

**MAT301**

*Groups and Symmetries*

SINAN LI

2024



---

# CONTENTS

I	Notes	5
---	-------	---

## 1 | Chapter 1

Introduction

1.1	Course Information	7
1.1.1	Communication	7
1.1.2	Evaluation Criteria	8
1.2	Important Dates	8
1.3	Course Description	8

## 2 | Chapter 2

Introduction to Symmetry

2.1	Intuition and Motivation	9
2.2	Symmetric Group	11

## 3 | Chapter 3

Introduction to Group

3.1	Introduction	17
3.2	Subgroups	23

## 4 | Chapter 4

Cyclic Groups

4.1	Introduction	27
-----	--------------	----

# 5

## Chapter 5 Isomorphic Theorems

5.1	Normal Subgroups	33
5.2	The First Two Isomorphism Theorem	34

II Appendices	37
Bibliography	39
Index	41

Part I

Notes



## CHAPTER

# INTRODUCTION

# 1

### 1.1

### Course Information

- **Instructor:** Malors Emilio Espinosa Lara
- **Office:** BA 6256
- **Email:** [srolam.espinosalara@mail.utoronto.ca](mailto:srolam.espinosalara@mail.utoronto.ca)
- **TA:** Shuofeng Xu, Mohammad Honari and Mohammadmahdi Rafiei
- **Office Hours**

LEC101, LEC2001	Tuesday 9 - 11 (PB B250)	Thursday 10 - 11 (MP 202)
Instructor Office Hours	Monday 12 - 1	BA6256 (My office)

- There are **no tutorials** for this course.

#### 1.1.1 Communication

All communication will occur by U of T email. Feel free to contact the instructor via email to ask extra questions and doubts, corrections about homeworks, inquiries, etc. However, the following titles must be used in the subject of the email:

- **MAT301: Mark Correction.** Put this title whenever you feel a correction is needed in one of your homeworks or midterm.

- **MAT301: Math Doubt.** If you have a mathematical doubt.
- **MATH301: Administrative Issue.** If you have any other concern that doesn't fall into the previous categories.

### 1.1.2 Evaluation Criteria

We will follow the following grading scheme for this course.

10 Homeworks (drop the lowest scored one of the first five and of the last five)	25%
Midterm	25%
Final Examination	50%

Notice that **late homework submission are usually given mark zero**. Exceptions due to required accommodations or unexpected circumstances will be of course taken into account and discussed in a case by case basis. Please write to the instructor in these situations.

Any grade curve that might occur will only be done over the final course mark and not for particular homework, midterm or final test.

### 1.2 Important Dates

The following are some of the dates relevant, and with respect, to MAT301:

First day of classes of University	Monday, January 8
First Lecture	Tuesday, January 9
Family Day	February 19 (University Closed)
Winter Reading Week(No lectures, nor Office hours)	February 19 to 23
Our Course Midterm	February 26, 19:00 - 21:00 (Venues TBA)
Good Friday	March 29 (University Closed)
Last day of classes	April 5
Study Day	April 9
Final Exam Period	April 10 - 30

### 1.3 Course Description

This course covers Groups oriented to computations. In order to understand groups well, a solid background in *linear algebra* is required: matrices, determinants, eigenvalues, eigenvectors, etc. *Modular arithmetic* is also required, as well as some basic notions of *number theory*.

## CHAPTER

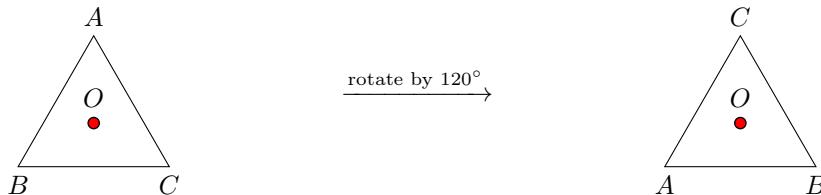
# INTRODUCTION TO SYMMETRY

# 2

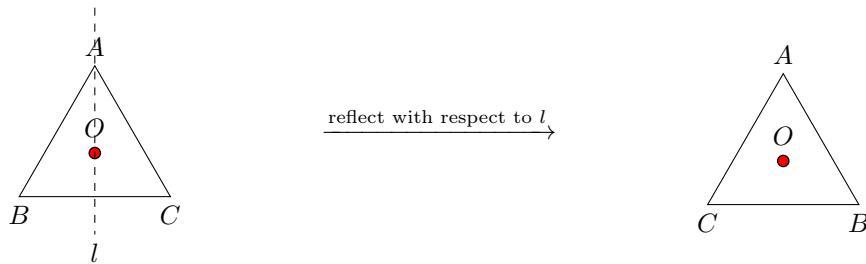
### 2.1 Intuition and Motivation

The idea of symmetry is the object has a property that remains invariant under a transformation. For example, if we rotate a square by 90 degrees, the square remains the same. However, symmetry is more than a geometric concept. It is a fundamental concept in mathematics and physics.

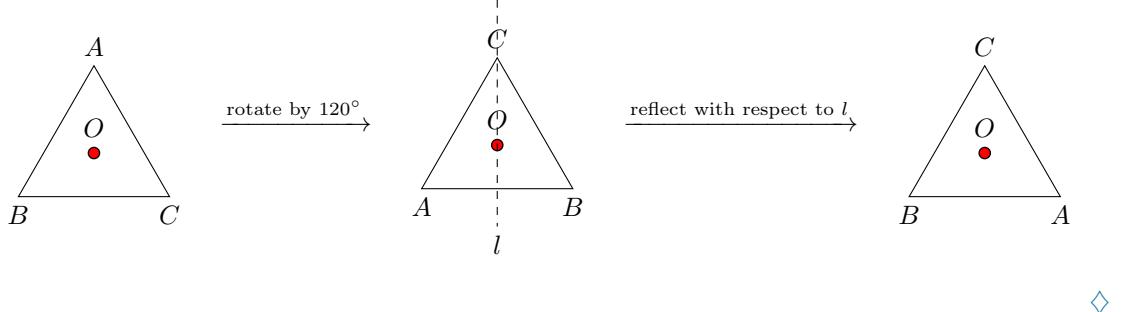
**Example (Polygons).** We can rotate the following triangle with respect to  $O$  by  $120^\circ$ , and the triangle remains the same. This triangle has rotational symmetry.



Moreover, we can also reflect the triangle with respect to the line  $l$  passing through  $O$ , and the triangle remains the same. This triangle has reflection symmetry.

