



Lecture **2**

Introduction of Group

What you will learn in Lecture 2

2.1 Binary Operations (二項演算)

2.2 Symmetries (対称性)

2.3 Introduction of Group (群)

2.4 Permutation Group (置換群)

2.1 Binary Operations (二項演算)

Definition 2.1

A **binary operation** (or *law of composition*) on a **nonempty set** G is a function $G \times G \rightarrow G$.

It implies “closure” property.

For example, $+$ is a binary operation on \mathbb{Z} which assigns 3 to the pair $(2, 1)$ (Notice: here all of the elements 1, 2, 3 are in set G).

Namely, for any ordered pair $(a, b) \in G \times G$ of elements $a, b \in G$, a binary operation \circ assigns the third element $a \circ b$ of G .

If \circ is a **binary operation** on G , we write $a \circ b$ as the element of operation result (the composition of a and b), where $a, b \in G$

Since the image of \circ is a **subset** of G , we say **the set G is closed under \circ** .

Example 2.1

Is $+$ (addition) a binary operation on \mathbb{Z} ?

Example 2.2

Is $-$ (subtraction) a binary operation on \mathbb{N} ?

Definition 2.2

A **mathematical system** is an ordered $(n + 1)$ -tuple $(G, \circ_1, \dots, \circ_n)$, where G is a nonempty set and \circ_i is a binary operation on G , where $i = 1, 2, \dots, n$. G is called the underlying set of the system.

Definition 2.3

Let (G, \circ) be a mathematical system with only one binary operation. Then

- (i) \circ is called **associative** if for all $x, y, z \in G$, $x \circ (y \circ z) = (x \circ y) \circ z$.
- (ii) \circ is called **commutative** if for all $x, y \in G$, $x \circ y = y \circ x$.

Example 2.3

Consider the mathematical system $(\mathbb{Z}, +)$.

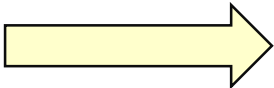
2.1 Binary Operations (二項演算)

operation table

A convenient way to define a **binary operation** on a finite set G is by means of an **operation table**.

For example, let $G = \{a, b, c\}$. Define \circ on G by the following operation table.

(i th entry on the left) \circ (j th entry on the top)
= (entry in the i th row and j th column of the table body)

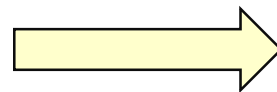
\circ	a	b	c		\circ	a	b	c
a	$a \circ a$	$a \circ b$	$a \circ c$	For example 	a	c	b	a
b	$b \circ a$	$b \circ b$	$b \circ c$		b	a	a	a
c	$c \circ a$	$c \circ b$	$c \circ c$		c	b	b	b

Notice: here **all of the elements** $a \circ a, a \circ b, a \circ c, b \circ a, b \circ b, b \circ c, c \circ a, c \circ b, c \circ c \in G$

2.1 Binary Operations (二項演算)

\circ	a	b	c
a	$a \circ a$	$a \circ b$	$a \circ c$
b	$b \circ a$	$b \circ b$	$b \circ c$
c	$c \circ a$	$c \circ b$	$c \circ c$

For example



\circ	a	b	c
a	c	b	a
b	a	a	a
c	b	b	b

Table 2.1

Example 2.4

Is the binary operation \circ in Table 2.1 commutative?

Definition 2.4

Let (G, \circ) be a mathematical system. An element $e \in G$ is called an **identity** of (G, \circ) if for all $x \in G$,

$$e \circ x = x = x \circ e.$$

Example 2.5

Let $G = \{e, a, b\}$. Define \circ on G by the following operation table

\circ	e	a	b
e	e	a	b
a	a	a	a
b	b	a	a

Theorem 2.1

An identity element (if it exists) of a mathematical system (G, \circ) is unique.

Proof.

2.1 Binary Operations (二項演算)

Example 1 of Binary Operation

The Integers mod n

The integers mod n have become indispensable in the theory and applications of algebra. In mathematics they are used in cryptography, coding theory, and the detection of errors in identification codes.

