MAT301

Groups and Symmetries

Sinan Li

2024

CONTENTS

Part I

Notes

CHAPTER

INTRODUCTION 1

1.1 Course Information

- **Instructor**: Malors Emilio Espinosa Lara
- **Office**: BA 6256
- **Email**: 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*.

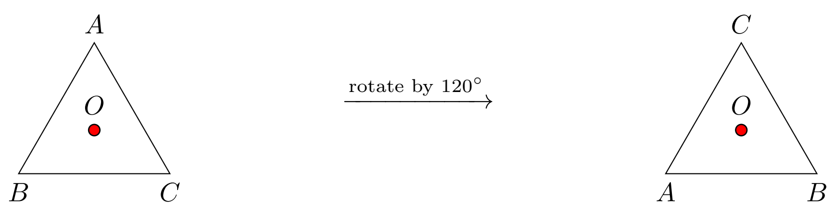
CHAPTER

INTRODUCTION TO SYMMETRY 2

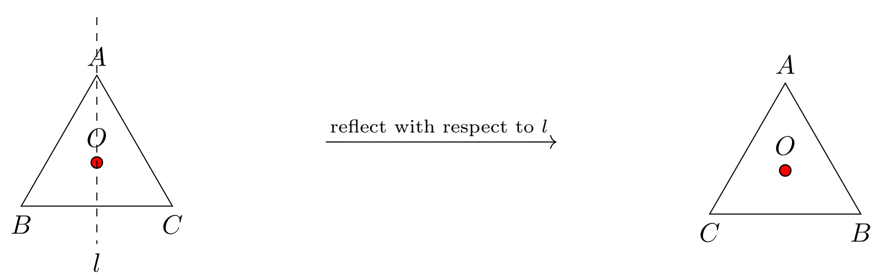
2.1 Intuition and Motivation

The idea of symmetry is the 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.

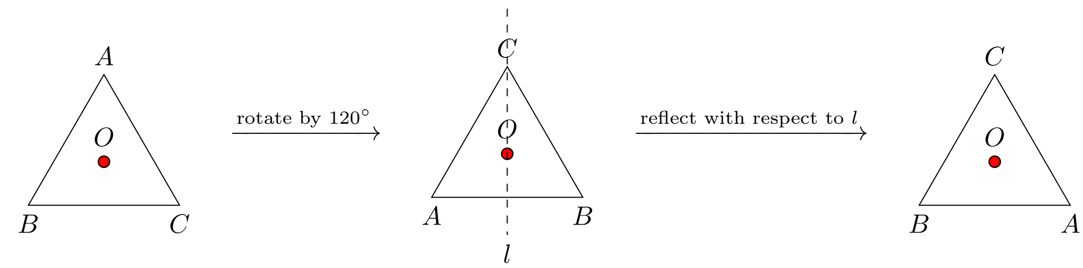
Example (Polygons)**.** We can rotate the following triangle with respect to O by $120°$, and the triangle remains the same. This triangle has rotational symmetry.



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.

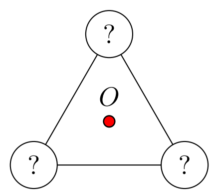


Is there any other symmetry? Yes, we can combine the two symmetries above. We first rotate the triangle by $120°$, and then reflect it with respect to l. This triangle has both rotational and reflection symmetry.



$\diamondsuit$

The above example is a very simple one. However, given an 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.



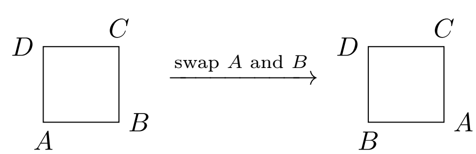
Since the transformations are linear, they preserve linearity. This, it suffices to consider the transformations of the vertices.

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. $\diamondsuit$

Naively, given an 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 $1, 2, \ldots, n$.

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.

1 2 3	1 2 3	1 2 3	1 2 3	1 2 3	1 2 3
1 2 3	1 3 2	3 2 1	2 1 3	3 1 2	2 3 1
(1)(2)(3)	(1)(23)	(13)(2)	(12)(3)	(132)	(123)

Here, (1)(23) means

- 1 goes to 1.

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

$\diamondsuit$

Example. Consider the following permutation.