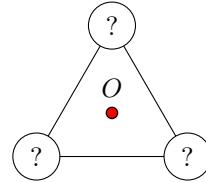


Is there any other symmetry? Yes, we can combine the two symmetries above. We first rotate the triangle by  $120^\circ$ , and then reflect it with respect to  $l$ . This triangle has both rotational and reflection symmetry.



◇

The above example is a very simple one. However, given a general object, it is not easy to find all its symmetries. We can label the vertices of the triangle with  $A, B, C$ , then permute the labels.



Since the transformations are linear, they preserve linearity. This, it suffices to consider the transformations of the vertices.

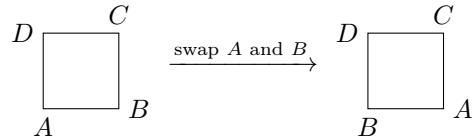
**Example (Continued).** The following table shows all the permutations of the vertices of the triangle.

Identity	$A$	$B$	$C$
Rotation	$C$	$A$	$B$
Reflection	$A$	$C$	$B$
Rotation + Reflection	$C$	$B$	$A$
	$B$	$A$	$C$
	$B$	$C$	$A$

As we can see, there are six transformations of the vertices, each of which corresponds to a symmetry of the triangle.

◇

Naively, given a square, one would argue that there are 24 ways to permute the vertices, and thus 24 symmetries. However, this is not true. There are certain permutations that are not symmetries.



## 2.2

# Symmetric Group

### Definition 2.2.1 Symmetric Group

The **symmetric group**, denoted  $S_n$ , is the set of all permutations of  $n$  elements  $1, 2, \dots, n$ .

### Definition 2.2.2 Identity Permutation

The **identity permutation** is the permutation that does not change the order of the elements.

**Example.** The identity permutation of  $S_3$  is the identity permutation of  $1, 2, 3$ . ◊

### Definition 2.2.3 Transposition

A **transposition** is a permutation that swaps two elements and leaves the other elements unchanged.

**Example.** The following are some transpositions of  $S_3$ .

- $2, 1, 3$  swaps 1 and 2.
- $1, 3, 2$  swaps 2 and 3.
- $3, 2, 1$  swaps 1 and 3.



### Definition 2.2.4 Cycle

A **cycle** is a permutation that moves the first element to the second, the second to the third, and so on, and the last element to the first.

**Example.** The cycle  $3, 2, 1$  moves 1 to 3, 3 to 2, and 2 to 1. ◊

### Definition 2.2.5 Permutation

A permutation is a way to order  $n$  elements. We codify them in “cycles”

**Example.** Consider  $S_3$ .

$$\begin{array}{cccccc} 1 & 2 & 3 & 1 & 2 & 3 \\ \hline 1 & 2 & 3 & 1 & 3 & 2 & 3 & 2 & 1 & 2 & 1 & 3 \\ (1)(2)(3) & (1)(23) & (13)(2) & (12)(3) & (132) & (123) \end{array}$$

Here,  $(1)(23)$  means

- 1 goes to 1.

- 2 goes to 3, and 3 goes to 2.



**Example.** Consider the following permutation.

$$\begin{array}{r|l} \begin{array}{ccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ \hline 3 & 4 & 2 & 1 & 7 & 5 & 6 \end{array} & \begin{array}{ccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ \hline 2 & 3 & 1 & 4 & 6 & 5 & 7 \end{array} \\ \begin{array}{c} (1324)(576) \end{array} & \begin{array}{c} (1\ 2\ 3)(5\ 6) \end{array} \end{array}$$



**Example.** Suppose you have two permutations  $\sigma$  and  $\tau$ :

- $\sigma = (12)(3456)$
- $\tau = (1654)(32)$

What happens if we perform one after the other?

- $\sigma$  first,  $\tau$  second<sup>1</sup>:  $(1654)(32)(12)(3456) = (1654)(32)(12)(3456)$ 
  - We start with 1:  $1 \rightarrow 2 \rightarrow 3$ , so  $1 \rightarrow 3$ .
  - We then consider 3:  $3 \rightarrow 4 \rightarrow 1$ , so  $3 \rightarrow 1$ .
  - Now, we consider 2:  $2 \rightarrow 1 \rightarrow 6$ , so  $2 \rightarrow 6$ .
  - $6 \rightarrow 3 \rightarrow 2$ , so  $6 \rightarrow 2$ .
  - $4 \rightarrow 5 \rightarrow 4$ , so  $4 \rightarrow 4$ .
  - $5 \rightarrow 6 \rightarrow 5$ , so  $5 \rightarrow 5$ .

Thus, we get

$$(13)(26)(4)(5).$$

- $\tau$  first,  $\sigma$  second:  $(12)(3456)(1654)(32) = (12)(3456)(1654)(32)$ 
  - We start with 1:  $1 \rightarrow 6 \rightarrow 4$ , so  $1 \rightarrow 3$ .
  - We then consider 3:  $4 \rightarrow 5 \rightarrow 1$ , so  $4 \rightarrow 1$ .
  - ...

Eventually, we get

$$(13)(24)(5)(6).$$

It is important to note that the order of the permutations matters.



The above example demonstrates an important property of permutations: closed under composition. That is, if we “merge” two permutations, we get another permutation.

---

<sup>1</sup>Note that we read from right to left.

$\circ$	$1$	$(12)$	$(13)$	$(23)$	$(123)$	$(132)$
$1$						
$(12)$						
$(13)$						
$(23)$	$(23)$	$(132)$	$(123)$	$1$	$(13)$	$(12)$
$(123)$						
$(132)$						

This is a multiplication table of  $S_3$ . Symmetries of the same group have the same multiplication table, despite the fact that they are different permutations.

### Remark

Note that in the above table of  $S_3$ , we have  $(123) = (23)(13)$ , and  $(132) = (23)(12)$ . **All the permutations can be written as a composition of transpositions.**

It is important to note that this is not unique. For example, we can write  $1 = (12)(12)$ .

### Theorem 2.2.1

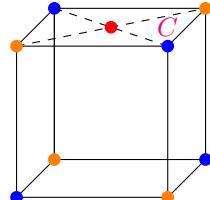
The amount of transpositions needed to create a permutation preserves its parity.

