This result is true for all of the twelve matrices above. Next, we list down all exhaustion numbers for all subsets of  $G_5^d$ .

Table 4.5: Exhaustion number for diagonal  $2 \times 2$  matrices over  $\mathbb{Z}_5$

Size of subset	Exhaustion number	Number of subsets
2	$\infty$	300
3	8	2000

Continued on next page

Table 4.5: Exhaustion number for diagonal  $2 \times 2$  matrices  
over  $\mathbb{Z}_5$  (Continued)

3	$\infty$	300
4	4	6500
	6	6000
	$\infty$	150
5	3	600
	4	49500
	6	3000
	$\infty$	30
6	3	90500
	4	86000
	5	600
7	3	449500
	4	31200
8	2	13875
	3	1065000
	4	2700
9	2	383875
	3	1658500
	4	600
10	2	1880700
	3	1388000
	4	60
11	2	3874800
	3	582600

Continued on next page



Table 4.5: Exhaustion number for diagonal  $2 \times 2$  matrices  
over  $\mathbb{Z}_5$  (Continued)

12	2	5099100
	3	101200
13	2	5200300
14	2	4457400
15	2	3268760
16	2	2042975
17	2	1081575
18	2	480700
19	2	177100
20	2	53130
21	2	12650
22	2	2300
23	2	300
24	2	25

The largest non-exhaustive subset for diagonal  $2 \times 2$  matrices over  $\mathbb{Z}_5$  is the 5-subset. When listing down and checking all 30 of the largest non-exhaustive subsets, it is found that the previous result holds: all elements in a subset sum up to the zero matrix. The list of all 30 largest non-exhaustive subsets of  $G_5^d$  is attached in Appendix A1.

### 4.3 Groups of $2 \times 2$ Upper Triangular Matrices over $\mathbb{Z}_n$

We listed down the exhaustion numbers of all subsets of  $G_2^t = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a, b, c \in \mathbb{Z}_2 \right\}$  and  $G_3^t = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a, b, c \in \mathbb{Z}_3 \right\}$ . The tables are attached in the Appendix A1. The tables below show some of the largest non-exhaustive subsets of  $G_2^t$  and  $G_3^t$ .

Table 4.6: Some Largest Non-Exhaustive Subsets of  $G_2^t$ 

Subset, $A$
$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \right\}$
$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \right\}$
$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\}$
$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\}$
$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \right\}$

Table 4.7: Some Largest Non-Exhaustive Subsets of  $G_3^t$ 

Subset, $A$
$\left\{ \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 2 & 2 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 2 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\}$
$\left\{ \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 2 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 2 & 2 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \right\}$
$\left\{ \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 0 & 0 \end{pmatrix} \right\}$
$\left\{ \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 2 & 2 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 2 \\ 0 & 2 \end{pmatrix} \right\}$
$\left\{ \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 2 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 2 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 2 & 2 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix} \right\}$

Observe that the sum of all elements in each of the subsets is the zero matrix. The list of all largest non-exhaustive subsets of  $G_2^t$  and  $G_3^t$  is displayed in Appendix A2 and Appendix A3 respectively.

#### 4.4 Groups of General $2 \times 2$ Matrices over $\mathbb{Z}_2$

We listed down all exhaustion numbers of subset of  $G_2 = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{Z}_2 \right\}$ .

Below is a table of some of the largest non-exhaustive subsets of  $G_2$ . The list of all largest non-exhaustive subsets of  $G_2$  is displayed in Appendix A4.

Table 4.8: Some Largest Non-Exhaustive Subsets of  $G_2$

Subset, $A$
$\left\{ \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \right.$ $\left. \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} \right\}$
$\left\{ \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \right.$ $\left. \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \right\}$
$\left\{ \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \right.$ $\left. \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\}$
$\left\{ \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \right.$ $\left. \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \right\}$
$\left\{ \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}, \right.$ $\left. \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \right\}$

A few patterns were observed when looking through the data:

**Proposition 4.1** Let  $G_n^d = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} : a, b \in \mathbb{Z}_n \right\}$  for  $n \geq 2$ . Let  $H =$

$\left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} : a \in \mathbb{Z}_n \right\} \subseteq G_n^d$ . Then  $H$  is a non-exhaustive subset of  $G_n^d$  where  $|H| = n$ .

*Proof.* Note that  $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$ , so

$$H = \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix}, \dots, \begin{pmatrix} n-1 & 0 \\ 0 & 0 \end{pmatrix} \right\},$$

and we see that  $|H| = n$ . We observe that  $mH \neq G_n^d \forall m \in \mathbb{N}$  since  $\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \notin$

$mH \forall m \in \mathbb{N}$ . So,  $H$  is a non-exhaustive subset of  $G_n^d$ .

**Proposition 4.2** Let  $G_n^t = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a, b, c \in \mathbb{Z}_n \right\}$  for  $n \geq 2$ . Let  $H = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} : a, b \in \mathbb{Z}_n \right\} \subset G_n^t$ . Then  $H$  is a non-exhaustive subset of  $G_n^t$  where  $|H| = n^2$ .

*Proof.* Since  $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$  then

$$H = \left\{ \begin{array}{ccccccc} \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, & \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, & \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix}, & \cdots & \begin{pmatrix} n-1 & 0 \\ 0 & 0 \end{pmatrix}, \\ \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, & \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}, & \begin{pmatrix} 2 & 1 \\ 0 & 0 \end{pmatrix}, & \cdots & \begin{pmatrix} n-1 & 1 \\ 0 & 0 \end{pmatrix}, \\ \vdots & & & & \vdots \\ \begin{pmatrix} 0 & n-1 \\ 0 & 0 \end{pmatrix}, & \begin{pmatrix} 1 & n-1 \\ 0 & 0 \end{pmatrix}, & \begin{pmatrix} 2 & n-1 \\ 0 & 0 \end{pmatrix}, & \cdots & \begin{pmatrix} n-1 & n-1 \\ 0 & 0 \end{pmatrix} \end{array} \right\}$$

and we see that  $|H| = n^2$ . We observe that  $mH \neq G_n^t \forall m \in \mathbb{N}$  since  $\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \notin mH \forall m \in \mathbb{N}$ . Therefore,  $H$  is a non-exhaustive subset of  $G_n^t$ .