1 2 3 4 5 6 7	1 2 3 4 5 6 7
3 4 2 1 7 5 6	2 3 1 4 6 5 7
(1324)(576)	(1 2 3)(5 6)

$\diamondsuit$

Example. Suppose you have two permutations σ and τ:

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

What happens if we perform one after the other?

- σ first, τ second[1]: $(1654)(32)(12)(3456) = (1654)(32)(12)(3456)$
  - We start with 1: $1 \to 2 \to 3$, so $1 \to 3$.
  - We then consider 3: $3 \to 4 \to 1$, so $3 \to 1$.
  - Now, we consider 2: $2 \to 1 \to 6$, so $2 \to 6$.
  - $6 \to 3 \to 2$, so $6 \to 2$.
  - $4 \to 5 \to 4$, so $4 \to 4$.
  - $5 \to 6 \to 5$, so $5 \to 5$.

  Thus, we get
  $$(13)(26)(4)(5).$$
- τ first, σ second: $(12)(3456)(1654)(32) = (12)(3456)(1654)(32)$
  - We start with 1: $1 \to 6 \to 4$, so $1 \to 3$.
  - We then consider 3: $4 \to 5 \to 1$, so $4 \to 1$.
  - ...

  Eventually, we get
  $$(13)(24)(5)(6).$$

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

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

[1] Note that we read from right to left.

$\circ$	$\mathbb{1}$	(12)	(13)	(23)	(123)	(132)
$\mathbb{1}$						
(12)						
(13)						
(23)	(23)	(132)	(123)	$\mathbb{1}$	(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 $\mathbb{1} = (12)(12)$.

Theorem 2.2.1

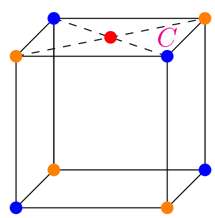
The amount of transpositions needed to create a permutation preservers its parity.

In other words, if a permutation α can be expressed as a product of transpositions

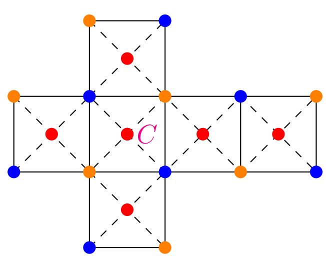
$$\alpha = \tau_1\tau_2\ldots\tau_n \qquad \text{and} \qquad \alpha = \sigma_1\sigma_2\ldots\sigma_m$$

where τ and σ 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.



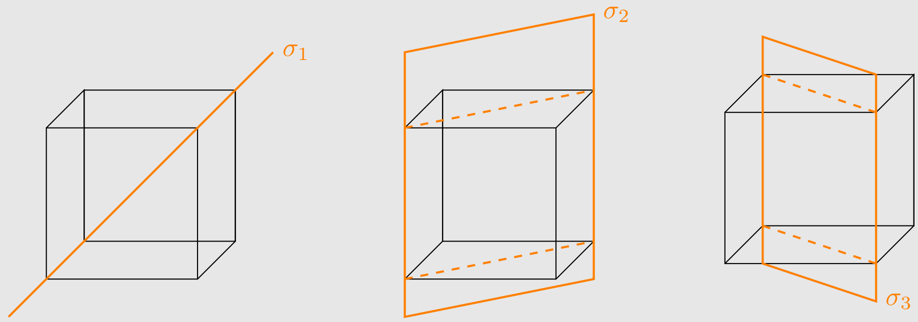
Question: What are the isometries that preserve the colouring of this object?

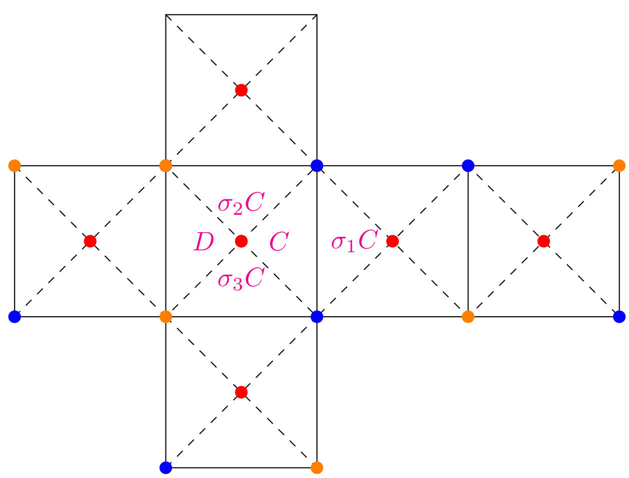
Definition 2.2.6 Isometry

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

Remark

Consider reflection with respect to the planes σ_1, σ_2, and σ_3.