In other words, if a permutation  $\alpha$  can be expressed as a product of transpositions

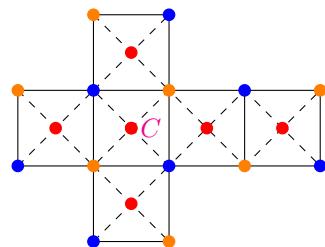
$$\alpha = \tau_1 \tau_2 \dots \tau_n \quad \text{and} \quad \alpha = \sigma_1 \sigma_2 \dots \sigma_m$$

where  $\tau$  and  $\sigma$  are transpositions, then  $n$  and  $m$  have the same parity (both even or both odd). The smaller groups are called **alternating groups**.

**Example.** Consider the following figure of a cube.



which expands to the following graph.



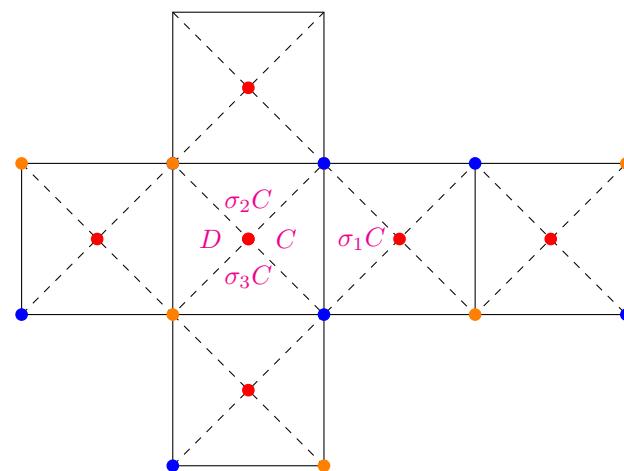
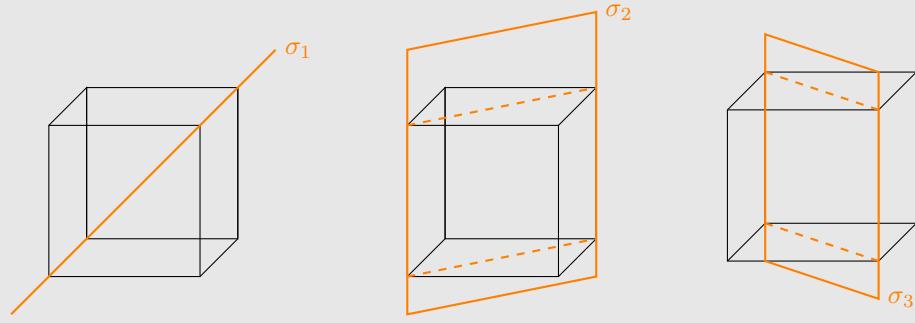
**Question:** What are the isometries that preserve the colouring of this object?

### Definition 2.2.6 Isometry

An **isometry** is a transformation that preserves distance.

### Remark

Consider reflection with respect to the planes  $\sigma_1$ ,  $\sigma_2$ , and  $\sigma_3$ .



$D$  can be obtained by either  $\sigma_3\sigma_2C$  or  $\sigma_2\sigma_3C$ .

$$\begin{array}{ccc} \mathbb{R}^3 & \xrightarrow{\sigma_3} & \mathbb{R}^3 & \xrightarrow{\sigma_2} & \mathbb{R}^3 \\ & & \sigma_3 & & \sigma_2 \\ & & \sigma_2 & & \sigma_3 \end{array}$$

Matrices are not commute, and thus these transformations may be different. We ask the questions: since  $\sigma_2\sigma_1$  and  $\sigma_1\sigma_2$  move the triangle  $C$  in the same way, are they the same map?

### Proposition 2.2.1

If  $S, T : \mathbb{R}^3 \rightarrow \mathbb{R}^3$  preserve the coloured ube and send the triangle to the same place, then  $S = T$  (as maps).

*Proof.* WTS  $S = T$ .

#### Remark

It is important that the triangle  $C$  is a field of vectors.

Consider  $o = (0, 0, \frac{1}{2})$ ,  $b = (\frac{1}{2}, \frac{1}{2}, \frac{1}{2})$ , and  $y = (-\frac{1}{2}, -\frac{1}{2}, \frac{1}{2})$ .

$Sb = Tb, So = To, Sy = Ty \implies (S - T)b = 0, (S - T)o = 0, (S - T)y = 0$ .

This implies  $b, o$ , and  $y$  are in the kernel of  $S - T$ .

Moreover,  $b, o, y$  are linearly independent since  $\det \begin{bmatrix} \frac{1}{2} & 0 & -\frac{1}{2} \\ \frac{1}{2} & 0 & -\frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \end{bmatrix} \neq 0$ .

Thus,  $\dim \ker((S - T)) = 3$ . Since  $\dim \mathbb{R}^3 = 3$ ,  $\ker((S - T)) = \mathbb{R}^3$ . Thus,  $S - T = 0$ . ■

We can reach all 24 locations of the triangle  $C$  by applying  $\sigma_1, \sigma_2$ , and  $\sigma_3$  to the triangle  $C$ . Thus, there are 24 isometries that preserve the coloured cube. Moreover, we know that 3 of them generates the set. It suffices to study these three isometries to understand the whole group. ◇



# INTRODUCTION TO GROUP 3

## 3.1

## Introduction

### Remark

What have we done so far: we have studied some **objects** with some properties, and we have asked how can we operate in this object and preserve its property.

### Definition 3.1.1 Group

A **group** is a pair  $(G, \cdot)$  where  $G$  is a set and  $\cdot$  is a binary operation on  $G$  such that

$$\begin{array}{rccc} \cdot & G \times G & \rightarrow & G \\ & (a, b) & \mapsto & a \cdot b \end{array}$$

such that

- **Identity:** There exists an element  $e \in G$  such that

$$e \cdot g = g \cdot e = a \quad \forall a \in G.$$

- **Inverse:** For every  $g \in G$  there exists an element  $h \in G$  such that

$$g \cdot h = h \cdot g = e.$$

- **Associativity:** For every  $g, h, k \in G$  we have

$$g \cdot (h \cdot k) = (g \cdot h) \cdot k.$$

### Definition 3.1.2 Abelian Group

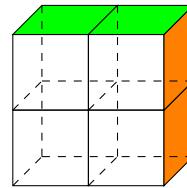
A group  $(G, \cdot)$  is called **abelian** if

$$g \cdot h = h \cdot g \quad \forall g, h \in G.$$

This group is also called a **commutative group**.

