



# Lecture 3

## Introduction of Group (群)

# What you will learn in Lecture 3

## 3.1 Introduction of Group (群)

## 3.2 Permutation Group (置換群)

## 3.1 Introduction of Group (群)

## Definition 3.1

A **group (群)** is an ordered pair  $(G, \circ)$ , where  $G$  is a nonempty set and  $\circ$  is a **binary operation** on  $G$  (i.e.  $G \times G \rightarrow G$ ) such that the following properties hold:

(G1) (associative law) For all  $a, b, c \in G$ ,  $a \circ (b \circ c) = (a \circ b) \circ c$ .

(G2) (existence of an identity) There exists identity element  $e \in G$  such that for all  $a \in G$ ,  $a \circ e = a = e \circ a$ .

(G3) (existence of an inverse) For all  $a \in G$ , there exists  $b \in G$  such that  $a \circ b = e = b \circ a$ .

\$(G4) (closure property) For all  $a, b \in G$ , the result of the operation,  $a \circ b$ , is also in  $G$ .

Thus, a group is a mathematical system  $(G, \circ)$  satisfying axioms (公理) G1, G2, G3 (and G4).

### Example 3.1

Consider  $\mathbb{Z}$ , the set of integers, together with the binary operation  $+$ , where  $+$  is the usual addition. We know that  $+$  is closed and associative on  $\mathbb{Z}$ . Now  $0 \in \mathbb{Z}$  and for all  $a \in \mathbb{Z}$ ,

$$a + 0 = a = 0 + a.$$

So 0 is an identity.

Also, for all  $a \in \mathbb{Z}$ ,  $-a \in \mathbb{Z}$  and  $a + (-a) = 0 = (-a) + a$ .

That is,  $-a$  is an inverse of  $a$ .

It now follows that  $(\mathbb{Z}, +)$  satisfies axioms G1 to G4, so  $(\mathbb{Z}, +)$  is a group.

As in Example 2.7, we can show that  $(\mathbb{Q}, +)$ ,  $(\mathbb{R}, +)$ ,  $(\mathbb{C}, +)$  are also groups, where  $+$  is the usual addition.

## 3.1 Introduction of Group (群)

### Theorem 3.1

Let  $(G, \circ)$  be a group.

- (i) There exists a **unique identity element**  $e \in G$  such that  $e \circ a = a = a \circ e$  for all  $a \in G$ .
- (ii) For all  $a \in G$ , there exists a **unique**  $b \in G$  such that  $a \circ b = e = b \circ a$ .

**Proof:** (i) Now  $(G, \circ)$  is group. Therefore, by axiom G2, there exists  $e \in G$  such that  $e * a = a = a * e$  for all  $a \in G$ . Because  $(G, \circ)$  is a mathematical system,  $e$  is unique by Theorem 2.1.

(ii) Let  $a \in G$ . By axiom G3, there exists  $b \in G$  such that  $a * b = e = b * a$ . Suppose there exists  $c \in G$  such that  $a * c = e = c * a$ . We show that  $b = c$ .

$$\begin{aligned} b &= b * e \\ &= b * (a * c) \text{ (substituting } e = a * c) \\ &= (b * a) * c \text{ (using the associativity of } *) \\ &= e * c \text{ (because } b * a = e) \\ &= c. \end{aligned}$$

2019/6/19 Thus,  $b$  is unique.

### Definition 3.2

Let  $(G, \circ)$  be a group. If for all  $a, b \in G$ ,

$$a \circ b = b \circ a$$

then  $(G, \circ)$  is called **commutative group (可換群)** or **Abelian group (アーベル群)**. A group  $(G, \circ)$  is called **noncommutative** if it is **not commutative**.

## 3.1 Introduction of Group (群)

### Example 3.2

Consider the group  $(\mathbb{Z}, +)$  of Example 2.7. Because  $a + b = b + a$  for all  $a, b \in \mathbb{Z}$ , it follows that  $+$  is commutative. Hence,  $(\mathbb{Z}, +)$  is a commutative group.