We have already seen that two integers a and b are equivalent mod n if n divides $a - b$. The integers mod n also **partition** \mathbb{Z} into n different equivalence classes $[\cdot]$; we will denote the entire set of these equivalence classes $[\cdot]$ by \mathbb{Z}_n .

For example, if we consider the equivalence relation established by the integers modulo 3, then we have corresponding partition sets of the integers

$$[0] = \{\dots, -3, 0, 3, 6, \dots\}$$

$$[1] = \{\dots, -2, 1, 4, 7, \dots\}$$

$$[2] = \{\dots, -1, 2, 5, 8, \dots\}$$

2.1 Binary Operations (二項演算)

Example 1 of Binary Operation

We can do arithmetic on \mathbb{Z}_n .

For two integers a and b , define **addition modulo n** to be $(a + b) \pmod{n}$; that is, the remainder when $a + b$ is divided by n .

Similarly, **multiplication modulo n** is defined as $(ab) \pmod{n}$, the remainder when ab is divided by n .

Example 2.6

The following examples illustrate integer arithmetic modulo n :

$$7 + 4 \equiv 1 \pmod{5}$$

$$7 \cdot 3 \equiv 1 \pmod{5}$$

$$3 + 5 \equiv 0 \pmod{8}$$

$$3 \cdot 5 \equiv 7 \pmod{8}$$

$$3 + 4 \equiv 7 \pmod{12}$$

$$3 \cdot 4 \equiv 0 \pmod{12}.$$

2.1 Binary Operations (二項演算)

Example 1 of Binary Operation

Most, but not all, of the usual laws of arithmetic hold for addition and multiplication in \mathbb{Z}_n .

Example 2.7

It is not necessarily true that there is a multiplicative inverse. Consider the multiplication operation table for \mathbb{Z}_8 in the following Table. Notice that 2, 4, and 6 do not have multiplicative inverses; that is, for $n = 2, 4$, or 6 , there is no integer k such that $kn \equiv 1 \pmod{8}$.

\cdot	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1



Notice: Never exist for $k \cdot 2 \equiv 1 \pmod{8}$

2.2 Symmetries (对称性)

2.2 Symmetries (対称性)

A **symmetry** of a geometric figure is a rearrangement of the figure **preserving** the arrangement of its **sides** (辺) and **vertices** (頂点) as well as its **distances** and **angles**.

A map from the plane to itself **preserving** the symmetry of an object is called a **rigid motion** (剛体運動).

For example, if we look at the rectangle in Figure 2.1, it is easy to see that a rotation of 180° or 360° returns a rectangle in the plane with the same orientation as the original **rectangle** (矩形) and the same relationship among the vertices.

However, a 90° rotation in either direction **cannot be** a symmetry unless the **rectangle** is a **square** (正方形).