The term *abelian* comes from the name of the Norwegian mathematician [Niels Henrik Abel](#). He was the first to prove the impossibility of solving the general quintic equation in radicals. He also made important contributions to the study of elliptic functions, discovered Abelian functions, and many other important fields in mathematics.

**Example.** We will consider the following “toy”



The left side is red, the bottom is blue, and the back is yellow.

We have 7 operations

$$V_1, V_2, H_1, H_2, V, H, R$$

where

- $V_1$  is the vertical flip of the first column
- $V_2$  is the vertical flip of the second column
- $H_1$  is the horizontal flip of the first row
- $H_2$  is the horizontal flip of the second row
- $V$  is the vertical flip of the whole cube
- $H$  is the horizontal flip of the whole cube
- $R$  is the rotation of the cube by  $90^\circ$  around the vertical axis

They satisfy

$$V_1^2 = 1, V_2^2 = 1, H_1^2 = 1, H_2^2 = 1, V^2 = 1, H^2 = 1, R^4 = 1,$$

However, we have redundancies:

- $V_1 V_2 = V_2 V_1 = V$
- $H_1 H_2 = H_2 H_1 = H$
- $V_1 H_1 = H_1 V_1 = R$

- $H_2 H_1 V_2 V_1 = R^2$
- $R^3 V_1 R = R^{-1} V_1 R = H_1$
- ...

We can flatten the cube into

$$\begin{array}{c|c} 1 & 2 \\ \hline 3 & 4 \end{array}$$

Then,

- $V_1 = (1, 4)$

$$\begin{array}{c|c} 1 & 2 \\ \hline 4 & 3 \end{array} \xrightarrow{V_1} \begin{array}{c|c} 4 & 2 \\ \hline 1 & 3 \end{array}$$

- $V_2 = (2, 3)$

$$\begin{array}{c|c} 1 & 2 \\ \hline 4 & 3 \end{array} \xrightarrow{V_2} \begin{array}{c|c} 1 & 3 \\ \hline 4 & 2 \end{array}$$

- $H_1 = (1, 2)$

$$\begin{array}{c|c} 1 & 2 \\ \hline 4 & 3 \end{array} \xrightarrow{H_1} \begin{array}{c|c} 4 & 3 \\ \hline 1 & 2 \end{array}$$

- $H_2 = (3, 4)$

$$\begin{array}{c|c} 1 & 2 \\ \hline 4 & 3 \end{array} \xrightarrow{H_2} \begin{array}{c|c} 1 & 2 \\ \hline 3 & 4 \end{array}$$

- $R = (1, 2, 3, 4)$

$$\begin{array}{c|c} 1 & 2 \\ \hline 4 & 3 \end{array} \xrightarrow{R} \begin{array}{c|c} 4 & 1 \\ \hline 3 & 2 \end{array}$$

We can verify that

$$(1, 2, 3, 4) = (3, 4)(1, 4)(1, 2),$$

which proposes that

$$R = H_2 \circ V_1 \circ H_1$$

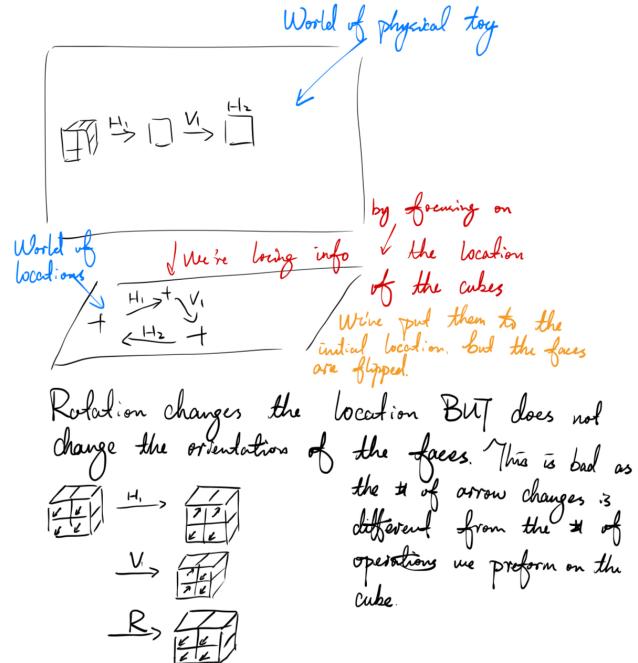


We have a group that is the one generator by the operations of the ‘toy’ above. We have two models to understand the group:

- 1 The complete toy

## 2 The location code

What we have seen is that these two models are codify information in different ways. We can generate a map of the potential positions.

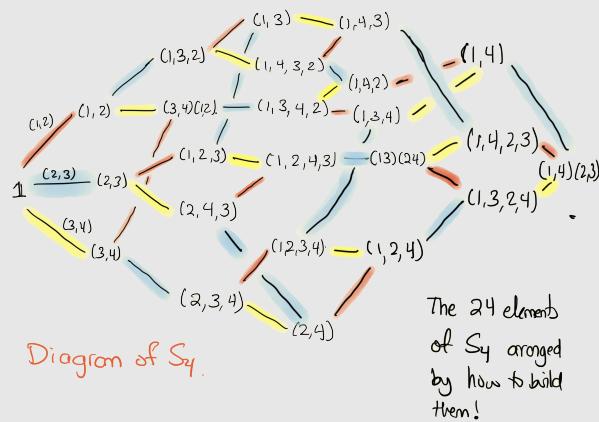


If we only allow  $H_1, V_1, H_2, V_2$ , then the locations are believable. The group they generate is  $S_4$ .

### Remark

Think of  $S_4$  independently.

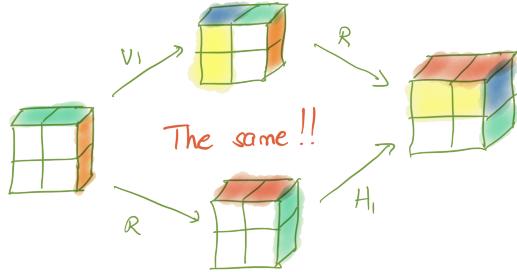
We consider the permutations independently as a group.



We want to merge  $R$  with the rest of the operations.