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

$$\begin{array}{ccccc} \mathbb{R}^3 & \to & \mathbb{R}^3 & \to & \mathbb{R}^3 \\ & \sigma_3 & & \sigma_2 & \\ & \sigma_2 & & \sigma_3 & \end{array}$$

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 $S, T : \mathbb{R}^3 \to \mathbb{R}^3$ 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 σ_1, σ_2, and σ_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. ♢

CHAPTER

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

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

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

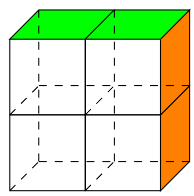
A group $(G, \cdot)$ is called **abelian** if

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

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 $90°$ 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:

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

- $H_2H_1V_2V_1 = R^2$
- $R^3V_1R = R^{-1}V_1R = H_1$
- ...

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

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

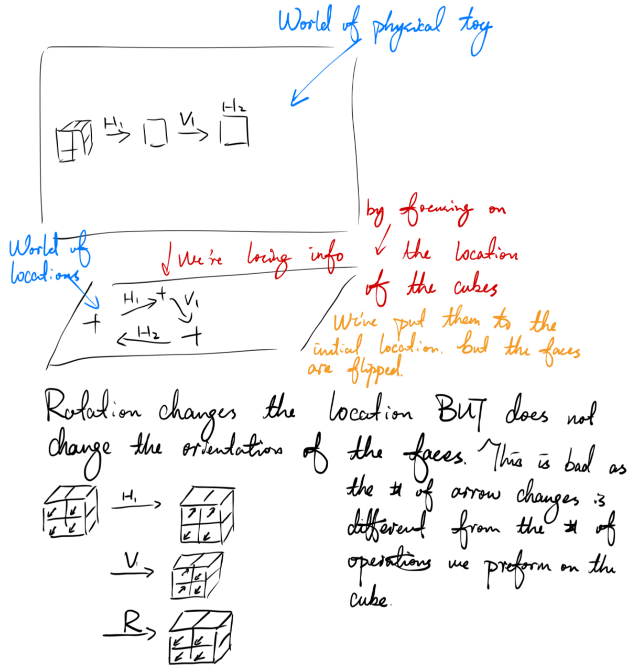
$\diamondsuit$

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

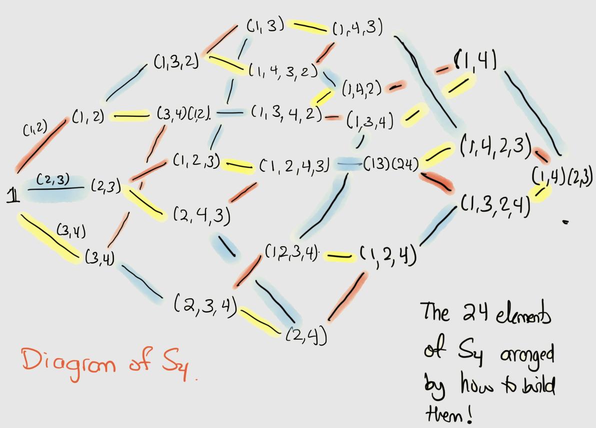
What we have seen is that these two models are codify information in different ways. We can generate a map of the potential positions.



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

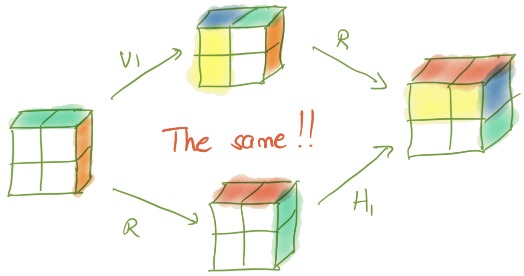
Remark

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

$$H_1R = RV_1 \qquad H_2R = RV_2$$



Example. "Simplify" the instructions

$$RV_1H_2RV_2H_1H_2RV_1H_2$$

Using the two equations above,

$$\begin{aligned} RV_1H_2RV_2H_1H_2RV_1H_2 &= RV_1H_2RV_2H_1RV_2V_1H_2 \\ &= RV_1H_2RV_2RV_1V_2V_1H_2 \\ &= RV_1H_2RRH_2V_1V_2V_1H_2 \\ &= RV_1H_2V_1V_2H_1H_2H_2V_1V_2V_1H_2 \qquad (RR = V_1V_2H_1H_2) \end{aligned}$$