**Proposition 4.3** Let  $G_n = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{Z}_n \right\}$  for  $n \geq 2$ . Let  $H = \left\{ \begin{pmatrix} a & b \\ c & 0 \end{pmatrix} : a, b, c \in \mathbb{Z}_n \right\} \subset G_n$ . Then  $H$  is a non-exhaustive subset of  $G_n^t$  where  $|H| = n^3$ .

*Proof.* Since  $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$  then each entry in  $H$  can have  $n$  values, so  $|H| = n^3$ . Since the second row and second column entry of  $H$  can only be 0, then  $\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \notin mH \forall m \in \mathbb{N}$ , so  $mH \neq G_n \forall m \in \mathbb{N}$ . Therefore  $H$  is a non-exhaustive subset of  $G_n$ .

## CHAPTER 5

### COMPLETE DECOMPOSITIONS OF ORDER $k$ OF FINITE GROUPS

#### 5.1 Introduction

**Definition 5.1** Let  $G$  be a nontrivial abelian group and let  $A_1, \dots, A_h (h \geq 2)$  be a partition of  $G$ .  $(A_1, \dots, A_h)$  is a complete decomposition of  $G$  of order  $h$  if  $A_1 + \dots + A_h = G$ .

**Example 5.1** Consider the same group  $G_2^d = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} : a, b \in \mathbb{Z}_2 \right\}$  and its partition:

$$C_1 = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \right\}$$

$$C_2 = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\}$$

Taking  $C_1 + C_2$ , we get:

$$C_1 + C_2 = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \right\} \neq G$$

Therefore, the partition  $C_1, C_2$  is not a complete decomposition of  $G$ .

Next, consider the group  $G_3^d = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} : a, b \in \mathbb{Z}_3 \right\}$  and the partition of  $G_3^d$ :

$$D_1 = \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \right\}$$

$$D_2 = \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \right\}$$

Taking  $D_1 + D_2$ , we get:

$$D_1 + D_2 = \left\{ \begin{array}{l} \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, \\ \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \end{array} \right\} \\ = G.$$

Therefore the partition  $(D_1, D_2)$  is a complete decomposition of order 2 of  $G_3^d$ .

Below is the algorithm used to find the complete decompositions of order  $k$  of a group  $G$ .

**Algorithm: Find the complete decompositions of order  $k$  of a finite group.**

1. Initialize the group  $G$ .
2. Initialize the order  $k$  of the complete decomposition
3. For each  $k$ -partition  $(A_1, A_2, \dots, A_k)$  of  $G$ :
  - (a) If  $A_1 + A_2 + \dots + A_k = G$ , then  $(A_1, A_2, \dots, A_k)$  is a complete decomposition of order  $k$  of  $G$ .
  - (b) Else,  $(A_1, A_2, \dots, A_k)$  is not a complete decomposition of order  $k$  of  $G$ .

## 5.2 Groups of $2 \times 2$ matrices over $\mathbb{Z}_2$

### 5.2.1 Complete Decompositions of order 3, 4, 5 of $G_2^d$

In project 1, we have proved that complete decompositions of order 2 of  $G_2^d$  do not exist. Below is the proof:

**Proposition 5.1.** There are no complete decompositions of order 2 of  $G_2$ .

*Proof.* Assume there exists a complete decomposition of order 2 of  $G_2$ ,  $(A, B)$ . Since  $(A, B)$  is a partition of a set,  $A$  and  $B$  are pairwise disjoint. Then there exist matrices  $a \in A$  and  $b \in B$  such that  $a + b = \bar{0} \in G_2$ . Since elements in  $G_2$  are matrices over  $\mathbb{Z}_2$ , then  $a + b = \bar{0}$  if and only if  $a = b$ . But this is impossible

since  $A$  and  $B$  are pairwise disjoint. Therefore, there does not exist a complete decomposition of order 2 of  $G_2$ .

Following this result, we try to list down complete decompositions of order  $> 2$ . To find the complete decompositions of order 3 of  $G_2^d$ , we list down all partitions of the set and find the sum of all sets in the partition:

Table 5.1: All Partitions of Size 3 of  $G_2^d$

$B_1$	$B_2$	$B_3$	$B_1 + B_2 + B_3$
$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\}$	$\left\{ \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \right\}$	$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \right\}$	$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\}$
$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}$	$\left\{ \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \right\}$	$\left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\}$	$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}$
$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\}$	$\left\{ \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \right\}$	$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}$	$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\}$
$\left\{ \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \right\}$	$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}$	$\left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\}$	$\left\{ \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \right\}$
$\left\{ \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}$	$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \right\}$	$\left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\}$	$\left\{ \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}$
$\left\{ \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\}$	$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \right\}$	$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}$	$\left\{ \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\}$

We conclude that there are no complete decompositions of order 3 of  $G_2^d$ . The same is true for order 4. Therefore, there are no complete decompositions of order 4 of  $G_2^d$ .

### 5.2.2 Complete Decompositions of order 3, 4, 5 of $G_2^t$

Let  $G_2^t = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a, b, c \in \mathbb{Z}_2 \right\}$ . In this section, we display the numerical data for the complete decompositions of order 3, 4, 5 of  $G_2^t$ . In Table 5.2, we show some complete decompositions of order 3 of  $G_2^t$ . More examples are displayed in Appendix B1. The total number of complete decompositions of order 3 of  $G_2^t$  is 448.

Table 5.2: Some Complete Decompositions of Order 3 of  $G_2^t$ 

$B_1$	$B_2$	$B_3$
$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \right\}$	$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \right\}$	$\left\{ \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\}$
$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \right\}$	$\left\{ \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \right\}$	$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\}$
$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \right\}$	$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \right\}$	$\left\{ \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\}$
$\left\{ \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \right\}$	$\left\{ \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \right\}$	$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \right\}$
$\left\{ \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \right\}$	$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \right\}$	$\left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \right\}$

In table 5.3, we list down some complete decompositions of order 4 of  $G_2^t$ . More examples are displayed in Appendix B2. The total number of complete decompositions of order 4 of  $G_2^t$  is 728





### 5.2.3 Complete Decompositions of order $k$ of $G_2$

As stated in section 5.2.1, in Project 1 we tried to list down all complete decompositions of order 2 of  $G_2 = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{Z}_2 \right\}$  and proved that no such complete decompositions exist. Now we show the existence of complete decompositions of order 3 of  $G_2$  by listing down some of them. More examples are displayed in Appendix B4.