Consider

$$H_1R = RV_1 \quad H_2R = RV_2$$



**Example.** “Simplify” the instructions

$$RV_1H_2RV_2H_1H_2RV_1H_2$$

Using the two equations above,

$$\begin{aligned} RV_1H_2RV_2H_1H_2RV_1H_2 &= RV_1H_2RV_2H_1\cancel{RV_2}V_1H_2 \\ &= RV_1H_2RV_2\cancel{RV_1}V_2V_1H_2 \\ &= RV_1H_2R\cancel{RH_2}V_1V_2V_1H_2 \\ &= RV_1H_2\cancel{V_1V_2H_1H_2}H_2V_1V_2V_1H_2 \quad (RR = V_1V_2H_1H_2) \end{aligned}$$

This way, we have moved all the “noise”,  $R$ , to the last steps. ◇

**Fact:** All elements of the group can be written as

$$X\sigma$$

where  $X = 1$  or  $R$  and  $\sigma \in S_4$ .

### Proposition 3.1.1

This writing is **unique**.

*Proof.* Suppose  $X_1\sigma_1 = X_2\sigma_2$ .

- If  $X_1 = X_2 = 1$ , then  $\sigma_1 = \sigma_2$ .
- If  $X_1 = X_2 = R$ , then  $R\sigma_1 = R\sigma_2$ .

Multiplying by  $R^{-1}$ , we have

$$R^{-1}R\sigma_1 = R^{-1}R\sigma_2$$

$$\sigma_1 = \sigma_2$$

- $X_1 = 1, X_2 = R$ . Then,

$$\begin{aligned}\sigma_1 &= R\sigma_2 \\ \sigma_1\sigma_2^{-1} &= R\sigma_2\sigma_2^{-1} \\ \sigma_1\sigma_2^{-1} &= R\end{aligned}$$

which means  $R \in S_4$ , which is impossible. ■

These decomposition also has coordinates.  $X$  uses the  $R$ -coordinate and  $\sigma$  uses the  $S_4$ -coordinate. We can write this as

$$(1, \sigma) \in \pm 1 \times S_4$$

However, note that  $(s_1, \sigma_1)(s_2, \sigma_2) = (s_1s_2, \sigma_1\sigma_2)$  is **not true**. The reason is because there is “noise” (procued by  $R$ ) in the first coordinate.

With this the multiplication table looks like

		$(1, \sigma)$	$(-1, \sigma)$
$(1, \sigma)$	$(1, \sigma)$	$(1, \sigma_1) \cdot (-1, \sigma_2)$ " " $(-1, \underline{F(\sigma_1)} \sigma_2)$	
$(-1, \sigma)$	$(-1, \sigma_1) \cdot (1, \sigma_2)$ " " $(-1, \sigma_1 \sigma_2)$		
	$(-1, \sigma_1) (1, \sigma_2)$ " " $R \sigma_1 \cdot \sigma_2$ $\sim R \sigma_1 \sigma_2$ " " $= (-1, \sigma_1 \sigma_2)$	Entry wise multiplication	$(1, \sigma_1) (-1, \sigma_2)$ " " $= \sigma_1 R \sigma_2$ $= R F(\sigma_1) \sigma_2$ $= (-1, F(\sigma_1) \sigma_2)$

*48 x 48 table!!*

$(-1, \sigma_1) (1, \sigma_2)$   
" "  
 $R \sigma_1 \cdot \sigma_2$   
 $\sim R \sigma_1 \sigma_2$   
" "  
 $= (-1, \sigma_1 \sigma_2)$

Entry wise multiplication

$(1, \sigma_1) (-1, \sigma_2)$   
" "  
 $= \sigma_1 R \sigma_2$   
 $= R F(\sigma_1) \sigma_2$   
 $= (-1, F(\sigma_1) \sigma_2)$

Entry wise multiplication  
in first entry, not in the second!

## 3.2

## Subgroups

### Definition 3.2.1 Subgroup

Let  $(G, \cdot)$  be a group. A non-empty<sup>a</sup> subset  $H \subseteq G$  is called a **subgroup** of  $G$  if  $H$  with the same operation  $\cdot$  is a group. We write  $H \leq G$ .

<sup>a</sup> $H$  has to be non-empty, as the identity  $e \in H$ .

**Example.** In the Rubik's cube example, the elements generated by  $H_1, V_1, H_2, V_2$  is a subgroup of  $S_4$ .  $\diamond$

### Definition 3.2.2 Order (Element)

Given an element  $g \in G$ , the **order** of  $g$  is the smallest positive integer  $n$  such that

$$g^n = e.$$

in case it exists. If no such  $n$  exists, then  $g$  has infinite order.

**Example.** Consider the following examples.

- In the Dihedral group  $D_n$ ,  $R$  has order  $n$ , and  $S$  has order 2.
- In  $S_4$  (which has 24 elements), the orders can only be 1, 2, 3, 4. This implies  $g^{12} = e$  for all  $g \in S_4$ .
- Not everything has an order.  $(\mathbb{Z}, +)$  is a group.

Given  $n \in \mathbb{Z}$ ,  $n \neq 0$ . If its order was  $k$ ,

$$\underbrace{n + n + \cdots + n}_{k \text{ times}} = 0 \implies kn = 0 \implies k = 0$$



**Claim.** A finite group always has an finite order.

### Definition 3.2.3 Order (Group)

Let  $G$  be a group. The **order** of  $G$  is its cardinality, denoted by  $|G|$ .

All of these definitions are languages to be able to understand the main question:

*What are all the groups?*

In order to take account of repetition, we give the following definition.

### Definition 3.2.4 Homomorphism

Let  $G, H$  be groups and  $\varphi : G \rightarrow H$  a function. We say  $\Phi$  is an **homomorphism** if

$$\varphi(g_1 \cdot g_2) = \varphi(g_1) \cdot \varphi(g_2) \quad \forall g_1, g_2 \in G.$$

This ia a “relabeling” of the multiplication table.

**Example.** Consider the following examples.

- The sign function

$$\begin{aligned} \text{sgn} : S_n &\rightarrow \{\pm 1\} \\ \sigma &\mapsto \text{sgn}(\sigma) \end{aligned}$$

We have  $\text{sgn}(\sigma_1 \sigma_2) = \text{sgn}(\sigma_1)\text{sgn}(\sigma_2)$ .

- For every isometry of the coloured cube  $\varphi$ , we assosiate a pemutation  $P_\varphi$ .  $P_{\varphi_1 \cdot \varphi_2} = P_{\varphi_1} \cdot P_{\varphi_2}$ .



### Definition 3.2.5 Mono-, Epi-, Iso-

An homomorphism is

- A **monomorphism** if it is injective.
- An **epimorphism** if it is surjective.
- An **isomorphism** if it is bijective.



