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*.

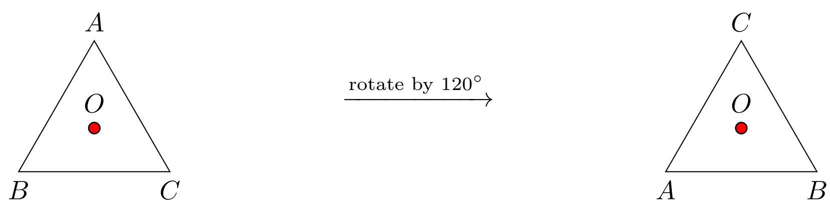
CHAPTER

INTRODUCTION TO SYMMETRY 2

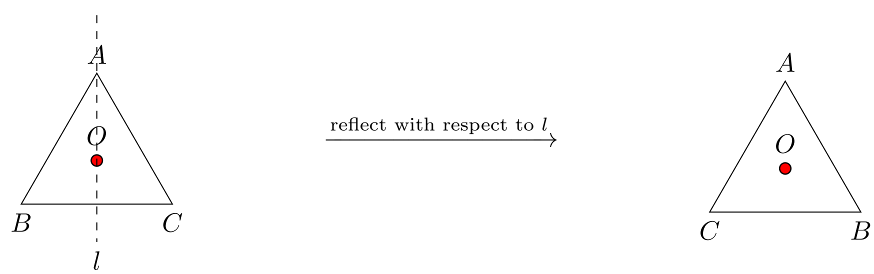
2.1 Intuition and Motivation

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.

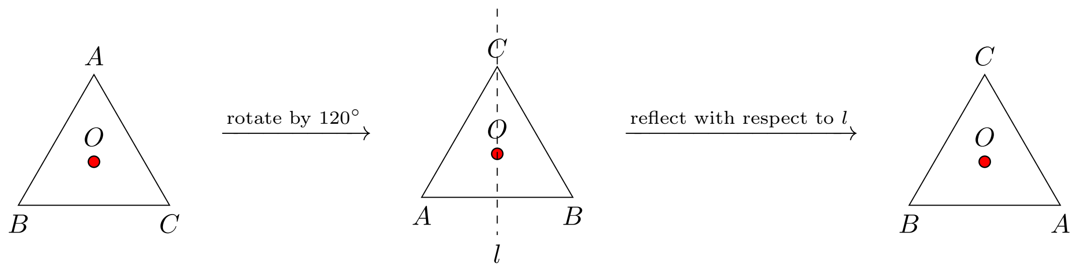
Example (Polygons)**.** We can rotate the following triangle with respect to O by $120°$, and the triangle remains the same. This triangle has rotational symmetry.



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.

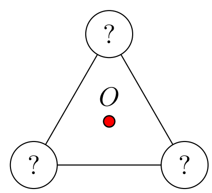


Is there any other symmetry? Yes, we can combine the two symmetries above. We first rotate the triangle by $120°$, and then reflect it with respect to l. This triangle has both rotational and reflection symmetry.



$\diamondsuit$

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.



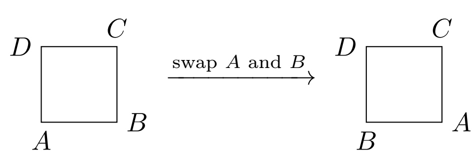
Since the transformations are linear, they preserve linearity. This, it suffices to consider the transformations of the vertices.

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

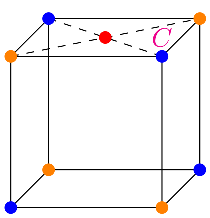
The amount of transpositions needed to create a permutation preservers its parity.

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

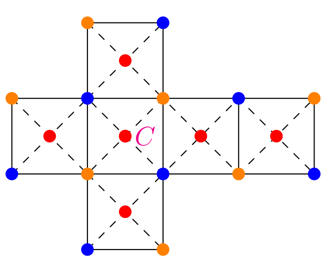
$$\alpha = \tau_1\tau_2 \dots \tau_n \qquad \text{and} \qquad \alpha = \sigma_1\sigma_2 \dots \sigma_m$$

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.



