TEST

Lecture 2

Binary Operation & Symmetries

What you will learn in Lecture 2

2.1 Binary Operations (二項演算)

2.2 Symmetries (对称性)

2.1 Binary Operations (二項演算)

2.1 Binary Operations (二項演算)

binary operation

Definition 2.1

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

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 $\mathbb{Z}$?

$\mathbb{Z}$ is closed under $+$ since if we add two integers we obtain an integer.

Example 2.2

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

Since $2, 5 \in \mathbb{N}$ and $2 - 5 = -3 \notin \mathbb{N}$, we see that $-$ (subtraction) is NOT a binary operation of $\mathbb{N}$ and we say that $\mathbb{N}$ is NOT closed under $-$.

2.1 Binary Operations (二項演算)

mathematical system, associative, commutative

Definition 2.2

A **mathematical system** is an ordered $(n+1)$-tuple $(G, \circ_1, \ldots, \circ_n)$, where G is a nonempty set and $\circ_i$ is a binary operation on G, where $i = 1, 2, \ldots, n$. 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 $(\mathbb{Z}, +)$.

Since addition of integers is both associative and commutative, then the binary operation $+$ is both associative and commutative.

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 ith row and jth column of the table body)

$\circ$	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 $\Rightarrow$

$\circ$	a	b	c
a	c	b	a
b	a	a	a
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** ?

No. Because $a \circ b \neq b \circ a$.

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

We note that $e \circ a = a = a \circ e$, $e \circ b = b = b \circ e$ and $e \circ e = e = e \circ e$. Thus, e is an identity of $(G,\circ)$

Identity in mathematical system

Theorem 2.1

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

Proof.

Suppose e_1, e_2 be identities of $(G,\circ)$. Since e_1 is identity, $e_1 * a = a$ for all $a \in G$.

Substituting $e_2$for a, we get

$$e_1 * e_2 = e_2 \qquad (2.1)$$

Now e_2 is identity and so $a * e_2 = a$ for all $a \in S$.

Substituting e_1 for a we get

$$e_1 * e_2 = e_1 \qquad (2.2)$$

From Eqs. (2.1) and (2.2), we get $e_1 = e_2$.

Hence, an identity element (if it exists) is unique.

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

$$[0] = \{\dots, -3, 0, 3, 6, \dots\}$$
$$[1] = \{\dots, -2, 1, 4, 7, \dots\}$$
$$[2] = \{\dots, -1, 2, 5, 8, \dots\}$$

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:

$$7 + 4 \equiv 1 \pmod{5} \qquad 7 \cdot 3 = 1 \pmod{5}$$

$$3 + 5 \equiv 0 \pmod{8} \qquad 3 \cdot 5 \equiv 7 \pmod{8}$$

$$3 + 4 \equiv 7 \pmod{12} \qquad 3 \cdot 4 \equiv 0 \pmod{12}.$$

In particular, notice that it is possible that the product of two nonzero numbers modulo n can be equivalent to 0 modulo n.

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 $n = 2, 4, \text{or } 6$, 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 (对称性)

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)**.