Similarly,  $(\mathbb{Q}, +)$ ,  $(\mathbb{R}, +)$ ,  $(\mathbb{C}, +)$ ,  $(\mathbb{Q} \setminus \{0\}, \cdot)$ ,  $(\mathbb{R} \setminus \{0\}, \cdot)$ ,  $(\mathbb{C} \setminus \{0\}, \cdot)$  are also commutative groups, where  $+$  is the usual addition and  $\cdot$  is the usual multiplication.



## 3.1 Introduction of Group (群)

## Cayley table

It is often convenient to describe a group in terms of an addition or multiplication table. Such a table is called a *Cayley table*.

### Example 3.3

The integers mod  $n$  form a group under addition modulo  $n$ . Consider  $\mathbb{Z}_5$ , consisting of the equivalence classes of the integers 0, 1, 2, 3, and 4. We define the group operation on  $\mathbb{Z}_5$  by modular addition.

We write the binary operation on the group additively; that is, we write  $m + n$ . The element 0 is the identity of the group and each element in  $\mathbb{Z}_5$  has an inverse. For instance,  $2 + 3 = 3 + 2 = 0$ . Table 3.1 is a Cayley table for  $\mathbb{Z}_5$ . We can see  $\mathbb{Z}_5$  is a group under the binary operation of addition mod  $n$ .

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Table 3.1

### Definition 3.3

A group  $(G, \circ)$  is called a **finite group (有限群)** if  $G$  has **only a finite number of elements**. The **order (位数)** of a group  $(G, \circ)$ , which is written as  $|G|$ , is **the number of elements of  $G$** .

### Definition 3.4

A group with **an infinite number of elements** is called an **infinite group (無限群)**.

### \*Definition 3.5

A **semigroup (半群)** is an ordered pair  $(M, \circ)$ , where  $M$  is a nonempty set and  $\circ$  is an associative binary operation on  $M$ .

Thus, a semigroup is a mathematical system with one binary operation such that the binary operation is associative.

### Remark

For any group  $(G, \circ)$ , the binary operation  $\circ$  is associative. Therefore, every group  $(G, \circ)$  is a semigroup.

Notice: \* mark is optional study material. It will be not included in middle and final examinations.

### \*Theorem 3.2

A semigroup  $(M, \circ)$  is a **group** if and only if

- (i) there exists  $e \in M$  such that  $e \circ a = a$  for all  $a \in M$ , (i.e.,  $e$  is a **left identity**),
- (ii) for all  $a \in M$  there exists  $b \in M$  such that  $b \circ a = e$ , (i.e., every element has a left inverse).

## 3.2 Permutation Group (置換群)

**Definition 3.6**

For any **nonempty set**  $S$ , a **one-to-one** and **onto** mapping  $\pi: S \rightarrow S$  is called a **permutation (置換)** of  $S$ .

**Example 3.4**

- (i) Let  $S$  be a nonempty set. Define  $\pi: S \rightarrow S$  by  $\pi(x) = x$  for all  $x \in S$ . Then  $\pi$  is one-one function of  $S$  onto  $S$ . Thus,  $\pi$  is a permutation of  $S$ . Note that  $\pi$  is called the identity permutations and is, usually, denoted by  $i_S$  or  $e$ .
- (ii) Let  $S = \{a, b, c\}$ . Define  $\alpha: S \rightarrow S$  such that  $\alpha(a) = b, \alpha(b) = a$ , and  $\alpha(c) = c$ . By the definition of  $\alpha$  it follows that  $\alpha$  is one-one function of  $S$  onto  $S$ . Thus,  $\alpha$  is a permutation of  $S$ .
- (iii) Consider  $\mathbb{R}$ , the set of real numbers. Define  $\alpha: \mathbb{R} \rightarrow \mathbb{R}$  by  $\alpha(x) = 3x + 5$  for all  $x \in \mathbb{R}$ . It can be shown that  $\alpha$  is a one-one function of  $\mathbb{R}$  onto  $\mathbb{R}$ . Thus,  $\alpha$  is a permutation of  $\mathbb{R}$ .  
Similarly, if  $\beta: \mathbb{R} \rightarrow \mathbb{R}$  by  $\beta(x) = x^3$  for all  $x \in \mathbb{R}$ . It can be shown that  $\beta$  is a one-one function of  $\mathbb{R}$  onto  $\mathbb{R}$ . Thus,  $\beta$  is a permutation of  $\mathbb{R}$ .