### Definition 3.2.6 Kernel

Let  $\Phi : G \rightarrow H$  be an homomorphism. The **kernel** of  $\Phi$  is

$$\ker ((\Phi)) = \{g \in G \mid \Phi(g) = e_H\}.$$

### Definition 3.2.7

Let  $\Phi : G \rightarrow H$  be an homomorphism. The **image** of  $\Phi$  is

$$\text{Im } (\Phi) = \{\Phi(g) \mid g \in G\}.$$

**Example.** Consider  $S_n$  and the sign function  $\text{sgn} : S_n \rightarrow \{\pm 1\}$ . We have

$$\ker ((\text{sgn})) = \{\sigma \in S_n \mid \sigma \text{ needs an even number of transpositions to write}\} = A_n.$$

This is called the **alternating group** of degree  $n$ , denoted  $A_n$ <sup>1</sup>.



<sup>1</sup>Note that this group is non-decomposable for  $n \geq 5$ . This is why there is no formula for the general quintic equation.

**Example.** Consider  $A_4$ .

- $\text{id} \in A_4$
- Transpositions have an odd number of transpositions, so they are not in  $A_4$ .
- Three cycles can be decomposed into two transpositions, so they are in  $A_4$ .
- Four cycles are decomposed into three transpositions, so they are not in  $A_4$ .

Thus,

$$A_4 = \{\text{id}, (a, b)(c, d), (a, b, c)\}$$

which has 12 elements. ◊

### Definition 3.2.8 Group Action

Let  $G$  be a group and  $X$  a set. A **group action** on  $X$  by  $G$ , denoted  $G \times X$ , is a function

$$\begin{aligned}\cdot : G \times X &\rightarrow X \\ (g, x) &\mapsto g \cdot x\end{aligned}$$

such that

- 1  $1 \cdot x = x \quad \forall x \in X$ .
- 2  $h \cdot (g \cdot x) = (h \cdot g) \cdot x \quad \forall g, h \in G, x \in X$ .

Given  $x \in X$ , all the elements reachable by  $x$  (i.e.  $\{g \cdot x \mid g \in G\}$ ) are called the **orbit** of  $x$ .



## CHAPTER

# CYCLIC GROUPS

# 4

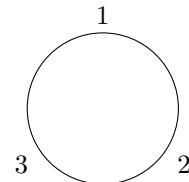
### 4.1

### Introduction

For every positive integer  $n$ , we consider the integers modulo  $n$ .

**Example.** For  $n = 3$ , we have the multiplication table:

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1



Similarly, for  $n = 4$ , we have the multiplication table:

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2



#### Definition 4.1.1 Cyclic Group

Let  $n$  be a positive integer. A **cyclic group** of order  $n$  is one that admits a generator of order  $n$ .

$$C_n = \{0, 1, \dots, n - 1\}$$

### Definition 4.1.2 Generator

A **generator** of a group  $G$  is an element  $g \in G$  such that every element of  $G$  can be written as a power of  $g$ .

The group of integers modulo  $n$  is called the **cyclic group of order  $n$**  and is denoted by  $C_n$  or  $\mathbb{Z}/n\mathbb{Z}$ .

**Example.** The integers  $\mathbb{Z}$  form a cyclic group under addition.

$$\dots \xrightarrow{+1} -2 \xrightarrow{+1} -1 \xrightarrow{+1} 0 \xrightarrow{+1} 1 \xrightarrow{+1} 2 \xrightarrow{+1} \dots$$



Given a group  $G$  and an element  $g \in G$ , we produce

$$\underbrace{\{\dots, g^{-2}, g^{-1}, 1 = g^0, g, g^2, g^3, \dots\}}_{\langle g \rangle} \subseteq G$$

### Proposition 4.1.1

Let  $G$  be a group and  $g \in G$ .

- 1 The set of powers of  $g$ ,  
 $\{g^m \mid m \in \mathbb{Z}\}$   
is a subgroup of  $G$  (denoted by  $\langle g \rangle$ ).
- 2  $g$  has order  $m$  if and only if  $\langle g \rangle$  is isomorphic to  $C_m$ .
- 3  $g$  has no order if and only if  $\langle g \rangle$  is isomorphic to  $\mathbb{Z}$ .

*Proof.* (Proposition 4.1.1) WTS  $\langle g \rangle$  is a subgroup of  $G$ .

- **Associativity** follows from that of  $G$ .
- **Identity** is a power of  $g$ , namely,  $g^0 = 1$ .
- Each element has an **inverse**, indeed, the inverse of  $g^n$  is  $g^{-n}$  which is also a power.
- **Closed** under the operation

$$g^n \cdot g^m = g^{n+m}$$

which is also a power.



*Proof.* (Proposition 4.1.2) WTS  $g$  has order  $m$  if and only if  $\langle g \rangle \cong C_m$ .  
If  $G$  has order  $m$ ,

$$1, g, g^2, \dots, g^{m-1}$$

are distinct.

Define  $\Phi : C_m \rightarrow \langle g \rangle$  by  $\Phi(k) = g^k$ .

This is well defined if  $a \equiv b \pmod{m}$ , then  $a = b + mt$  for some  $t \in \mathbb{Z}$ .

$$g^a = g^{b+mt} = g^b \cdot g^{mt} = g^b \cdot (g^m)^t = g^b \cdot 1^t = g^b$$

It is an homomorphism, indeed,

$$\Phi(a+b) = g^{a+b} = g^a \cdot g^b = \Phi(a) \cdot \Phi(b)$$

- **Injectivity**

If  $\Phi(a) = \Phi(b)$ , then  $g^a = g^b$ , so  $g^{a-b} = 1$ .

We can pick  $a, b \in \{0, 1, \dots, m-1\}$ . We can also suppose  $a \geq b$ , thus

$$0 \leq a - b \leq m - 1$$

Then  $g^{a-b} = 1$  implies  $a - b = 0$ , for otherwise  $g$  has order smaller than  $m$ .

Thus,  $a = b$ , so  $\Phi$  is injective.

- **Surjectivity**

By assumption

$$\langle h \rangle = \{g^0, g^1, \dots, g^{m-1}\}$$

Since by definition

$$\Phi(k) = g^k,$$

by taking  $k = 0, 1, \dots, m-1$  we produce all elements of  $\langle g \rangle$ .

Thus,  $\Phi$  is surjective.