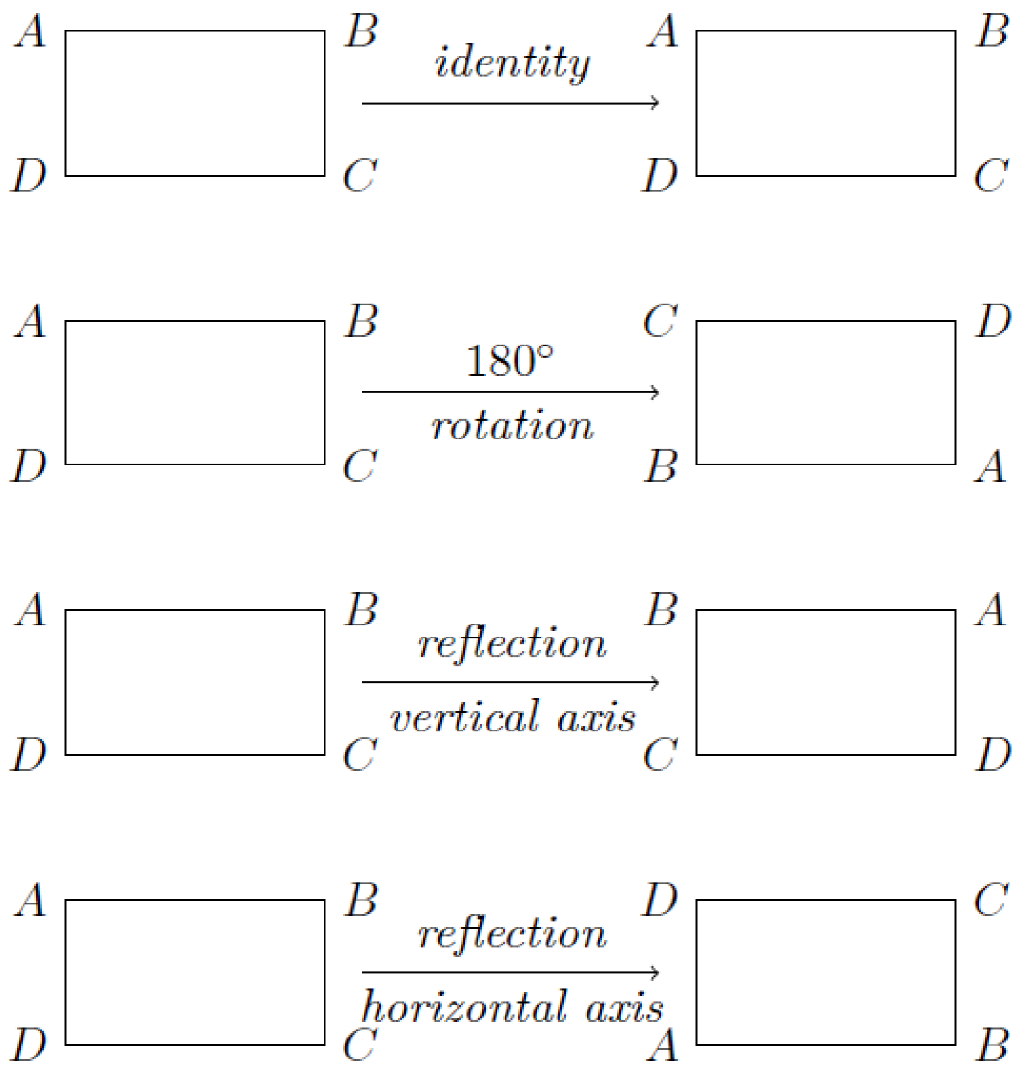