Table 5.5: Some Complete Decompositions of Order 3 of  $G_2$

$B_1$	$B_2$	$B_3$
$\left\{ \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \right.$ $\left. \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \right.$ $\left. \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \right\}$	$\left\{ \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \right\}$	$\left\{ \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \right\}$
$\left\{ \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \right.$ $\left. \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \right.$ $\left. \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \right\}$	$\left\{ \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \right\}$	$\left\{ \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \right\}$
$\left\{ \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \right.$ $\left. \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \right.$ $\left. \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \right\}$	$\left\{ \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \right\}$	$\left\{ \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \right\}$

## 5.3 Groups of $2 \times 2$ matrices over $\mathbb{Z}_3$

### 5.3.1 Complete Decompositions of order 2 of $G_3^d$

Let  $G_3^d = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} : a, b \in \mathbb{Z}_3 \right\}$ . In this section, we list down some complete decompositions of order 2 of groups of  $2 \times 2$  matrices over  $\mathbb{Z}_3$ . Table 5.6 shows the complete decompositions of order 2 of  $G_3^d$ . More examples can be found in Appendix B5.

Table 5.6: Some Complete Decompositions of Order 2 of  $G_3^d$ 

$B_1$	$B_2$
$\left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix}, \right. \\ \left. \begin{pmatrix} 0 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \right\}$	$\left\{ \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \right\}$
$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 2 \end{pmatrix}, \right. \\ \left. \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \right\}$	$\left\{ \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, \right. \\ \left. \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\}$
$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix}, \right. \\ \left. \begin{pmatrix} 0 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \right\}$	$\left\{ \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\}$
$\left\{ \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix}, \right. \\ \left. \begin{pmatrix} 0 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \right\}$	$\left\{ \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\}$
$\left\{ \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 2 \end{pmatrix}, \right. \\ \left. \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \right\}$	$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \right. \\ \left. \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}$

### 5.3.2 Complete Decompositions of order 2 of $G_3^t$

Let  $G_3^t = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a, b, c \in \mathbb{Z}_3 \right\}$ . Table 5.7 shows the complete decompositions of order 2 of  $G_3^t$ . More examples can be found in Appendix B6.



### 5.3.3 Complete Decompositions of order 2 of $G_3$

Let  $G_3 = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{Z}_3 \right\}$ . Table 5.8 shows the complete decompositions of order 2 of  $G_3$ . More examples can be found in Appendix B7.