We conclude that  $\Phi$  is an isomorphism. ■

**Example.** Consider  $C_6 = \{0, 1, 2, 3, 4, 5\}$ .

The cyclic groups the elements generate are

- 0 generates  $\{0\} \cong C_1$ .
- 1 and 5 generate  $\cong C_6$ ,  $C_6 = \langle 1 \rangle = \langle 5 \rangle$ .
- $\langle 2 \rangle = \{0, 2, 4\} = \langle 4 \rangle \cong C_3$ .
- $\langle 3 \rangle = \{0, 3\} \cong C_2$ .



**Example.** We have already seen in a previous example what happens. The cyclic subgroups are

- $\langle 1 \rangle = \{\text{id}\} = C_1$ .
- $\langle (1, 2) \rangle = \{\text{id}, \langle (1, 2) \rangle\} = C_2$
- $\langle (1, 3) \rangle = \{\text{id}, \langle (1, 3) \rangle\} = C_2$
- $\langle (2, 3) \rangle = \{\text{id}, \langle (2, 3) \rangle\} = C_2$
- $\langle (1, 2, 3) \rangle = \{\text{id}, (1, 2, 3), (1, 3, 2)\} = C_3$



### Proposition 4.1.2

Let  $p$  be a prime number, and  $G$  be a group of order  $p$ . Then  $G$  is cyclic,

$$G \cong C_p$$

*Proof.* Let  $G$  be a group of order  $p$ .

Since  $p$  is prime,  $G$  has at least two elements. Thus, there exists  $g \in G$  with  $g \neq e$ . Since  $G$  is finite,  $g$  must have a finite order  $m$ . Thus,

$$C_m = \{1, g, g^2, \dots, g^{m-1}\} \subseteq G$$

Let  $x \in G$  and multiply by  $g$  successively by the left.

$$x \xrightarrow{g} gx \xrightarrow{g} g^2x \xrightarrow{g} \dots \xrightarrow{g} g^{m-1}x \xrightarrow{g} g^mx = x$$

There is no repetition earlier than  $m$ , since otherwise  $g^i x = g^j x$  for some  $0 \leq i < j \leq m-1$ , so  $g^i = g^j$  (since  $g$  has order  $m$ ), which is a contradiction.

Doing this, we see that  $G$  decomposes into cycles of size  $m$ . There must be a finite number of cycles, say  $k$ .

Thus,  $|G| = km$ , so  $p = km$ . Since  $p$  is prime,  $k = 1$  or  $m = 1$ .

However,  $m \neq 1$  since  $g \neq e$ . Thus,  $k = 1$ , so  $m = p$  and  $G = C_p$ . ■

Let us rephrase a step. Let  $x \in G$ , and multiply  $x$  by every element of  $C_m$ .

Doing that we have

- $G$  a group
- $H$  a subgroup of  $G$  of order  $m$ .
- $x \in G$  an element.

Multiply every element of  $H$  by  $x$ ,

**Example.** Consider  $S_3 = \{\text{id}, (1, 2), (1, 3), (2, 3), (1, 2, 3), (1, 3, 2)\}$ .  
Let  $H = \{\text{id}, (1, 2)\}$ .

- $H(2, 3) = \{(1(2, 3), (1, 2)(2, 3)\} = \{(2, 3), (1, 2, 3)\}$
- $H(1, 3) = \{(1(1, 3), (1, 2)(1, 3)\} = \{(1, 3), (1, 3, 2)\}$

These two sets are called the **right cosets** of  $H$  in  $G$ . ◊

### Definition 4.1.3 Coset

Given a group  $G$  and a subgroup  $H$ , we define a **coset** of  $H$  in  $G$  as a set of the form

$$\begin{aligned} Hx &= \{hx \mid h \in H\} && \text{(right coset)} \\ xH &= \{xh \mid h \in H\} && \text{(left coset)} \end{aligned}$$

We denote by

- $H \setminus G$  the set of right cosets of  $H$  in  $G$ , and
- $G/H$  the set of left cosets of  $H$  in  $G$ .

### Proposition 4.1.3

Let  $G$  be a group and  $H$  be a subgroup of  $G$ . Then

- 1 All cosets of  $H$  in  $G$  have the cardinality of  $H$ .
- 2 All left cosets are disjoint, and so are all right cosets.

*Proof.* We prove the two statements.

- 1 Multiplying by  $x$  is a bijection.
- 2 Suppose  $xH \cap yH \neq \emptyset$ .

Then there exists  $z \in xH \cap yH$ , that is,  $z = xh_1 = yh_2$  for some  $h_1, h_2 \in H$ .

$$\begin{aligned} y^{-1}xh_1h_1^{-1} &= y^{-1}yh_2h_1^{-1} \\ y^{-1}x &= h_2h_1^{-1} \in H \end{aligned}$$

Then,  $y^{-1}x = h$  for some  $h \in H$ , so  $x = yh \in yH$ .

But then for  $x\tilde{h} \in xH$ ,  $x\tilde{h} = (yh)\tilde{h}$

$$= y(h\tilde{h}) \in yH$$

That is,  $xH \subseteq yH$ . Similarly,  $yH \subseteq xH$ , so  $xH = yH$ .

■

### Theorem 4.1.1 Langrange's Theorem

Let  $G$  be a finite group and  $H$  be a subgroup of  $G$ . Then

$$|G| = |H| \text{ divides } |G|$$

*Proof.*  $G$  is a disjoint union of cosets of  $H$  in  $G$ .

Say there are  $k$  cosets. Then

$$|G| = k|H| \implies H \mid G$$

■

### Corollary 4.1.1 Corollary of Proposition

Let  $H \leq G$  be a subgroup of a finite group  $G$ . Then

- 1  $xH = yH$  if and only if  $y^{-1}x \in H$ .
- 2  $Hx = Hy$  if and only if  $xy^{-1} \in H$ .

**Example.**  $C_n$  has order  $N$ .  $n$  has certain divisors, and  $C_n$  has a generator  $g$ :

$$C_n = \{1, g, g^2, \dots, g^{n-1}\}$$

Consider when  $n = 12$ .