### Definition 3.7

A group  $(G, \circ)$  is called a **permutation group (置換群)** on a **nonempty set  $S$**  if the elements of  $G$  are permutations of  $S$  and the operation  $\circ$  is the composition of two functions.

### Example 3.5

Let  $S = \{1, 2\}$ . Define  $\alpha : S \rightarrow S$  such that  $\alpha(1) = 1, \alpha(2) = 2$ .

Then  $\alpha$  is a one-one function of  $S$  onto  $S$ , so  $\alpha$  is a permutation of  $S$ .

Next define  $\beta : S \rightarrow S$  such that  $\beta(1) = 2$  and  $\beta(2) = 1$ .

Then  $\beta$  is a one-one function of  $S$  onto  $S$ , so  $\beta$  is a permutation of  $S$ .

Let  $G = \{\alpha, \beta\}$ . Then  $(G, \circ)$  is a group, where  $\circ$  is the composition of functions.

Note that on this set  $S$ ,  $\alpha$  and  $\beta$  are the only permutations on  $S$ .

Moreover,  $\alpha$  is the identity permutation and  $\beta^{-1} = \beta$ .

Let  $I_n = \{1, 2, \dots, n\}$ ,  $n \geq 1$ . Let  $\pi$  be a permutation on  $I_n$ . Then

$$\pi = \{(1, \pi(1)), (2, \pi(2)), \dots, (n, \pi(n))\}.$$

Recall that a function  $f : S \rightarrow S$  is a subset of  $S \times S$ . By introducing two-row notation, we have

$$\pi = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \pi(1) & \pi(2) & \pi(3) & \cdots & \pi(n) \end{pmatrix}$$

### Example 3.6

(1) Let  $n = 4$  and  $\pi$  be the permutation on  $I_4$  defined by  $\pi(1) = 2$ ,  $\pi(2) = 4$ ,  $\pi(3) = 3$ , and  $\pi(4) = 1$ . Then using the two-row notation we can write

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ \pi(1) & \pi(2) & \pi(3) & \pi(4) \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$$



(2) Let  $n = 7$  and  $\pi$  and  $\sigma$  be two permutations on  $I_7$  defined by

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 3 & 4 & 6 & 7 & 2 & 5 \end{pmatrix}$$

and

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 5 & 3 & 1 & 7 & 6 & 4 \end{pmatrix}$$

Let us compute  $\pi \circ \sigma$ . Now by the definition of the composition of functions

$$(\pi \circ \sigma)(i) = \pi(\sigma(i))$$

for all  $i \in I_7$ . Thus,

$$(\pi \circ \sigma)(1) = \pi(\sigma(1)) = \pi(2) = 3$$

$$(\pi \circ \sigma)(2) = \pi(\sigma(2)) = \pi(5) = 7$$

and so on.

## 3.2 Permutation Group (置換群)

## Permutation group

From this, it is clear that when determining, say,  $(\pi \circ \sigma)(1)$ , we start with  $\sigma$  and finish with  $\pi$  and read as follows: 1 goes to 2 (under  $\sigma$ ) and 2 goes to 3 (under  $\pi$ ), so 1 goes to 3 (under  $\pi \circ \sigma$ ).