Table 5.8: Some Complete Decompositions of Order 2 of  $G_3$ 

$B_1$	$B_2$
$\left\{ \begin{array}{l} \binom{0}{2} \binom{1}{1}, \binom{0}{1} \binom{1}{2}, \binom{0}{0} \binom{1}{0}, \binom{2}{1} \binom{2}{0}, \binom{0}{2} \binom{2}{1}, \\ \binom{2}{0} \binom{2}{1}, \binom{1}{2} \binom{0}{0}, \binom{0}{0} \binom{0}{2}, \binom{2}{0} \binom{0}{1}, \binom{1}{1} \binom{0}{0}, \\ \binom{0}{1} \binom{2}{2}, \binom{0}{2} \binom{0}{0}, \binom{2}{2} \binom{2}{1}, \binom{1}{0} \binom{1}{1}, \binom{2}{2} \binom{0}{0}, \\ \binom{2}{2} \binom{0}{0}, \binom{0}{2} \binom{0}{0}, \binom{1}{2} \binom{1}{1}, \binom{1}{1} \binom{2}{2}, \binom{2}{2} \binom{0}{0}, \\ \binom{2}{1} \binom{1}{0}, \binom{2}{0} \binom{2}{1}, \binom{1}{1} \binom{2}{2}, \binom{0}{2} \binom{0}{1}, \binom{1}{1} \binom{2}{2}, \\ \binom{1}{2} \binom{2}{1}, \binom{0}{1} \binom{1}{1}, \binom{1}{1} \binom{1}{0}, \binom{0}{0} \binom{0}{0}, \binom{2}{2} \binom{1}{2}, \\ \binom{2}{2} \binom{1}{1}, \binom{1}{0} \binom{0}{0}, \binom{0}{0} \binom{1}{1}, \binom{2}{2} \binom{2}{2}, \binom{0}{2} \binom{0}{2}, \\ \binom{1}{0} \binom{2}{2}, \binom{2}{0} \binom{0}{0}, \binom{0}{2} \binom{1}{1}, \binom{1}{1} \binom{2}{2}, \binom{0}{0} \binom{0}{0}, \\ \binom{0}{0} \binom{1}{1}, \binom{1}{1} \binom{2}{2}, \binom{2}{0} \binom{0}{2}, \binom{0}{0} \binom{0}{0}, \binom{1}{1} \binom{1}{1}, \\ \binom{2}{0} \binom{1}{1}, \binom{1}{0} \binom{2}{2}, \binom{0}{0} \binom{1}{1}, \binom{1}{2} \binom{2}{0}, \binom{0}{1} \binom{1}{0}, \\ \binom{2}{2} \binom{0}{0}, \binom{0}{0} \binom{2}{2}, \binom{2}{2} \binom{2}{1}, \binom{1}{0} \binom{0}{0}, \binom{1}{2} \binom{1}{2}, \\ \binom{0}{0} \binom{1}{1}, \binom{2}{2} \binom{2}{2}, \binom{2}{2} \binom{2}{0}, \binom{1}{0} \binom{1}{1}, \binom{1}{1} \binom{0}{0}, \\ \binom{0}{2} \binom{2}{2}, \binom{1}{2} \binom{2}{2}, \binom{2}{2} \binom{2}{2}, \binom{0}{0} \binom{2}{2}, \binom{0}{0} \binom{0}{2}, \\ \binom{1}{1} \binom{1}{1}, \binom{0}{0} \binom{0}{0}, \binom{2}{2} \binom{0}{0}, \binom{0}{0} \binom{0}{0}, \binom{2}{2} \binom{1}{1}, \\ \binom{1}{0} \binom{0}{2}, \binom{1}{1} \binom{0}{0}, \binom{2}{2} \binom{2}{2}, \binom{1}{0} \binom{1}{1}, \binom{2}{2} \binom{0}{0}, \\ \binom{2}{2} \binom{0}{1}, \binom{0}{0} \binom{0}{0}, \binom{1}{2} \binom{1}{1} \end{array} \right\}$	$\left\{ \binom{1}{1} \binom{2}{1}, \binom{2}{0} \binom{1}{0}, \binom{2}{1} \binom{1}{1} \right\}$
$\left\{ \begin{array}{l} \binom{0}{1} \binom{1}{2}, \binom{0}{0} \binom{1}{0}, \binom{2}{1} \binom{2}{0}, \binom{0}{2} \binom{2}{1}, \binom{2}{0} \binom{2}{2}, \\ \binom{1}{1} \binom{0}{0}, \binom{0}{0} \binom{0}{2}, \binom{2}{2} \binom{0}{0}, \binom{1}{1} \binom{0}{0}, \binom{0}{0} \binom{0}{2}, \\ \binom{0}{2} \binom{0}{0}, \binom{2}{2} \binom{2}{1}, \binom{1}{0} \binom{1}{1}, \binom{2}{0} \binom{2}{0}, \binom{2}{0} \binom{0}{0}, \\ \binom{0}{0} \binom{0}{0}, \binom{1}{1} \binom{1}{1}, \binom{1}{1} \binom{2}{2}, \binom{2}{0} \binom{2}{0}, \binom{2}{1} \binom{1}{0}, \\ \binom{2}{0} \binom{2}{2}, \binom{0}{0} \binom{1}{1}, \binom{0}{2} \binom{0}{1}, \binom{2}{2} \binom{0}{0}, \binom{1}{1} \binom{2}{2}, \\ \binom{0}{1} \binom{1}{1}, \binom{1}{1} \binom{1}{0}, \binom{0}{0} \binom{0}{0}, \binom{2}{1} \binom{2}{1}, \binom{2}{1} \binom{2}{1}, \\ \binom{1}{0} \binom{0}{1}, \binom{0}{0} \binom{0}{1}, \binom{2}{2} \binom{2}{2}, \binom{0}{0} \binom{0}{2}, \binom{1}{0} \binom{1}{0}, \\ \binom{2}{0} \binom{0}{0}, \binom{0}{0} \binom{2}{2}, \binom{1}{1} \binom{1}{1}, \binom{0}{0} \binom{0}{0}, \binom{0}{0} \binom{0}{0}, \\ \binom{1}{0} \binom{0}{2}, \binom{2}{0} \binom{0}{0}, \binom{0}{0} \binom{0}{0}, \binom{1}{1} \binom{1}{1}, \binom{2}{2} \binom{0}{1}, \\ \binom{1}{0} \binom{2}{2}, \binom{0}{0} \binom{0}{0}, \binom{2}{2} \binom{2}{1}, \binom{2}{2} \binom{2}{2}, \binom{0}{0} \binom{0}{0}, \\ \binom{1}{2} \binom{0}{0}, \binom{0}{0} \binom{0}{0}, \binom{1}{1} \binom{2}{2}, \binom{0}{0} \binom{1}{1}, \binom{2}{2} \binom{2}{2}, \\ \binom{0}{0} \binom{0}{0}, \binom{2}{2} \binom{2}{1}, \binom{1}{0} \binom{0}{0}, \binom{1}{1} \binom{2}{2}, \binom{0}{0} \binom{0}{1}, \\ \binom{2}{2} \binom{2}{2}, \binom{2}{2} \binom{2}{0}, \binom{1}{1} \binom{1}{1}, \binom{1}{1} \binom{0}{0}, \binom{0}{0} \binom{0}{2}, \\ \binom{1}{2} \binom{2}{2}, \binom{2}{2} \binom{2}{2}, \binom{0}{0} \binom{0}{2}, \binom{0}{0} \binom{0}{2}, \binom{1}{1} \binom{1}{1}, \\ \binom{0}{0} \binom{0}{0}, \binom{2}{2} \binom{0}{0}, \binom{0}{0} \binom{0}{0}, \binom{2}{2} \binom{1}{1}, \binom{1}{0} \binom{0}{0}, \\ \binom{1}{0} \binom{0}{1}, \binom{2}{2} \binom{2}{2}, \binom{1}{1} \binom{1}{1}, \binom{2}{2} \binom{0}{0}, \binom{2}{2} \binom{0}{0}, \\ \binom{1}{1} \binom{0}{0}, \binom{2}{2} \binom{2}{2}, \binom{1}{1} \binom{1}{1}, \binom{2}{2} \binom{0}{0}, \binom{2}{2} \binom{0}{0}, \\ \binom{0}{0} \binom{0}{0}, \binom{1}{2} \binom{1}{1} \end{array} \right\}$	$\left\{ \binom{1}{1} \binom{2}{1}, \binom{2}{0} \binom{1}{0}, \binom{2}{1} \binom{1}{1}, \binom{0}{2} \binom{1}{1} \right\}$

From the numerical data, we are able to show the existence of complete decompositions of order 2 of  $G_3^d$ , but we can also prove the existence of complete decompositions of order 2 of  $G_n^d$  for  $n \geq 3$ .

**Proposition 4.1** Let  $G_n^d = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} : a, b \in \mathbb{Z}_n \right\}$  for  $n \geq 3$ . There exists a complete decomposition  $(B_1, B_2)$  of  $G_n^d$  of order 2.