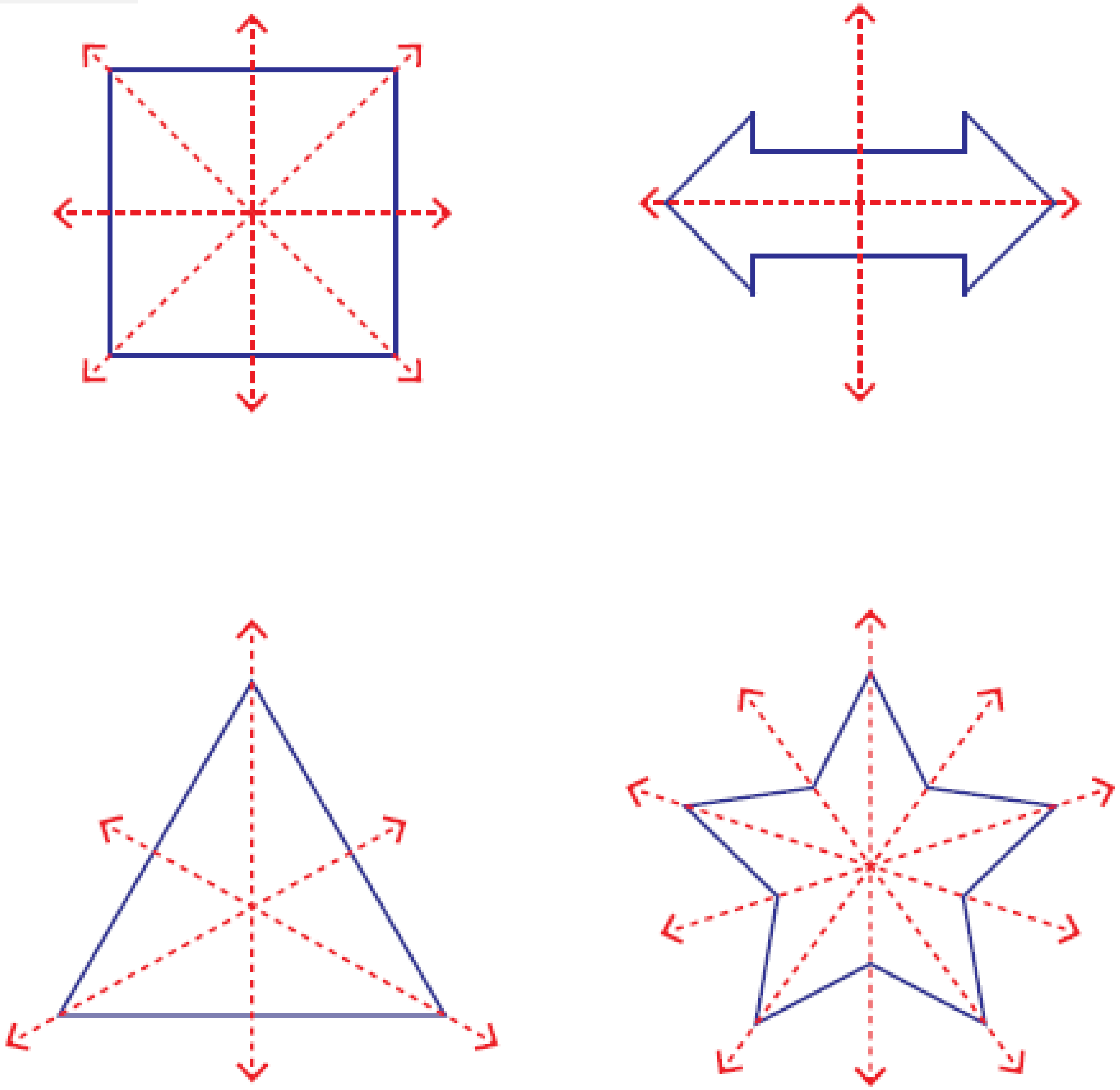