We can exhibit this in the following form:

$$\begin{array}{ll} 1 \xrightarrow{\sigma} 2 \xrightarrow{\pi} 3 & 1 \xrightarrow{\pi \circ \sigma} 3 \\ 2 \xrightarrow{\sigma} 5 \xrightarrow{\pi} 7 & 2 \xrightarrow{\pi \circ \sigma} 7 \\ 3 \xrightarrow{\sigma} 3 \xrightarrow{\pi} 4 & 3 \xrightarrow{\pi \circ \sigma} 4 \\ 4 \xrightarrow{\sigma} 1 \xrightarrow{\pi} 1 & 4 \xrightarrow{\pi \circ \sigma} 1 \\ 5 \xrightarrow{\sigma} 7 \xrightarrow{\pi} 5 & 5 \xrightarrow{\pi \circ \sigma} 5 \\ 6 \xrightarrow{\sigma} 6 \xrightarrow{\pi} 2 & 6 \xrightarrow{\pi \circ \sigma} 2 \\ 7 \xrightarrow{\sigma} 4 \xrightarrow{\pi} 6 & 7 \xrightarrow{\pi \circ \sigma} 6. \end{array}$$

Thus,

$$\pi \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 7 & 4 & 1 & 5 & 2 & 6 \end{pmatrix}$$

**Example 3.7**

In this example, we describe  $S_3$ , i.e., the set of all permutations on  $I_3 = \{1, 2, 3\}$ .

From equilateral triangle example in Lecture 2, we know that the number of one-to-one functions of  $I_3$  onto  $I_3$  is  $3! = 6$ . Thus,  $|S_3| = 6$ . Let  $e$  denote the identity permutation on  $I_3$ , i.e.,

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

Let  $\alpha$  be a nonidentity permutation on  $I_3$ . Let us see some of the choices for  $\alpha$ .

Suppose  $\alpha(1) = 1$ . If  $\alpha(2) = 2$ , then we must have  $\alpha(3) = 3$  because  $\alpha$  is a permutation.

In this case, we see that  $\alpha = e$ , a contradiction. Thus, we must have  $\alpha(2) = 3$  and  $\alpha(3) = 2$ , i.e., we define this  $\alpha$  as

$$\alpha_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

In a similar manner, we can show that the other four permutations on  $I_3$  are

$$\alpha_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad \alpha_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \quad \alpha_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \alpha_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

For closure property, it can check that, for example

$$\alpha_2 \alpha_4 = \alpha_1$$

Hence, we can write

$$S_3 = \{e, \alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5\}$$

### Theorem 3.3

- (i)  $(S_n, \circ)$  is a **group** for any positive integer  $n \geq 1$ .
- (ii) If  $n \geq 3$ , then  $(S_n, \circ)$  is **noncommutative**.
- (iii)  $|S_n| = n!$

### Definition 3.8

The **symmetric group** (对称群)  $S_n$  is a group with  $n!$  elements, where the binary operation is the composition of maps.

The group  $(S_n, \circ)$  is called the **symmetric group** on  $I_n$ .

## Definition 3.9

Let  $\pi$  be an element of  $S_n$ . Then  $\pi$  is called a  $k$ -cycle, written as  $(i_1 \ i_2 \ \cdots \ i_k)$ , if

$$\pi = \begin{pmatrix} i_1 & i_2 & \cdots & i_{k-1} & i_k \\ i_2 & i_3 & \cdots & i_k & i_1 \end{pmatrix},$$

i.e.,  $\pi(i_j) = i_{j+1}, j = 1, 2, \dots, k-1, \pi(i_k) = i_1$ , and  $\pi(a) = a$  for any other element of  $I_n$ .

**Notice:** When  $k = 2$ , a  $k$ -cycle is called a **transposition (互換)**.

For **example**, consider the cycle notation  $(3 \ 4)$  for  $\pi \in S_4$

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ \pi(1) & \pi(2) & \pi(3) & \pi(4) \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix} = (3 \ 4)$$



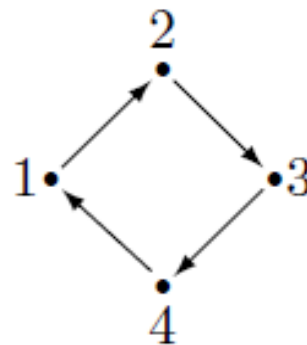
### Example 3.8

Consider the permutation

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

It permutes the elements 1, 2, 3, and 4 cyclically, then we have the cycle notation  $\alpha = (1\ 2\ 3\ 4)$ .