*Proof.* Let  $G_n^d = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} : a, b \in \mathbb{Z}_n \right\}$ ,

$$G_n^d = \left\{ \begin{array}{ccccccc} \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, & \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, & \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix}, & \cdots & \begin{pmatrix} n-1 & 0 \\ 0 & 0 \end{pmatrix}, \\ \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, & \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, & \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, & \cdots & \begin{pmatrix} n-1 & 0 \\ 0 & 1 \end{pmatrix}, \\ \vdots & & & & \vdots \\ \begin{pmatrix} 0 & 0 \\ 0 & n-1 \end{pmatrix}, & \begin{pmatrix} 1 & 0 \\ 0 & n-1 \end{pmatrix}, & \begin{pmatrix} 2 & 0 \\ 0 & n-1 \end{pmatrix}, & \cdots & \begin{pmatrix} n-1 & 0 \\ 0 & n-1 \end{pmatrix} \end{array} \right\}$$

Let  $(B_1, B_2)$  be a partition of  $G_n^d$  where  $B_1 = \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \right\}$

and  $B_2 = G_n^d \setminus B_1$ . Let  $B = B_1 + B_2$ . Since  $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in B_1$ , then  $B_2 \subset B$

because  $\left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\} + B_2 = B_2$ . Now we need to show that the elements in

$B_1$  are the sum of elements from  $B_1$  and  $B_2$ :

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} n-2 & 0 \\ 0 & n-1 \end{pmatrix}$$

$\in B_1 \qquad \qquad \in B_2$

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} n-1 & 0 \\ 0 & n-1 \end{pmatrix}$$

$\in B_1 \qquad \qquad \in B_2$

$$\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$\in B_1 \qquad \in B_2$

So  $B_1 \subset B$ . Since  $B_1 \subset B$ ,  $B_2 \subset B$  with  $B_1 \cap B_2 = \emptyset$  and  $B_1 \cup B_2 = G_n^d$ , then  $B = G_n^d$ . Therefore  $(B_1, B_2)$  is a complete decompositions of order 2 of  $G_n^d$  for  $n \geq 2$ .



## CHAPTER 6

### CONCLUSION AND RECOMMENDATIONS

#### 6.1 Conclusion

Over the course of this project we have managed to achieve the objectives and gathered extra numerical data as well. We listed down the exhaustion numbers of all subsets of  $G_n^d$  for  $n = 3, 5$  and  $G_n^t$  for  $n = 2, 3$ . We were also able to generalize some non-exhaustive subsets of a group.

We listed down some complete decompositions of order 3 of  $G_n$  for  $n = 2$ . We were also able to show that complete decompositions of order 2 of  $G_n$  exists for  $n \geq 3$ .

#### 6.2 Recommendations

In Chapter 4, we observed that the sum of the elements in a largest non-exhaustive subset is equal to zero, but we were unable to prove it. We recommend that research is done on this problem.

## REFERENCES

- Baba, S., Kotyada, S. and Teja, R., 2011. 'A non-abelian factorization problem and an associated cryptosystem', *Cryptology, EPrint Archive Report* **2011**, 48.
- Cauchy, A., 1813. 'J. de l'ecole polytechnique', *XVIe Cahier* **9**.
- Chen, H. V. and Chin, A. Y. M., 2017. 'Covering finite groups by subset products', *Ars Combinatoria -Waterloo then Winnipeg-* **131**, 3–9.
- Chen, H. V., Chin, A. Y. M. and Sharmini, S., 2012. 'Exhaustion numbers of 2-subsets of dihedral groups', *World Acad. Sci. Eng. Technol* **62**, 174–175.
- Chen, H. V. and Sin, C. S., 2021a. 'Complete decompositions of dihedral groups and group based key exchange protocol', *Jurnal Kejuruteraan* **33**(3), 733–739.
- Chen, H. V. and Sin, C. S., 2021b. 'On complete decompositions of dihedral groups', *ITM Web of Conferences* **36**, 03001.
- Chin, A. Y. M., 1999. 'Exhaustion numbers of maximal sum-free sets of certain cyclic groups', *MATEMATIKA: Malaysian Journal of Industrial and Applied Mathematics* **15**, 57–63.
- Chin, A. Y. M., 2003. 'Exhaustion numbers of subsets of abelian groups', *Ars Comb.* **68**, 1.
- Chin, A. Y. M. and Chen, H. V., 2018. 'Complete decompositions of finite abelian groups', *Applicable Algebra in Engineering, Communication and Computing* **30**(3), 263–274.
- Cong, Y., Hong, H., Shao, J., Han, S., Lin, J. and Zhao, S., 2019. 'A new secure encryption scheme based on group factorization problem', *IEEE Access* **PP**, 1.
- Davenport, H., 1935. 'On the addition of residue classes', *J. London Math. Soc.* **10**, 160–170.

- Hajós, G., 1938. ‘Covering multidimensional spaces by cube lattices’, *Mat. Fiz. Lapok* **45**, 171–190.
- Hajós, G., 1942. ‘Über einfache und mehrfache bedeckung des  $n$ -dimensionalen raumes mit einem würfelgitter’, *Math. Zeit.* **47**, 427–467.
- Hajós, G., 1949. ‘Sur la factorisation des groupes ab‘eliens’, *Casopis P<sup>˘</sup>es. Mat. Fys.* **74**, 157–162.
- Hamermesh, M., 1989. *Group Theory and Its Application to Physical Problems*, Courier Corporation.
- Herstein, I., 1975. *Topics in Algebra*, Open university set book, Wiley.  
**URL:** <https://books.google.com.my/books?id=-gfvAAAAMAAJ>
- Lal, R., 2017. *Algebra I*, Springer.
- Magliveras, S. S., 2002. ‘Secret and public-key cryptosystems from group factorizations.’, *Journal of Cryptology* **25**, 1–12.
- Miller, G. H., 1964. ‘Evolution of group theory’, *The Mathematics Teacher* **57**(1), 26–30.
- Minkowski, H., 1896. *Geometrie Der Zahlen*, Teubner, Leipzig.
- Prince, E., ed., 1984. *International tables for crystallography.*, D. Reidel Pub. Co., Dordrecht, Holland.
- Sands, A. D., 1962. ‘On the factorisation of finite abelian groups ii’, *Acta Math. Acad. Sci. Hungar.* **13**, 153–169.
- Soklaski, R., 2021. ‘Python’s "itertools"”.  
**URL:** [https://www.pythonlikeyoumeanit.com/Module2\\_EssentialsOfPython/Itertools.html](https://www.pythonlikeyoumeanit.com/Module2_EssentialsOfPython/Itertools.html)
- Szabo, S. and Sands, A. D., 2009. ‘Factoring groups into subsets’, *Lecture Notes in Pure and Applied Mathematics* **257**.  
**URL:** <http://dx.doi.org/10.1201/9781420090475>

Szabó, S., 2006. 'Completing codes and the rédei property of groups', *Theoretical Computer Science* **359**(1), 449–454.