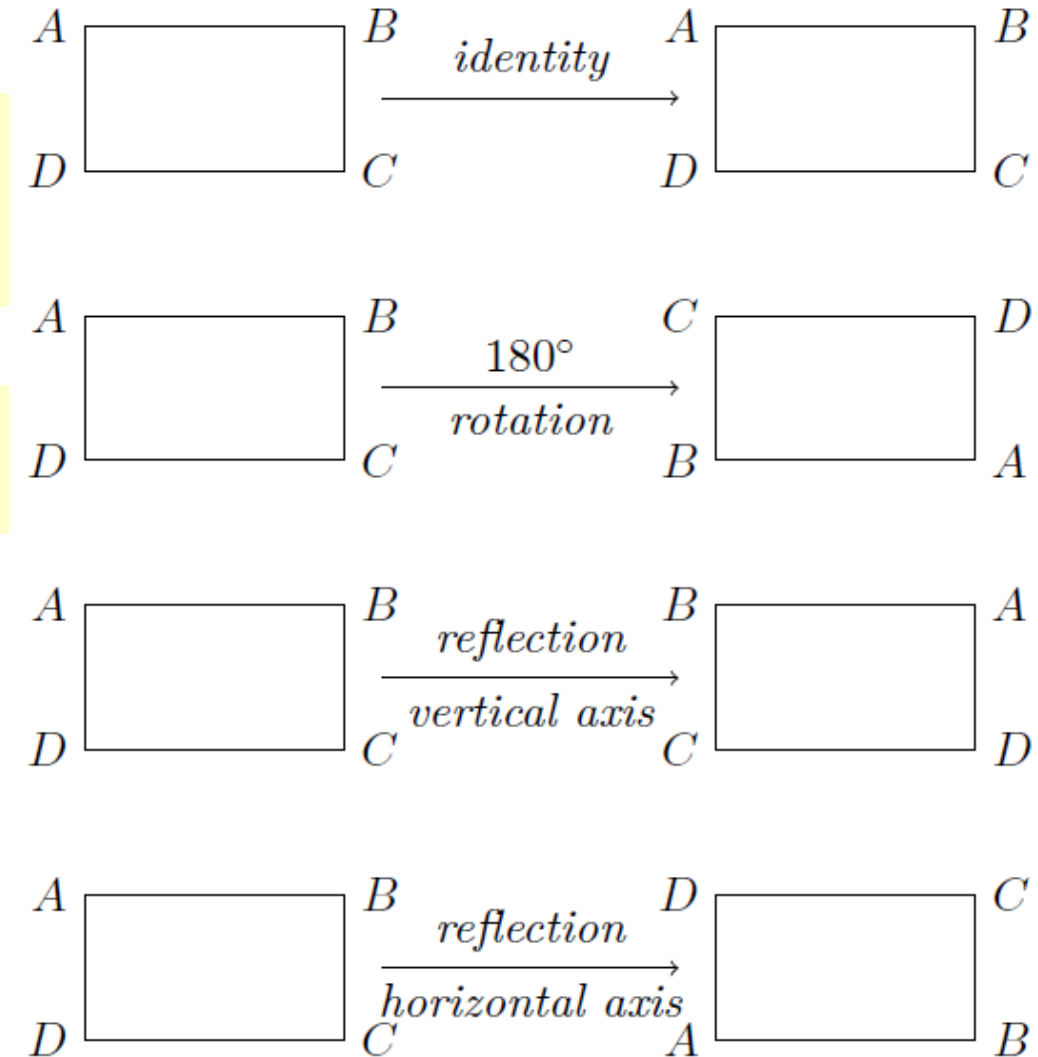
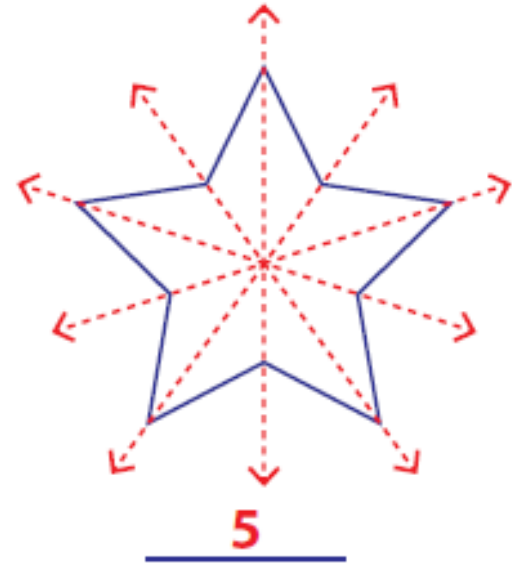