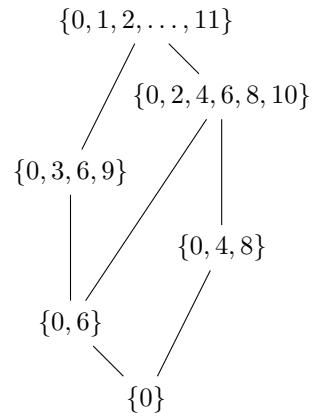
$$C_n = \mathbb{Z}/12\mathbb{Z} = \{0, 1, 2, \dots, 11\}$$

$12 = 4 \times 3$ , so the divisors are

1	{0}
2	{0, 6}
3	{0, 4, 8}
4	{0, 3, 6, 9}
6	{0, 2, 4, 6, 8, 10}
12	{0, 1, 2, ..., 11}

$C_n$  has exactly one subgroup of each order dividing  $n$ .

We can construct a subgroup map.



This is called the **Hasse diagram** of the subgroup lattice of  $C_{12}$ . ◇

## CHAPTER

# 5

## ISOMORPHIC THEOREMS

### 5.1

### Normal Subgroups

#### Definition 5.1.1 Normal Subgroup

Let  $G$  be a group and  $N$  be a subgroup. We say  $N$  is a **normal subgroup** of  $G$ , denoted  $N \triangleleft G$ , if

$$\forall g \in G, gN = Ng.$$

Equivalently, if  $gNg^{-1} = N$ .

#### Definition 5.1.2 Simple Group

A group  $G$  is **simple** if it has no nontrivial normal subgroups.

**Example.** Kernels of group homomorphisms are normal subgroups.

*Proof.* Let  $x \in \ker(\varphi)$  for some homomorphism  $\varphi : G \rightarrow H$ .

Then,  $\varphi(gxg^{-1}) = \varphi(g)\varphi(x)\varphi(g)^{-1} = \varphi(g)e\varphi(g)^{-1} = e$ .

Therefore,  $gxg^{-1} \in \ker(\varphi)$ . ■



It is important to note that some groups are normal under one group but not under another.

**Example.** The alternating group,  $A_n$ , is normal in the symmetric group,  $S_n$ .

This is because  $A_n$  is the kernel of the sign homomorphism, which is a normal subgroup by the previous example.

For example, consider  $S_3$  and  $A_3$ .

$$S_3 = \{e, (12), (13), (23), (123), (132)\}, \quad A_3 = \{e, (123), (132)\}.$$

We have  $(13)A_3(13) = \{(13)e(13), (13)(123)(13), (13)(132)(13)\} = \{e, (132), (123)\} = A_3$ . ◇

## 5.2

## The First Two Isomorphism Theorem

### Definition 5.2.1 Quotient Group

Let  $G$  be a group and  $N$  a normal subgroup. Then, we can define the **quotient group**  $G/N$  as the set of left cosets of  $N$  in  $G$  with the operation

$$(gN)(hN) := (gh)N.$$

### Theorem 5.2.1

$G/N$  is a group if and only if  $N \triangleleft G$ .

**Example.**  $A_n$  is normal in  $S_n$ , so  $S_n/A_n$  is a group.

$A_n$  has 2 cosets: itself, and the set of all odd permutations. Therefore,  $S_n/A_n \cong \mathbb{Z}_2$ .

	$A_n$	$(12)A_n$		$0$	$1$
$A_n$	$A_n$	$(12)A_n$	$0$	$0$	$1$
$(12)A_n$	$(12)A_n$	$A_n$	$1$	$1$	$0$

We have  $S_n/A_n \cong \mathbb{Z}/2\mathbb{Z} = \{0, 1\} = \{-1, 1\}$ .

Moreover, since  $\text{sgn} : S_n \rightarrow \{-1, 1\}$ , we see  $S_n/\ker(\text{sgn}) \cong \text{Im}(\text{sgn})$ . ◇

### Theorem 5.2.2 The First Isomorphism Theorem

Let  $G$  be a group, and  $\varphi : G \rightarrow H$  be an homomorphism. Then,

$$G/\ker(\varphi) \cong \text{Im}(\varphi).$$

and the isomorphism is given by

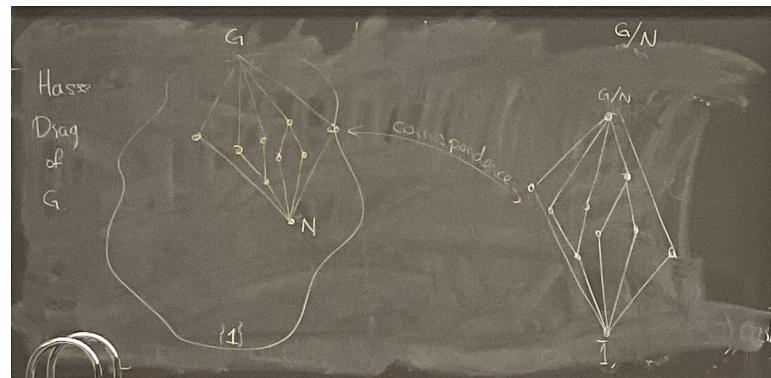
$$\begin{aligned} G/\ker(\varphi) &\rightarrow \text{Im}(\varphi) \\ g\ker(\varphi) &\mapsto \varphi(g) \end{aligned}$$

### Theorem 5.2.3 The Correspondence Theorem

Let  $G$  be a group, and  $N \triangleleft G$ . Then, there is a correspondence between the set of subgroups

of  $G$  containing  $N$  and the set of subgroups of  $G/N$ .

$$\begin{array}{ccc} \{H \leq G \mid N \subseteq H \subseteq G\} & \longleftrightarrow & \{K \leq G/N\} \\ H & \longleftrightarrow & H/N \end{array}$$



The first isomorphism theorem tells us how to reduce the complexity of the group, and the correspondence theorem tells us that we do not lose any information when we do so.



## Part II

# Appendices



---

## BIBLIOGRAPHY



---

# INDEX

**A**

Abelian Group, 18

**C**

correspondence theorem, 34  
Coset, 30  
Cycle, 11  
Cyclic Group, 27

**E**

Epimorphism, 24

**F**

first isomorphism theorem, 34

**G**

Generator, 28  
Group, 17  
Group Action, 25

**H**

Homomorphism, 24

**I**

Identity Permutation, 11  
Isometry, 14  
Isomorphism, 24

**K**

Kernel, 24

**L**

Langrange's Theorem, 31

**M**

Monomorphism, 24

**N**

normal subgroup, 33

**O**

Orbit, 25  
Order (Element), 23  
Order (Group), 23

**P**

Permutation, 11

**Q**

quotient group, 34

**S**

simple group, 33  
Subgroup, 23  
Symmetric Group, 11

**T**

Transposition, 11