This way, we have moved all the "noice", 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

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

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

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

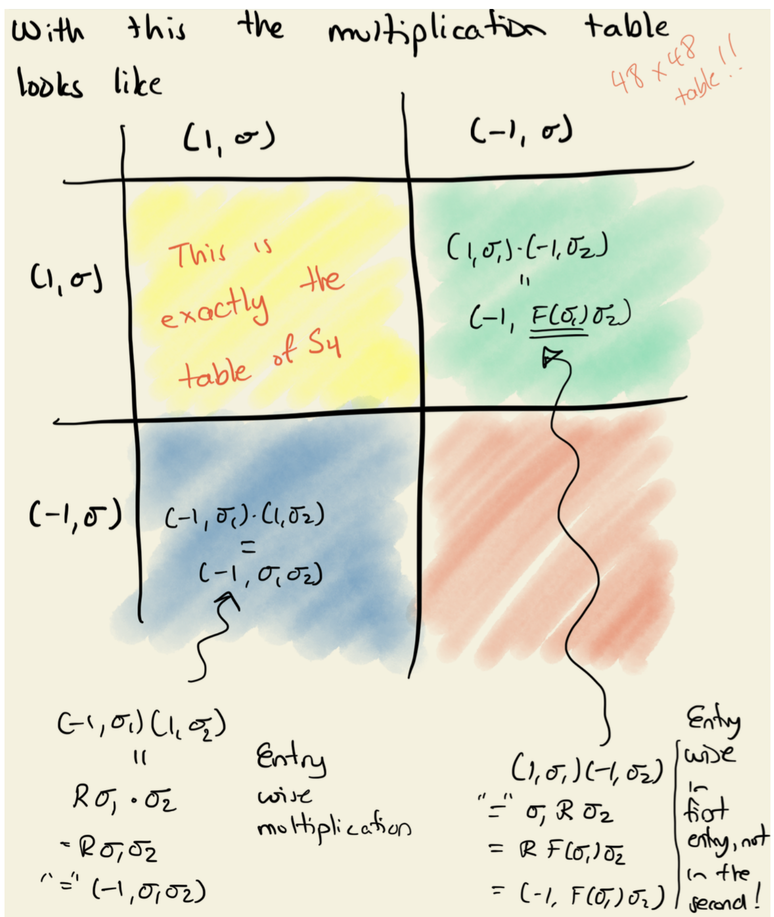
  which means $R \in S_4$, which is impossible.

∎

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

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

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



3.2 Subgroups

Definition 3.2.1 Subgroup

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

[a] 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. ♢

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 $\varphi : G \to H$ a function. We say Φ 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

$$\begin{array}{rccc} \mathrm{sgn}: & S_n & \to & \{\pm 1\} \\ & \sigma & \mapsto & \mathrm{sgn}(\sigma) \end{array}$$

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

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

$\diamondsuit$

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 $\Phi : G \to H$ be an homomorphism. The **kernel** of Φ is

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

Definition 3.2.7

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

$$\mathrm{Im}\left(\Phi\right) = \{\Phi(g) \mid g \in G\}.$$

Example. Consider S_n and the sign function $\mathrm{sgn} : S_n \to \{\pm 1\}$. We have

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

This is called the **alternating group** of degree n, denoted A_n[1]. $\diamondsuit$

[1] Note that this group is non-decomposible for $n \geq 5$. This is why there is no formula for the general quintic equation.

Example. Consider A_4.

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

Thus,

$$A_4 = \{\mathbb{I}, (a,b)(c,d), (a,b,c)\}$$

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 $G \circlearrowleft X$, is a function

$$\begin{array}{rccc} \cdot : & G \times X & \to & X \\ & (g,x) & \mapsto & g \cdot x \end{array}$$

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 reachible by x (i.e. $\{g \cdot x \mid g \in G\}$) are called the **orbit** of x.

CHAPTER

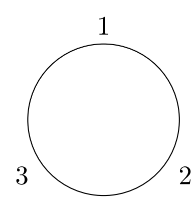
4 CYCLIC GROUPS

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 Cuclic Group

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

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

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.