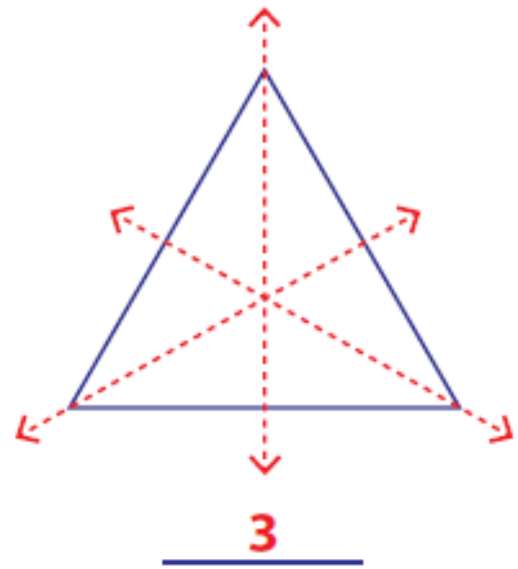
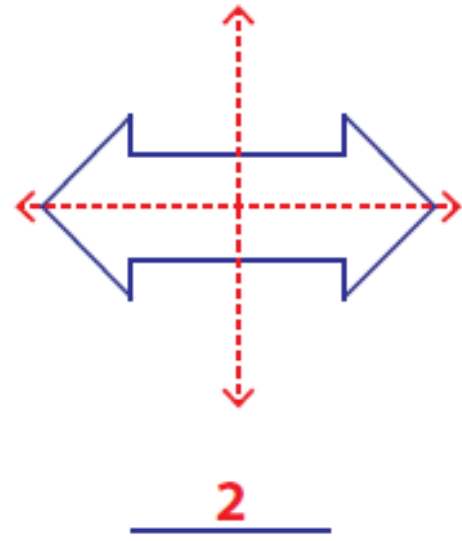