**URL:** <https://www.sciencedirect.com/science/article/pii/S0304397506001277>

Wong, D. C. K., Wong, K. W. and Yap, W.-S., 2018. 'Exhaustion 2-subsets in dihedral groups of order  $2p$ ', *Asian-European Journal of Mathematics* **11**(03), 1850047.

Zhou, Y., 2017. 'Multiple factorizations of cyclic groups', *Discrete Mathematics* **340**(7), 1581–1583.

## Appendix A1: List Of Exhaustion Numbers Of Subsets Of Finite Groups

### Exhaustion Numbers of Subsets of $G_2^d$

Size of subset	Exhaustion number	Number of subsets
2	$\infty$	6 (All)
3	2	4 (All)

### Exhaustion Numbers of Subsets of $G_3^d$

Size of subset	Exhaustion number	Number of subsets
2	$\infty$	36 (All)
3	4	72
	$\infty$	12
4	2	54
	3	72
5	2	126 (All)
6	2	84 (All)
7	2	36 (All)
8	2	9 (All)

### Exhaustion Numbers of Subsets of $G_5^d$

Size of subset	Exhaustion number	Number of subsets
2	$\infty$	300
3	8	2000
	$\infty$	300
4	4	6500
	6	6000
	$\infty$	150
5	3	600
	4	49500
	6	3000
	$\infty$	30
6	3	90500
	4	86000
	5	600
7	3	449500
	4	31200
8	2	13875

	3	1065000
	4	2700
9	2	383875
	3	1658500
	4	600
10	2	1880700
	3	1388000
	4	60
11	2	3874800
	3	582600
12	2	5099100
	3	101200
13	2	5200300
14	2	4457400
15	2	3268760
16	2	2042975
17	2	1081575
18	2	480700
19	2	177100
20	2	53130
21	2	12650
22	2	2300
23	2	300
24	2	25

### Exhaustion Numbers of Subsets of $G_2^t$

Size of subset	Exhaustion number	Number of subsets
2	$\infty$	28 (All)
3	$\infty$	56 (All)
4	3	56
	$\infty$	14
5	2	56 (All)
6	2	28 (All)
7	2	8 (All)

### Exhaustion Numbers of Subsets of $G_3^t$

Size of subset	Exhaustion number	Number of subsets
2	$\infty$	351
3	$\infty$	2925
4	6	12636
	$\infty$	4914
5	3	12636
	4	37908
	5	25272
	$\infty$	4914
6	3	174798
	4	117936
	$\infty$	3276
7	3	802386
	4	84240
	$\infty$	1404
8	2	44226
	3	2141802
	4	33696
	$\infty$	351
9	2	543348
	3	4136184
	4	7254
	$\infty$	39
10	2	3250611
	3	5185674

## Exhaustion Numbers of Subsets of $G_2$

Size of subset	Exhaustion number	Number of subsets
2	$\infty$	120 (All)
3	$\infty$	560 (All)
4	$\infty$	1820 (All)
5	4	2688
	$\infty$	1680
6	2	448
	3	6720
	$\infty$	840
7	2	4480
	3	6720
	$\infty$	240
8	2	10080
	3	2760
	$\infty$	30
9	2	11440 (All)
10	2	8008 (All)
11	2	4368 (All)
12	2	1820 (All)
13	2	560 (All)
14	2	120 (All)
15	2	16 (All)



## Appendix A2: All Largest Non-Exhaustive Subsets of $G_2^t$

---

---

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \right\}$$

---

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \right\}$$

---

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\}$$

---

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\}$$

---

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \right\}$$

---

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \right\}$$

---

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \right\}$$

---

$$\left\{ \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \right\}$$

---

$$\left\{ \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \right\}$$

---

$$\left\{ \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\}$$

---

$$\left\{ \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \right\}$$

---

$$\left\{ \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \right\}$$

---

$$\left\{ \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\}$$

---

$$\left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \right\}$$









$$\left\{ \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 2 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 0 & 2 \\ 0 & 2 \end{pmatrix} \right\}$$

























	$B_1$	$B_2$
7	$\left\{ \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 2 \end{pmatrix}, \right.$ $\left. \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \right\}$	$\left\{ \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}$
8	$\left\{ \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 2 \end{pmatrix}, \right.$ $\left. \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \right\}$	$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}$
9	$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 2 \end{pmatrix}, \right.$ $\left. \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \right\}$	$\left\{ \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}$
10	$\left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, \right.$ $\left. \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \right\}$	$\left\{ \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}$







$B_1$  $B_2$ 

$$\begin{aligned} & \begin{pmatrix} 2 & 2 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 2 \\ 0 & 0 \end{pmatrix}, \\ & \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix}, \\ & \begin{pmatrix} 2 & 2 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 0 & 0 \end{pmatrix}, \\ & \left. \begin{pmatrix} 0 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 0 & 2 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\} \end{aligned}$$