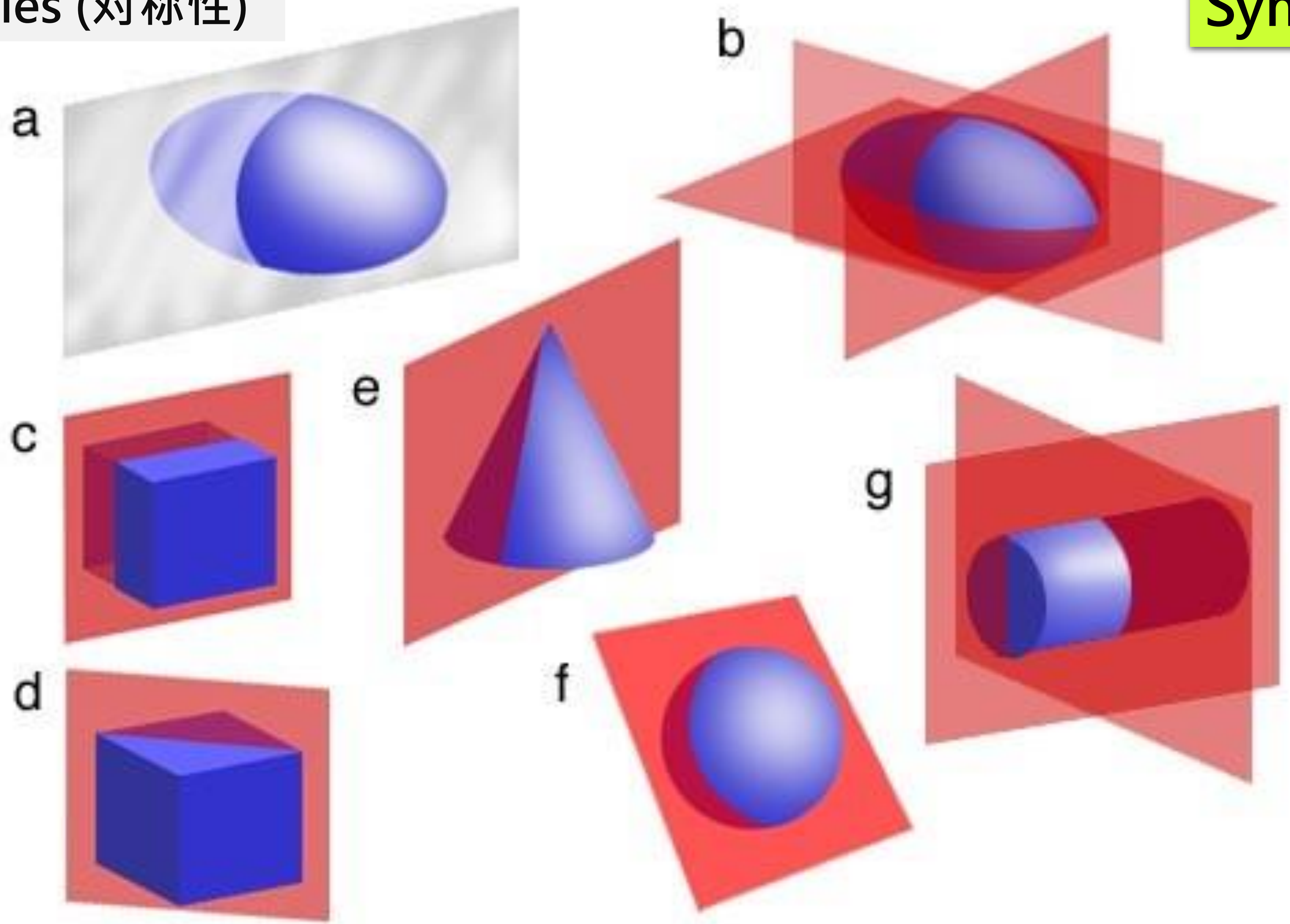
Figure 2.1 Rigid motions of a rectangle

2.2 Symmetries (对称性)



2.2 Symmetries (对称性)

Symmetries



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 $\pi: S \to S$. 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.)

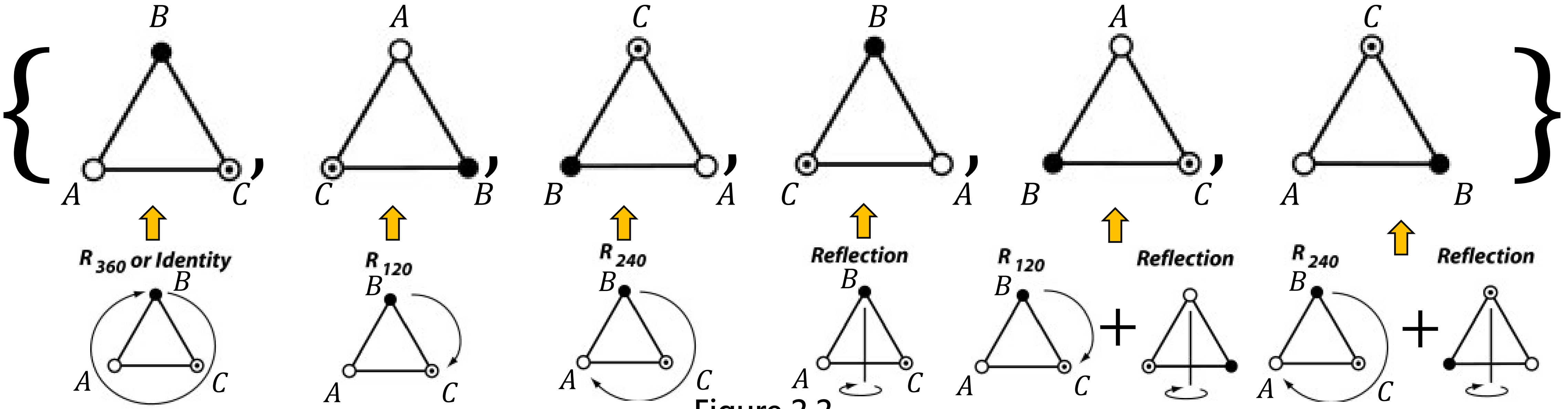


Figure 2.2

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.