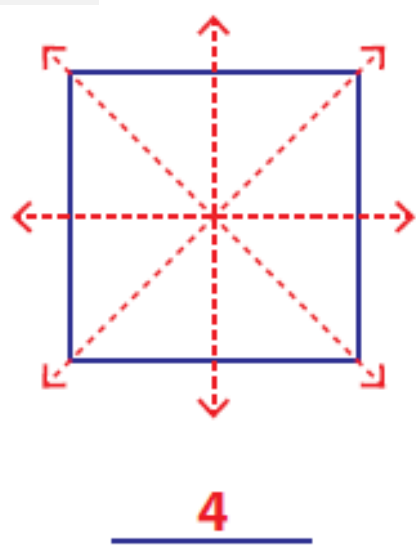
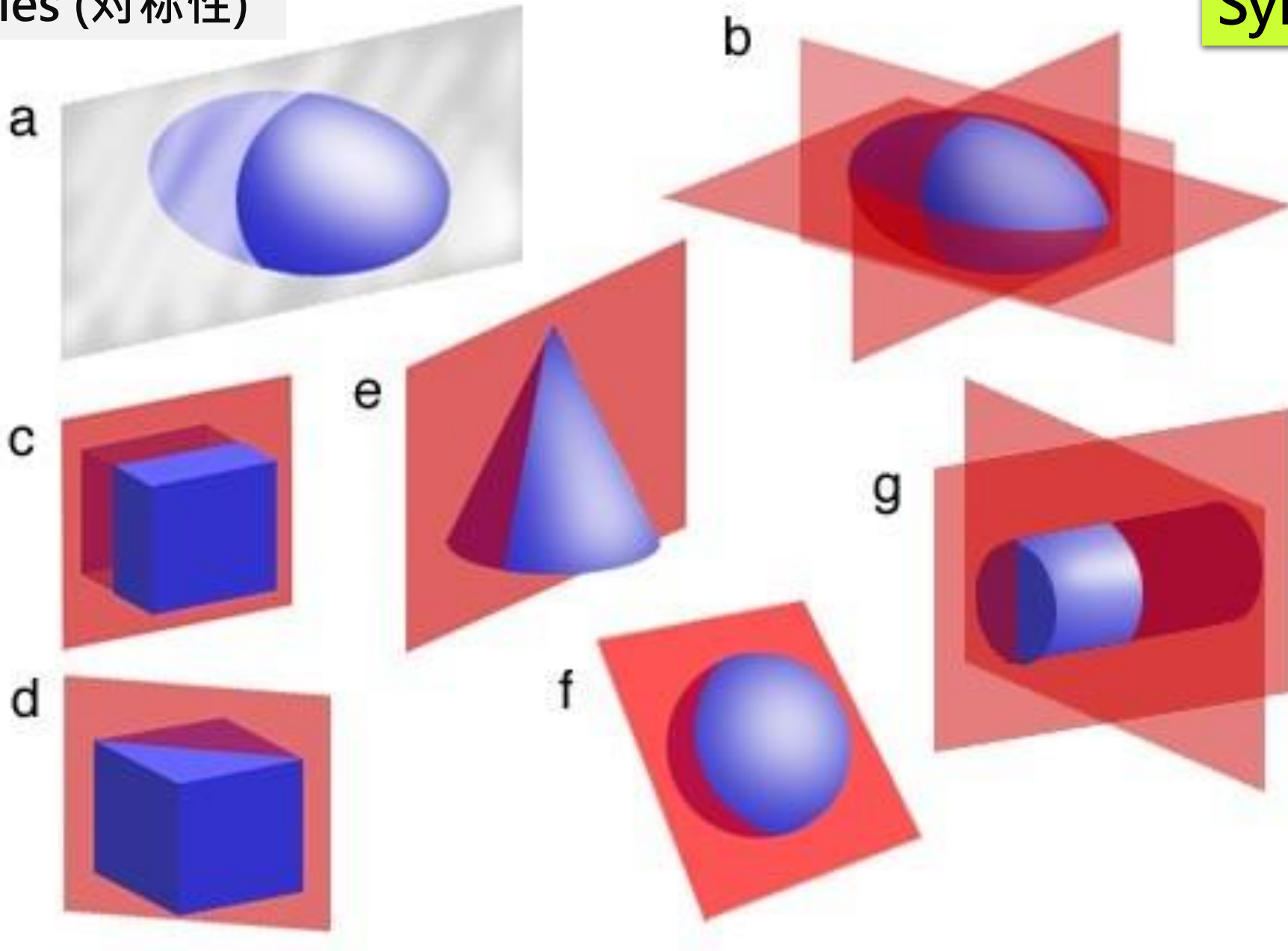