# Appendix B7: Some Complete decompositions of order 2 of $G_3$

	$B_1$	$B_2$
1	$\left\{ \begin{array}{l} \binom{0}{0} \binom{1}{2}, \binom{0}{0} \binom{1}{1}, \binom{0}{0} \binom{1}{0}, \binom{2}{0} \binom{2}{1}, \\ \binom{0}{0} \binom{2}{2}, \binom{2}{0} \binom{2}{0}, \binom{1}{0} \binom{0}{2}, \binom{0}{0} \binom{0}{2}, \\ \binom{2}{0} \binom{0}{0}, \binom{1}{0} \binom{0}{1}, \binom{0}{0} \binom{0}{2}, \binom{0}{0} \binom{0}{0}, \\ \binom{2}{0} \binom{2}{2}, \binom{1}{0} \binom{1}{1}, \binom{2}{0} \binom{0}{1}, \binom{2}{0} \binom{0}{2}, \\ \binom{0}{0} \binom{0}{2}, \binom{0}{0} \binom{0}{0}, \binom{0}{0} \binom{0}{1}, \binom{0}{0} \binom{0}{2}, \\ \binom{0}{0} \binom{0}{0}, \binom{1}{0} \binom{1}{1}, \binom{1}{0} \binom{1}{2}, \binom{2}{0} \binom{0}{0}, \\ \binom{0}{0} \binom{0}{2}, \binom{0}{0} \binom{0}{2}, \binom{0}{0} \binom{0}{1}, \binom{0}{0} \binom{0}{2}, \\ \binom{2}{0} \binom{1}{1}, \binom{2}{0} \binom{2}{1}, \binom{1}{0} \binom{1}{2}, \binom{0}{0} \binom{0}{1}, \\ \binom{0}{0} \binom{0}{1}, \binom{0}{0} \binom{0}{2}, \binom{0}{0} \binom{0}{1}, \binom{1}{0} \binom{1}{1}, \\ \binom{0}{0} \binom{0}{0}, \binom{2}{0} \binom{2}{1}, \binom{2}{0} \binom{2}{1}, \binom{1}{0} \binom{1}{0}, \\ \binom{0}{0} \binom{0}{0}, \binom{0}{0} \binom{0}{1}, \binom{0}{0} \binom{0}{2}, \binom{0}{0} \binom{0}{0}, \\ \binom{0}{0} \binom{0}{1}, \binom{2}{0} \binom{2}{2}, \binom{0}{0} \binom{0}{2}, \binom{1}{0} \binom{1}{0}, \\ \binom{0}{0} \binom{0}{0}, \binom{0}{0} \binom{0}{1}, \binom{0}{0} \binom{0}{2}, \binom{0}{0} \binom{0}{2}, \\ \binom{2}{0} \binom{0}{0}, \binom{0}{0} \binom{0}{2}, \binom{1}{0} \binom{1}{1}, \binom{0}{0} \binom{0}{0}, \\ \binom{0}{0} \binom{0}{1}, \binom{0}{0} \binom{0}{1}, \binom{0}{0} \binom{0}{0}, \binom{0}{0} \binom{0}{2}, \\ \binom{1}{0} \binom{1}{1}, \binom{2}{0} \binom{2}{1}, \binom{1}{0} \binom{1}{2}, \binom{0}{0} \binom{0}{1}, \\ \binom{0}{0} \binom{0}{2}, \binom{0}{0} \binom{0}{0}, \binom{0}{0} \binom{0}{0}, \binom{0}{0} \binom{0}{2}, \\ \binom{1}{0} \binom{1}{2}, \binom{0}{0} \binom{0}{1}, \binom{2}{0} \binom{2}{2}, \binom{0}{0} \binom{0}{2}, \\ \binom{0}{0} \binom{0}{2}, \binom{0}{0} \binom{0}{1}, \binom{0}{0} \binom{0}{0}, \binom{0}{0} \binom{0}{0}, \\ \binom{2}{0} \binom{2}{1}, \binom{1}{0} \binom{1}{0}, \binom{1}{0} \binom{1}{2}, \binom{0}{0} \binom{0}{1}, \\ \binom{0}{0} \binom{0}{2}, \binom{0}{0} \binom{0}{0}, \binom{0}{0} \binom{0}{0}, \binom{0}{0} \binom{0}{0}, \\ \binom{2}{0} \binom{2}{2}, \binom{2}{0} \binom{2}{2}, \binom{1}{0} \binom{1}{1}, \binom{1}{0} \binom{1}{0}, \\ \binom{0}{0} \binom{0}{1}, \binom{0}{0} \binom{0}{2}, \binom{0}{0} \binom{0}{0}, \binom{0}{0} \binom{0}{2}, \\ \binom{0}{0} \binom{0}{2}, \binom{1}{0} \binom{1}{2}, \binom{2}{0} \binom{2}{2}, \binom{0}{0} \binom{0}{2}, \\ \binom{0}{0} \binom{0}{2}, \binom{0}{0} \binom{0}{2}, \binom{0}{0} \binom{0}{0}, \binom{0}{0} \binom{0}{1}, \\ \binom{0}{0} \binom{0}{2}, \binom{1}{0} \binom{1}{1}, \binom{0}{0} \binom{0}{0}, \binom{2}{0} \binom{2}{0}, \\ \binom{0}{0} \binom{0}{0}, \binom{0}{0} \binom{0}{1}, \binom{0}{0} \binom{0}{0}, \binom{0}{0} \binom{0}{1}, \\ \binom{0}{0} \binom{0}{0}, \binom{2}{0} \binom{2}{1}, \binom{1}{0} \binom{1}{0}, \binom{1}{0} \binom{1}{0}, \\ \binom{0}{0} \binom{0}{1}, \binom{0}{0} \binom{0}{2}, \binom{0}{0} \binom{0}{0}, \binom{0}{0} \binom{0}{1} \end{array} \right\}$	$\left\{ \binom{1}{0} \binom{2}{1}, \binom{2}{0} \binom{1}{0}, \binom{2}{0} \binom{1}{1} \right\}$