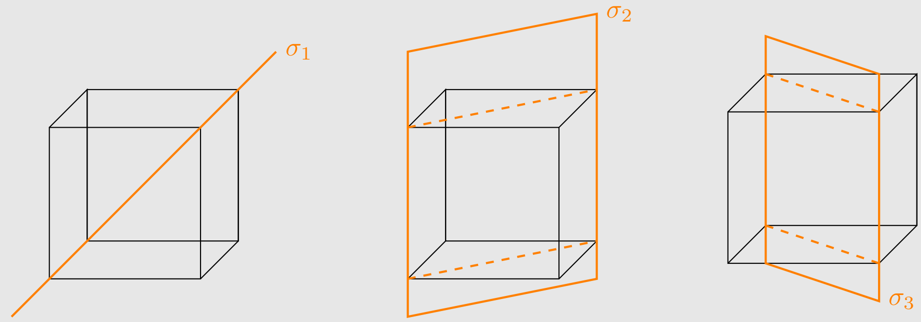
Question: What are the isometries that preserve the colouring of this object?

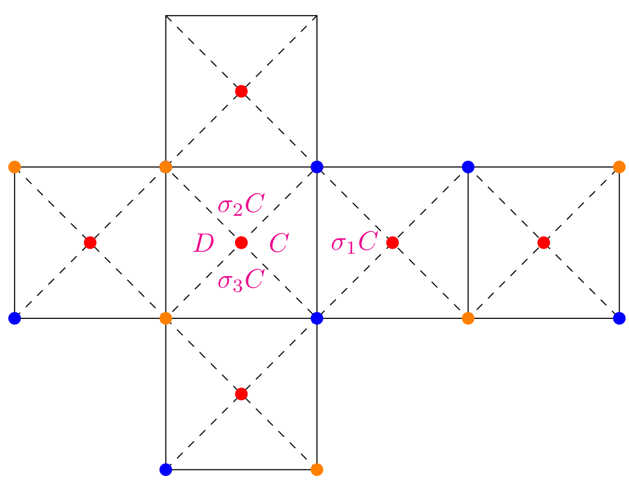
Definition 2.2.6 Isometry

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

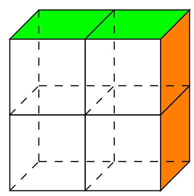
A group $(G, \cdot)$ is called **abelian** if

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

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:

- $V_1V_2 = V_2V_1 = V$
- $H_1H_2 = H_2H_1 = H$
- $V_1H_1 = H_1V_1 = R$

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

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

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

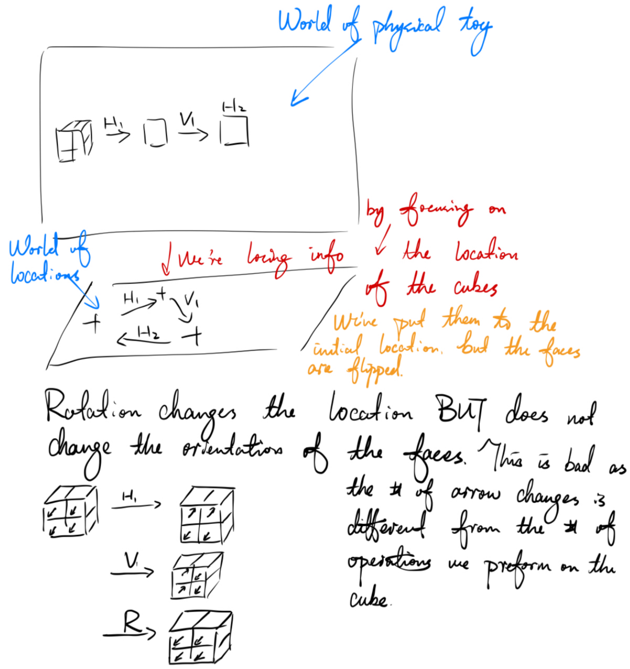
$\diamondsuit$

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

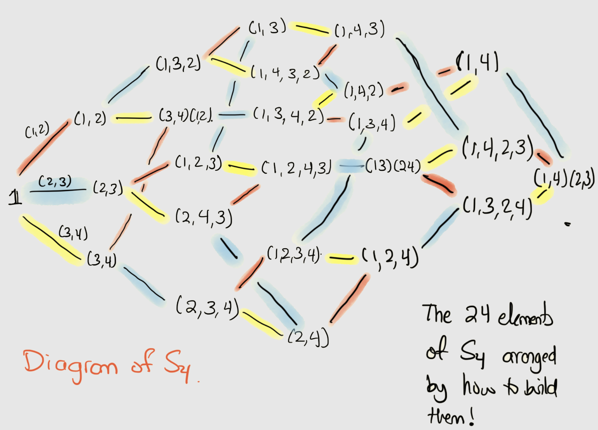
1. The complete toy

❷ 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.