Figure 2.1 Rigid motions of a rectangle



2.2 Symmetries (对称性)

Symmetries



2.2 Symmetries (对称性)

Symmetries of equilateral triangle

Let us find the **symmetries** of the **equilateral triangle** $\triangle ABC$. To find a symmetry of $\triangle ABC$, we must first examine the **permutations of the vertices** A, B , and C and then ask if a permutation extends to a symmetry of the triangle.

Recall that a **permutation of a set S** is a **one-to-one and onto map $\pi: S \rightarrow S$** . The three vertices have $3! = 6$ permutations, so the triangle has **at most six symmetries**. (To see that there are six permutations, observe there are three different possibilities for the first vertex, and two for the second, and the remaining vertex is determined by the placement of the first two. So we have $3 \cdot 2 \cdot 1 = 3! = 6$ different arrangements.)

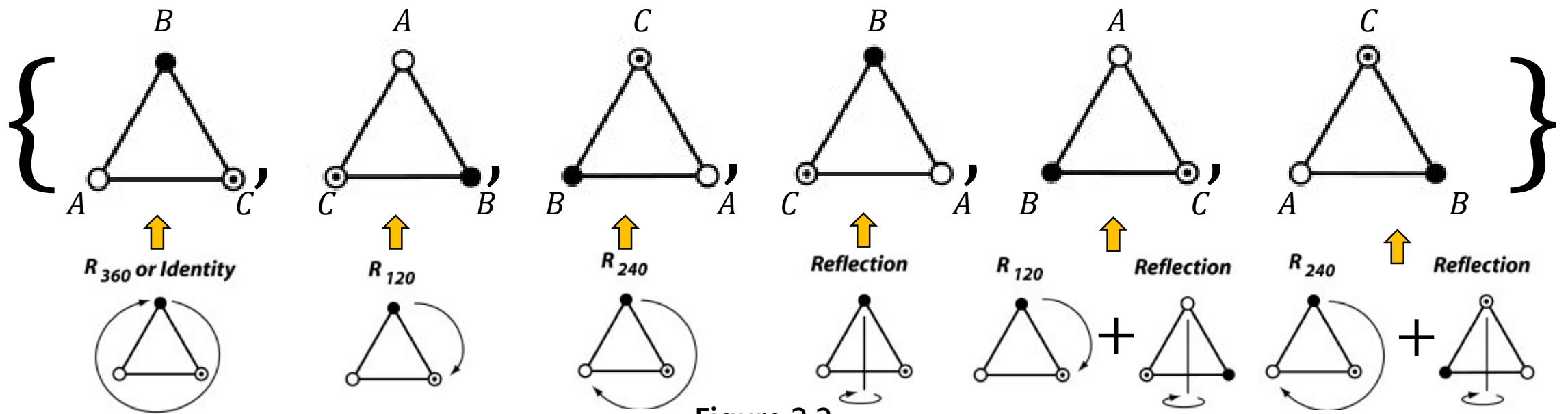


Figure 2.2

2.2 Symmetries (对称性)

To denote the **permutation** of the vertices of an equilateral triangle that sends **A to B, B to C, and C to A**, we write the array

$$\begin{pmatrix} A & B & C \\ \pi(A) & \pi(B) & \pi(C) \end{pmatrix} = \begin{pmatrix} A & B & C \\ B & C & A \end{pmatrix}$$

Notice that this particular permutation corresponds to the rigid motion of rotating the triangle by 120° in a clockwise direction.

In fact, every permutation gives rise to a symmetry of the triangle.