And the following picture suggests:



## Theorem 3.4

Any permutation (置換)  $\pi$  of  $S_n$  can be expressed as a product of disjoint cycles.

## Example 3.9

Let

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 3 & 1 & 5 & 2 \end{pmatrix}$$

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 1 & 5 & 6 & 4 \end{pmatrix}$$

Using cycle notation, we can write

$$\sigma = (1\ 6\ 2\ 4)$$

$$\tau = (1\ 3)(4\ 5\ 6)$$

$$\sigma\tau = (1\ 3\ 6)(2\ 4\ 5)$$

$$\tau\sigma = (1\ 4\ 3)(2\ 5\ 6)$$

### Corollary 3.1

Let  $n \geq 2$ . Any permutation (置換)  $\pi$  of  $S_n$  can be expressed as a product of transpositions (互換).

The cycle  $(i_1 \ i_2 \ \cdots \ i_k) = (i_1 \ i_n)(i_1 \ i_{n-1}) \cdots (i_1 \ i_3)(i_1 \ i_2)$

For example, the Fifteen Puzzle



<http://lorecioni.github.io/fifteen-puzzle-game/>

**Definition 3.10**

Let  $\pi \in S_n$ . If  $\pi$  is a product of an **even number** of transpositions, then  $\pi$  is called an **even permutation** (偶置換); otherwise  $\pi$  is called an **odd permutation** (奇置換).

**Corollary 3.2**

Let  $\pi \in S_n$  be a  $k$ -cycle. Then  $\pi$  is an **even permutation** if and only if  $k$  is **odd**.

**Proof.**

Let  $\pi = (1 \ 2 \ \cdots \ k)$ . Then  $\pi = (1 \ k) \circ (1 \ k-1) \circ \cdots \circ (1 \ 2)$ , i.e.,  $\pi$  is a product of  $k-1$  transposition. If  $\pi$  is an even permutation then  $k-1$  is even, so  $k$  is odd. On the other hand, if  $k$  is odd, then  $k-1$  is even, so  $\pi$  is an even permutation. This completes the proof.

# Review for Lecture 3

- Definition of Group (群)
- Commutative Group (可換群) or Abelian Group (アーベル群)
- Finite Group (有限群) and Infinite Group (無限群)
- Order (位数) of a group
- Permutation Group (置換群)
- Symmetry Group (対称群)
- $k$ -cycle & Transposition (互換)
- Even Permutation (偶置換) and Odd Permutation (奇置換)

# Assignment

Please Check <https://github.com/uoaworks/Applied-Algebra>

## References

- [1] Thomas W. Judson etc. Abstract Algebra Theory and Applications, 2018
- [2] D. S. Malik, John N. Mordeson, M.K. Sen, Introduction to Abstract Algebra, 2007
- [3] (おすすめ) 松本 眞, 代数系への入門, <http://www.math.sci.hiroshima-u.ac.jp/~m-mat/TEACH/daisu-nyumon2014.pdf>
- [4] Wikipedia
- [5] Materials from internet.

**Example 28.** If  $n = 3$ , we consider the set  $X = \{1, 2, 3\}$ . Since  $3! = 6$ , we have 6 permutations:

$$S_3 = \{\sigma_1 = (), \sigma_2 = (12), \sigma_3 = (13), \sigma_4 = (23), \sigma_5 = (123), \sigma_6 = (132)\}.$$

We compute the Cayley table of  $S_3$ .

	$()$	$(12)$	$(23)$	$(13)$	$(123)$	$(132)$
$()$	$()$	$(12)$	$(23)$	$(13)$	$(123)$	$(132)$
$(12)$	$(12)$	$()$	$(123)$	$(132)$	$(23)$	$(13)$
$(23)$	$(23)$	$(132)$	$()$	$(123)$	$(13)$	$(12)$
$(13)$	$(13)$	$(123)$	$(132)$	$()$	$(12)$	$(23)$
$(123)$	$(123)$	$(13)$	$(12)$	$(23)$	$(132)$	$()$
$(132)$	$(132)$	$(23)$	$(13)$	$(12)$	$()$	$(123)$