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

$\diamondsuit$

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

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

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.

$\blacksquare$

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,

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

are distinct.
Define $\Phi : C_m \to \langle g \rangle$ 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 $a, b \in \{0, 1, \ldots, m-1\}$. 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 owtherwise g has order smaller than m.
  Thus, $a = b$, so Φ is injective.
- **Surjectivity**
  By assumption
  $$\langle h \rangle = \{g^0, g^1, \ldots, g^{m-1}\}$$
  Since by definition
  $$\Phi(k) = g^k,$$
  by taking $k = 0, 1, \ldots, m-1$ we produce all elements of $\langle g \rangle$.
  Thus, Φ is surjective.

We conclude that Φ is an isomorphism. ■

Example. Consider $C_6 = \{0, 1, 2, 3, 4, 5\}$.
The cyclic groups the elements generate are

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

♢

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

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

♢

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,

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

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

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

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 vy 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 $S_3 = \{\mathrm{id}, (1,2), (1,3), (2,3), (1,2,3), (1,3,2)\}$.
Let $H = \{\mathrm{id}, (1,2)\}$.

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

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

$$Hx = \{hx \mid h \in H\} \qquad (\textbf{right coset})$$
$$xH = \{xh \mid h \in H\} \qquad (\textbf{left coset})$$

We denote by

- $H\backslash G$ 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 $xH \cap yH \neq \varnothing$.
   Then there exists $z \in xH \cap yH$, that is, $z = xh_1 = yh_2$ for some $h_1, h_2 \in H$.
   $$\begin{aligned} y^{-1}xh^1{h_1}^{-1} &= y^{-1}yh_2{h_1}^{-1} \\ y^{-1}x &= h_2{h_1}^{-1} \in H \end{aligned}$$
   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 $xy^{-1} \in H$.

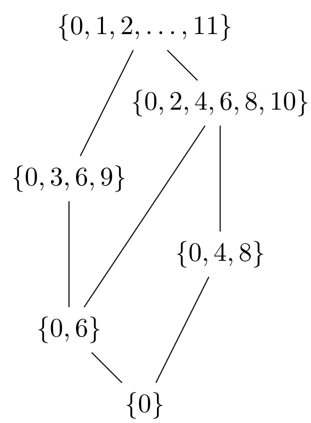
Example. C_n has order N. n has certain divisors, and C_n has a generator g:

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

Consider when $n = 12$.
$C_n = \mathbb{Z}/12\mathbb{Z} = \{0, 1, 2, \ldots, 11\}$
$12 = 4 \times 3$, so the devisors are

1	$\{0\}$
2	$\{0, 6\}$
3	$\{0, 4, 8\}$
4	$\{0, 3, 6, 9\}$
6	$\{0, 2, 4, 6, 8, 10\}$
12	$\{0, 1, 2, \ldots, 11\}$

$C_n$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

ISOMORPHIC THEOREMS 5

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 $\varphi : G \to H$.
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 group 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 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, $S_n/A_n \cong \mathbb{Z}_2$.

$$\begin{array}{c|c|c} & A_n & (12)A_n \\ \hline A_n & A_n & (12)A_n \\ \hline (12)A_n & (12)A_n & A_n \end{array} \quad \cong \quad \begin{array}{c|c|c} & 0 & 1 \\ \hline 0 & 0 & 1 \\ \hline 1 & 1 & 0 \end{array}$$

We have $S_n/A_n \cong \mathbb{Z}/2\mathbb{Z} = \{0, 1\} = \{-1, 1\}$.
Moreover, since $\mathrm{sgn} : S_n \to \{-1, 1\}$, we see $S_n/\ker(\mathrm{sgn}) \cong \mathrm{Im}(\mathrm{sgn})$. ◊