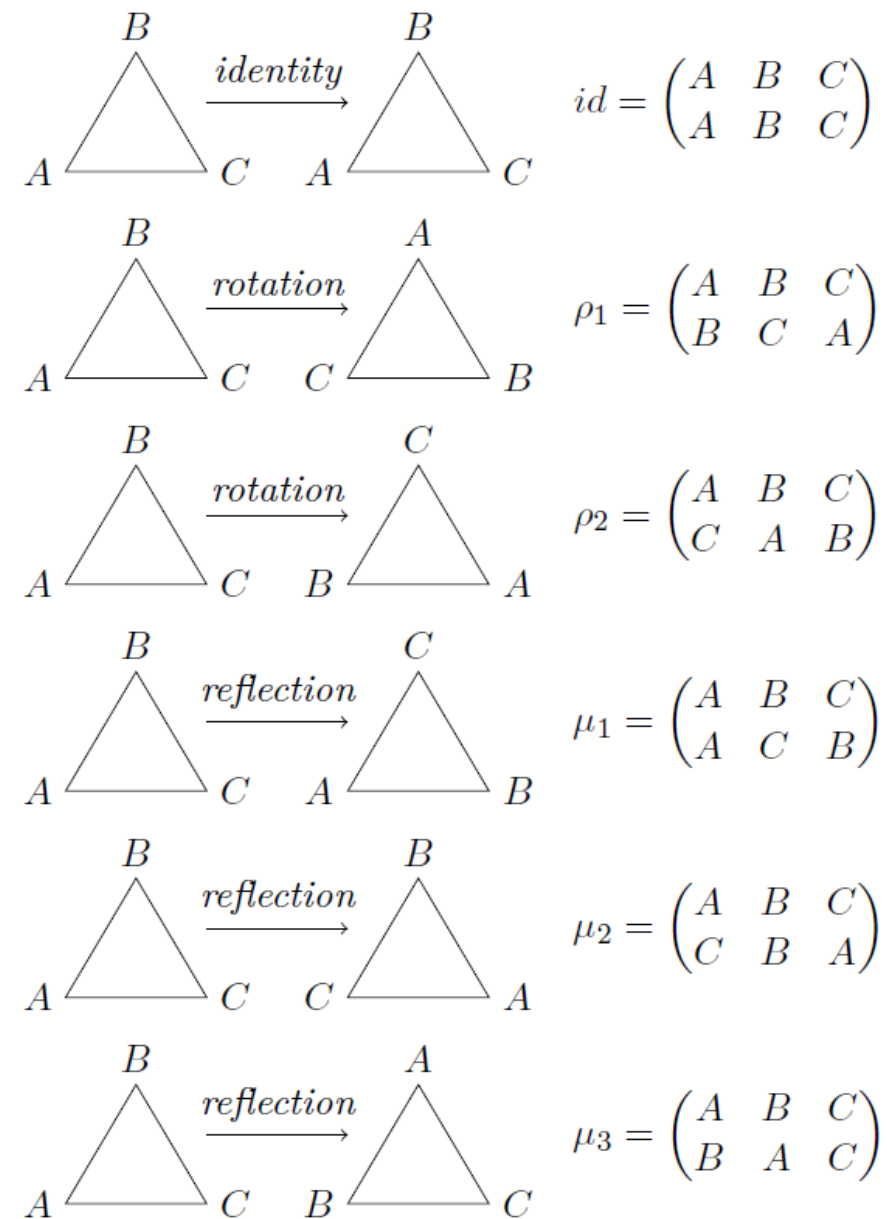


Figure 2.3 Symmetries of an equilateral triangle

A natural question to ask is what happens if one motion of the triangle $\triangle ABC$ is followed by another. Which symmetry is $\mu_1\rho_1$; that is, what happens when we do the permutation ρ_1 and then the permutation μ_1 ?

Remember that **we are composing functions** here. *Although we usually multiply left to right, we compose functions right to left.* We have

Notice: Compute From right ρ_1 to left μ_1

$$\begin{aligned}(\mu_1\rho_1)(A) &= \mu_1(\rho_1(A)) = \mu_1(B) = C \\(\mu_1\rho_1)(B) &= \mu_1(\rho_1(B)) = \mu_1(C) = B \\(\mu_1\rho_1)(C) &= \mu_1(\rho_1(C)) = \mu_1(A) = A.\end{aligned}$$

This is the same symmetry as μ_2 . Suppose we do these motions in the opposite order, ρ_1 then μ_1 . It is easy to determine that this is the same as the symmetry μ_3 ; hence, $\rho_1\mu_1 \neq \mu_1\rho_1$.

2.2 Symmetries (对称性)

An operation table for the symmetries of an equilateral triangle $\triangle ABC$ is given in Table 2.2.

\circ	id	ρ_1	ρ_2	μ_1	μ_2	μ_3
id	id	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	id	μ_3	μ_1	μ_2
ρ_2	ρ_2	id	ρ_1	μ_2	μ_3	μ_1
μ_1	μ_1	μ_2	μ_3	id	ρ_1	ρ_2
μ_2	μ_2	μ_3	μ_1	ρ_2	id	ρ_1
μ_3	μ_3	μ_1	μ_2	ρ_1	ρ_2	id

Table 2.2 Symmetries of an equilateral triangle

Notice that in the operation table for the symmetries of an equilateral triangle, for every motion α of the triangle, there is another motion β such that $\alpha \beta = \text{id}$; that is, **for every motion there is another motion that takes the triangle back to its original orientation.** It also tells us this is an binary operation.