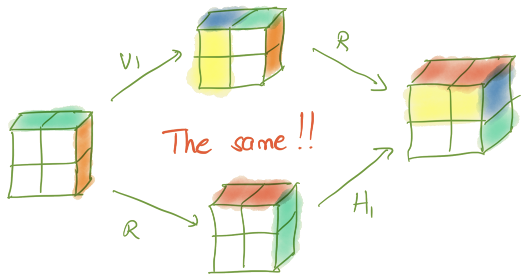


If we only allow H_1, V_1, H_2, V_2, then the locations are believable. The group they generate is S_4.

> **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

$$H_1 R = R V_1 \qquad H_2 R = R V_2$$



Example. "Simplify" the instructions

$$R V_1 H_2 R V_2 H_1 H_2 R V_1 H_2$$

Using the two equations above,

$$\begin{aligned} R V_1 H_2 R V_2 H_1 H_2 R V_1 H_2 &= R V_1 H_2 R V_2 H_1 R V_2 V_1 H_2 \\ &= R V_1 H_2 R V_2 R V_1 V_2 V_1 H_2 \\ &= R V_1 H_2 R R H_2 V_1 V_2 V_1 H_2 \\ &= R V_1 H_2 V_1 V_2 H_1 H_2 H_2 V_1 V_2 V_1 H_2 \qquad (RR = V_1 V_2 H_1 H_2) \end{aligned}$$

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,

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

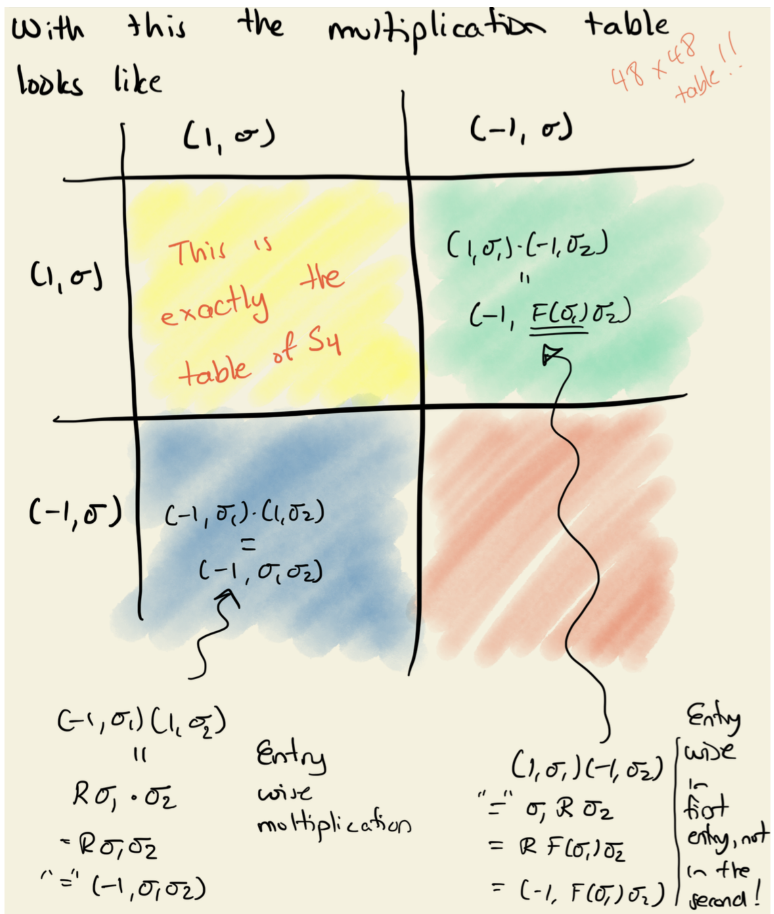
  which means $R \in S_4$, which is impossible.

■

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.



Part II

Appendices

BIBLIOGRAPHY

INDEX