Theorem 5.2.2 The First Isomorphism Theorem

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

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

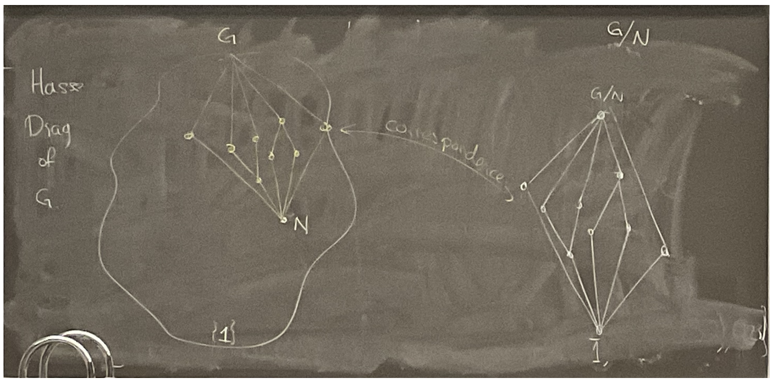
and the isomorphism is given by

$$\begin{array}{ccc} G/\ker(\varphi) & \to & \mathrm{Im}(\varphi) \\ g\ker(\varphi) & \mapsto & \varphi(g) \end{array}$$

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 loose any information when we do so.

Proposition 5.2.1

Let G be a group, and H a subgroup. Then H is normal in G if any only if there exists some homomorphism $\varphi : G \to K$ to some group K such that $H = \ker(\varphi)$.

Remark

Sometimes, it is difficult to prove that a subgroup is normal directly. However, if we can find a homomorphism with the subgroup as its kernel, then we can conclude that the subgroup is normal.

Definition 5.2.2 Index

Let H be a subgroup of G. The cardinality of G/H is called the **index** of H in G, denoted $[G : H]$.

Informally, the index of a subgroup is the number of cosets of the subgroup in the group.

Theorem 5.2.4

Let G be a group and $H \leq G$ of index 2. Then, H is normal in G.

We will construct a homomorphism $\varphi : G \to \mathbb{Z}_2$ with $H = \ker(\varphi)$, and thus $H \triangleleft G$.

Remark
We often construct the homomorphism by manifesting some property of the subgroup.

Proof. Since $[G : H] = 2$, we have $G = H \sqcup g_0 H$ for some $g_0 \in G \setminus H$.
Define a function
$$phi : G \to \{1, -1\}$$
by
$$\varphi(g) = \begin{cases} 1 & g \in H \\ -1 & g \in g_0 H \end{cases}$$
We claim that φ is a homomorphism. That means to prove $\varphi(gh) = \varphi(g)\varphi(h)$ for all $g, h \in G$.
In words, this means

- $g, h \in H$ implies $gh \in H$

  This follows from the fact that H is a subgroup.

- $g, h \notin H$ implies $gh \in H$

- $g \in H$ and $h \notin H$ implies $gh \notin H$

  If $g \in H$ and $h \notin H$, then $g \in H$ and $h \in g_0 H$.

  This means $\exists t \in H$ s.t. $h = g_0 t$.

  Suppose for contradiction that $gh = g g_0 t \in H$.

  Then, $g_0 = g^{-1}(gh)t^{-1} \in H$, which is a contradiction.

We conclude that φ is indeed a homomorphism.
By definition,
$$\ker(\varphi) = \{g \in G \mid \varphi(g) = 1\} = \{g \in G \mid g \in H\} = H.$$
Therefore, H is normal in G. ∎

Example. These are some examples of normal subgroups we have seen before.

1. Let D_n be the dihedral group generated by R and S.

   $|D_n| = 2n$.

   $\{1, R, \ldots, R^{n-1}\} \cong C_n$ is a subgroup of index 2, $[D_n : C_n] = 2$.

   Thus, $\{1, R, \ldots, R^{n-1}\} \triangleleft D_n$.

2. Let $\mathcal{R}$ be the group generated by Rubik's cube of $2 \times 2 \times 1$.

   $|\mathcal{R}| = 48$.

   V_1, V_2, H_1, H_2 is a subgroup that generates S_4, so $[\mathcal{R} : S_4] = 2$.

   Thus, $S_4 \triangleleft \mathcal{R}$.

♢

Theorem 5.2.5

Let p be a prime number, and G be a group of order p^2. Then, G is isomorphic to

$$C_{p^2} \quad \text{or} \quad C_p \times C_p.$$

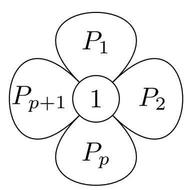
Proof. If G is cyclic, then $G \cong C_{p^2}$.
Suppose G is not cyclic.
Let $x \in G$. Since $|x|$ divides $|G| = p^2$ by Lagrange Theorem, we have $|x| \in \{1, p, p^2\}$.
$|x| = 1$ iff $x = e$, and $|x| \neq p^2$ since G is not cyclic.
Every non-identity element must have has order p.