$B_1$  $B_2$ 

$$\left\{ \begin{array}{l} \binom{0}{0} \binom{2}{2}, \binom{1}{0} \binom{0}{2}, \binom{2}{0} \binom{0}{0}, \binom{0}{0} \binom{0}{2}, \\ \binom{1}{0} \binom{1}{1}, \binom{0}{0} \binom{0}{0}, \binom{0}{0} \binom{0}{0}, \binom{0}{1} \binom{1}{0}, \\ \binom{0}{2} \binom{0}{1}, \binom{0}{0} \binom{0}{0}, \binom{0}{1} \binom{0}{1}, \binom{0}{1} \binom{0}{1}, \\ \binom{2}{0} \binom{0}{0}, \binom{0}{0} \binom{0}{2}, \binom{0}{2} \binom{0}{2}, \binom{2}{1} \binom{0}{0}, \\ \binom{1}{1} \binom{2}{2}, \binom{0}{0} \binom{0}{1}, \binom{1}{1} \binom{2}{2}, \binom{0}{1} \binom{0}{1}, \\ \binom{0}{0} \binom{0}{0}, \binom{0}{2} \binom{0}{2}, \binom{0}{2} \binom{0}{2}, \binom{0}{1} \binom{0}{1}, \\ \binom{2}{2} \binom{0}{2}, \binom{0}{0} \binom{0}{2}, \binom{2}{1} \binom{1}{0}, \binom{1}{0} \binom{0}{0}, \\ \binom{0}{0} \binom{0}{0}, \binom{0}{0} \binom{0}{0}, \binom{0}{2} \binom{0}{2}, \binom{2}{2} \binom{2}{2}, \\ \binom{1}{1} \binom{1}{1}, \binom{1}{0} \binom{0}{0}, \binom{0}{2} \binom{0}{2}, \binom{1}{2} \binom{0}{2}, \\ \binom{0}{0} \binom{0}{0}, \binom{0}{2} \binom{0}{2}, \binom{0}{2} \binom{0}{2}, \binom{0}{2} \binom{0}{2}, \\ \binom{2}{2} \binom{0}{0}, \binom{0}{0} \binom{0}{1}, \binom{0}{0} \binom{0}{0}, \binom{1}{1} \binom{0}{1}, \\ \binom{0}{0} \binom{0}{0}, \binom{2}{0} \binom{0}{1}, \binom{0}{0} \binom{0}{0}, \binom{2}{1} \binom{0}{1}, \\ \binom{0}{0} \binom{0}{0}, \binom{0}{1} \binom{0}{1}, \binom{0}{1} \binom{0}{2}, \binom{0}{2} \binom{0}{2}, \\ \binom{1}{0} \binom{1}{0}, \binom{1}{0} \binom{0}{1}, \binom{2}{2} \binom{1}{1}, \binom{1}{1} \binom{1}{1}, \\ \binom{0}{0} \binom{0}{0}, \binom{0}{1} \binom{0}{2}, \binom{0}{2} \binom{0}{0}, \binom{0}{0} \binom{0}{0}, \\ \binom{2}{0} \binom{0}{1}, \binom{2}{0} \binom{0}{2}, \binom{0}{0} \binom{0}{1}, \binom{1}{1} \binom{0}{2} \end{array} \right\}$$

7

$$\left\{ \begin{array}{l} \binom{1}{0} \binom{2}{1}, \binom{0}{0} \binom{0}{1}, \binom{2}{0} \binom{2}{1}, \binom{0}{0} \binom{0}{2}, \\ \binom{2}{0} \binom{2}{2}, \binom{1}{0} \binom{0}{2}, \binom{0}{0} \binom{0}{0}, \binom{2}{0} \binom{0}{0}, \\ \binom{1}{0} \binom{1}{0}, \binom{0}{0} \binom{0}{2}, \binom{0}{0} \binom{0}{0}, \binom{2}{2} \binom{2}{2}, \\ \binom{0}{0} \binom{0}{1}, \binom{0}{0} \binom{0}{1}, \binom{0}{0} \binom{0}{2}, \binom{0}{0} \binom{0}{2}, \\ \binom{1}{0} \binom{1}{1}, \binom{2}{0} \binom{0}{0}, \binom{2}{0} \binom{0}{0}, \binom{0}{0} \binom{0}{0}, \\ \binom{0}{0} \binom{0}{0}, \binom{0}{0} \binom{0}{1}, \binom{0}{0} \binom{0}{2}, \binom{0}{0} \binom{0}{2}, \\ \binom{1}{0} \binom{1}{1}, \binom{1}{2} \binom{0}{1}, \binom{2}{0} \binom{2}{0}, \binom{2}{1} \binom{2}{1}, \\ \binom{0}{2} \binom{0}{1}, \binom{0}{1} \binom{0}{1}, \binom{0}{2} \binom{0}{2}, \binom{0}{1} \binom{0}{1}, \\ \binom{2}{1} \binom{0}{0}, \binom{1}{2} \binom{0}{0}, \binom{0}{1} \binom{0}{2}, \binom{1}{2} \binom{0}{1}, \\ \binom{0}{0} \binom{0}{0}, \binom{0}{0} \binom{0}{0}, \binom{0}{2} \binom{0}{2}, \binom{0}{1} \binom{0}{1}, \\ \binom{1}{2} \binom{0}{0}, \binom{0}{1} \binom{0}{1}, \binom{1}{1} \binom{0}{0}, \binom{0}{0} \binom{0}{0}, \\ \binom{2}{1} \binom{0}{1}, \binom{2}{1} \binom{0}{1}, \binom{1}{0} \binom{0}{0}, \binom{0}{0} \binom{0}{1}, \\ \binom{0}{1} \binom{0}{1}, \binom{0}{2} \binom{0}{2}, \binom{0}{0} \binom{0}{0}, \binom{0}{0} \binom{0}{0}, \\ \binom{0}{2} \binom{0}{2}, \binom{1}{1} \binom{1}{1}, \binom{0}{0} \binom{0}{0}, \binom{0}{0} \binom{0}{0}, \\ \binom{0}{1} \binom{0}{1}, \binom{0}{1} \binom{0}{1}, \binom{0}{0} \binom{0}{0}, \binom{0}{1} \binom{0}{1}, \\ \binom{1}{0} \binom{1}{0}, \binom{2}{0} \binom{0}{0}, \binom{0}{0} \binom{0}{0}, \binom{1}{1} \binom{1}{1}, \\ \binom{0}{0} \binom{0}{1}, \binom{0}{0} \binom{0}{0}, \binom{0}{2} \binom{0}{2}, \binom{0}{2} \binom{0}{2}, \\ \binom{2}{1} \binom{1}{2}, \binom{0}{0} \binom{1}{2}, \binom{0}{1} \binom{1}{2}, \binom{0}{2} \binom{0}{2} \end{array} \right\}$$







$B_1$

$B_2$