Example 2 of Binary Operation

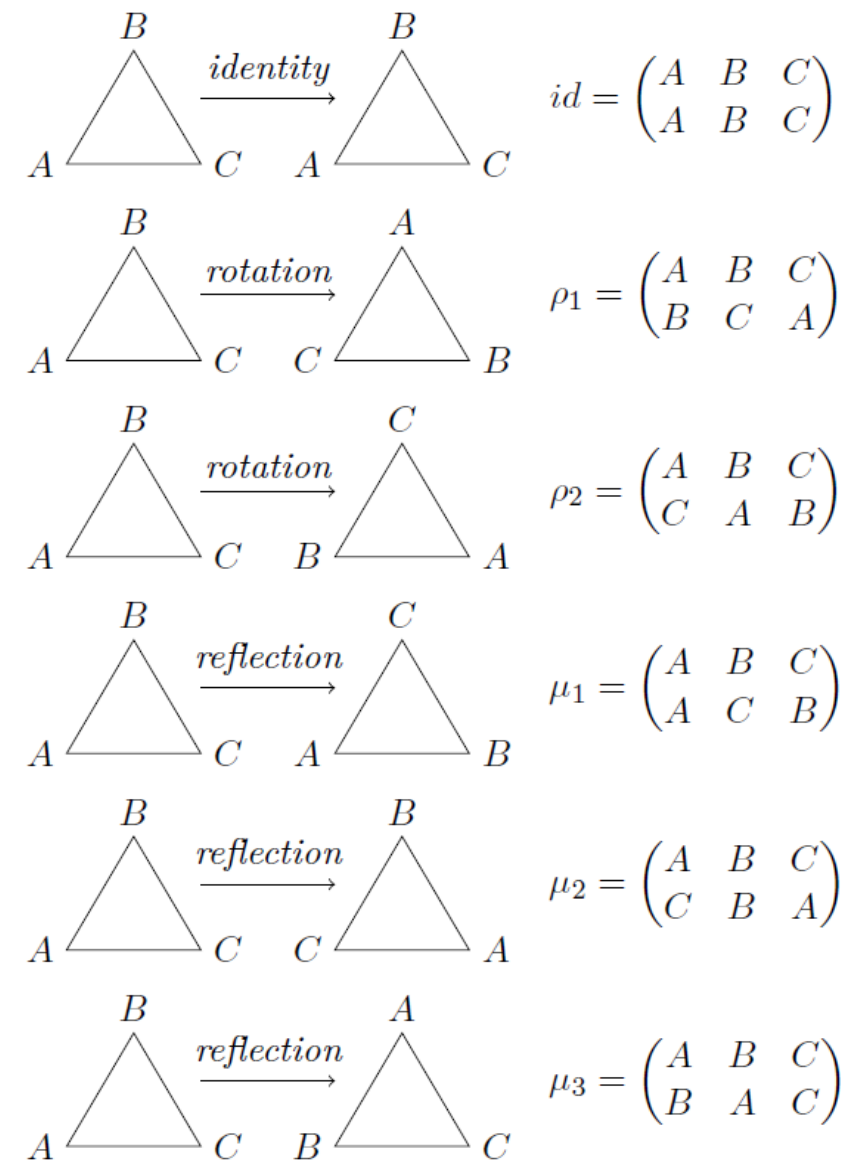


Figure 2.3 Symmetries of an equilateral triangle

2.3 Introduction of Group (群)

Definition 2.5

A **group** is an ordered pair (G, \circ) , where G is a **nonempty set** and \circ is a **binary operation** on 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**) 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 2.7

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.

2.3 Introduction of Group (群)

Theorem 2.2

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:

Definition 2.6

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**.

Example 2.8

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.

2.3 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 2.9

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 2.2 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 2.2

2.4 Permutation Group (置換群)

Definition 2.7

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 2.10

- (i) Let S be a nonempty set. Define $\pi: S \rightarrow S$ by $\pi(x) = x$ for all $x \in S$. Then π is one-one function of S onto S . Thus, π is a permutation of S . Note that π 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 α it follows that α is one-one function of S onto S . Thus, α 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 α is a one-one function of \mathbb{R} onto \mathbb{R} . Thus, α 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 β is a one-one function of \mathbb{R} onto \mathbb{R} . Thus, β is a permutation of \mathbb{R} .

Definition 2.8

A group (G, \circ) is called a **permutation group** 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 2.11

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

Then α is a one-one function of S onto S , so α is a permutation of S . Next define $\beta : S \rightarrow S$ such that $\beta(1) = 2$ and $\beta(2) = 1$.

Then β is a one-one function of S onto S , so β is a permutation of S .

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

Note that on this set S , α and β are the only permutations on S .

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

Let $I_n = \{1, 2, \dots, n\}$, $n \geq 1$. Let π 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 2.12

Review for Lecture 2

- Binary Operations (二項演算)
- Symmetries (対称性)
- Rigid Motion (剛体運動)
- Permutations (置換) of equilateral triangle $\triangle ABC$
- Definition of (群)
- Permutation Group (置換群)

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.