We count the number of C_p's in G.
The only intersections two of these C_p's can have is the identity, $\{e\}$, since p is prime.
The count is as follows:

$$(\text{number of } C_p) \times (p-1) + 1 = p^2.$$

The number of C_p's is

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



Each of these is a cyclic group of order p.
Take $g \in G$, P_i the cyclic group generated by g.

$$gP_ig^{-1} = P_j$$

for some cyclic group P_j.
Let us call $\Phi(g) \in S_{p+1}$ such that

$$gP_ig^{-1} = P_{\Phi(g)(i)}.$$

In this way we have created a map

$$\Phi : G \to S_{p+1}.$$

We claim that Φ is a homomorphism.
Pick $xy \in G$, $(xy)P_i(xy)^{-1} = x(yP_iy^{-1})x^{-1}$

$$= xP_{\Phi(y)(i)}x^{-1}$$
$$= P_{\Phi(x)(\Phi(y)(i))}.$$

Meanwhile, $(xy)P_i(xy)^{-1} = P_{\Phi(xy)(i)}$, so $\Phi(xy)(i) = \Phi(x)(\Phi(y)(i))$ for all i.
Therefore, $\Phi(xy) = \Phi(x) \circ \Phi(y)$.

Thus, $\Phi : G \to S_{p+1}$ must satisfy
$$p^2 = |\ker(\Phi)| \cdot |\mathrm{Im}(\Phi)|.$$
If $\ker(\Phi) = \{e\}$, then $|\mathrm{Im}(\Phi)| = p^2$.
This cannot happen, since p^2 is not a divisor of $(p+1)!$, the order of S_{p+1}.
This is a violation of Lagrange's Theorem.
Then, the kernel of Φ is not trivial.

There are elements $x \neq e$ such that
$$xP_ix^{-1} = P_i \quad \text{for all } i.$$
Suppose P_i does not contain x, and consider y a generator of P_i.
Then, $xyx^{-1} = y^n$ for some n.
$$y^{2n} = (xyx^{-1})(xyx^{-1}) = xy^2x^{-1}$$
Continuing like this,
$$xy^kx^{-1} = y^{kn}$$

The powers of x, $\{1, x, x^2, \ldots, x^{p-1}\}$, move the elements of P_i as follows:
$$\begin{aligned} x^2yx^{-2} &= x(xyx^{-1})x^{-1} \\ &= xy^nx^{-1} \\ &= (xyx^{-1})^n \\ &= (y^n)^n \\ &= y^{n^2}. \end{aligned}$$
Continuing like this,
$$x^kyx^{-k} = y^{n^k}.$$

Pick $k = p-1$, we know that $x^{p-1} = x^{-1}$, so
$$x^{-1}yx = y^{n^{p-1}} = y$$
by Fermat's Little Theorem.

Theorem 5.2.6 Fermat's Little Theorem
Let p be a prime number, and a be an integer not divisible by p. Then,
$$a^{p-1} \equiv 1 \mod p.$$

This allows us to conclude the following face:
$$\exists x, y \in G \text{ of order } p \text{ that commute.}$$
Define
$$\begin{aligned} \Psi : \quad \mathbb{Z}/p\mathbb{Z} \quad &\times \quad \mathbb{Z}/p\mathbb{Z} \to G \\ (m,n) \quad &\mapsto \quad x^my^n \end{aligned}$$

Claim. Φ is an isomorphism.

- **Injectivity**
  $x^m y^n = 1 \implies x^m = y^{-n} \in P_i n P_j = \{e\}$, where $x \in P_i$ and $y \in P_j$.
- **Surjectivity**
  Let $g \in G$. Then, $g = x^m y^n$ for some $m, n \in \mathbb{Z}/p\mathbb{Z}$.
- **Homomorphism**
$$\begin{aligned}\Psi(m_1 + m_2, n_1 + n_2) &= x^{m_1+m_2} y^{n_1+n_2} \\ &= x^{m_1} x^{m_2} y^{n_1} y^{n_2} \\ &= x^{m_1} y^{n_1} x^{m_2} y^{n_2} \\ &= \Psi(m_1, n_1)\Psi(m_2, n_2)\end{aligned}$$

This completes the proof. ■

Part II

Appendices

BIBLIOGRAPHY

INDEX