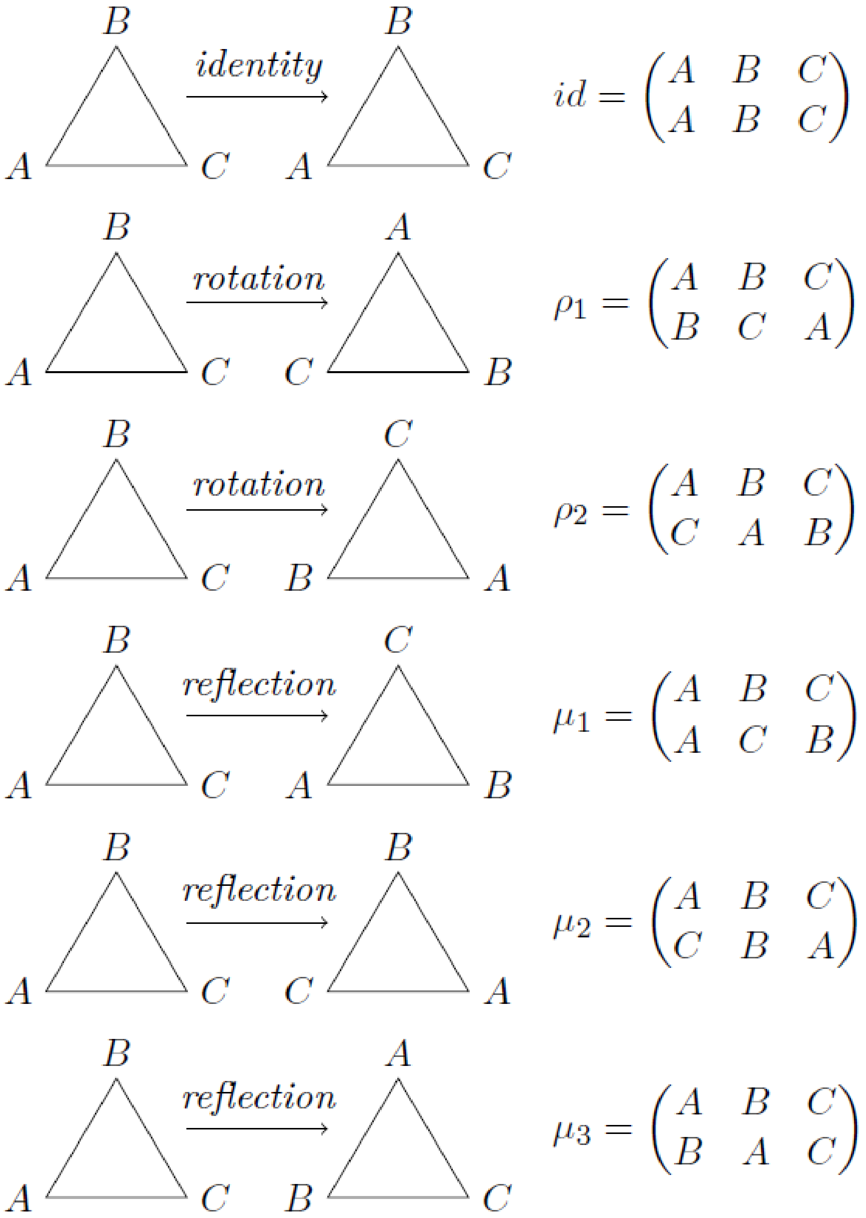


Figure 2.3 Symmetries of an equilateral triangle

Example 2 of Binary Operation

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, $\rho_1\mu_1 \neq \mu_1\rho_1$.

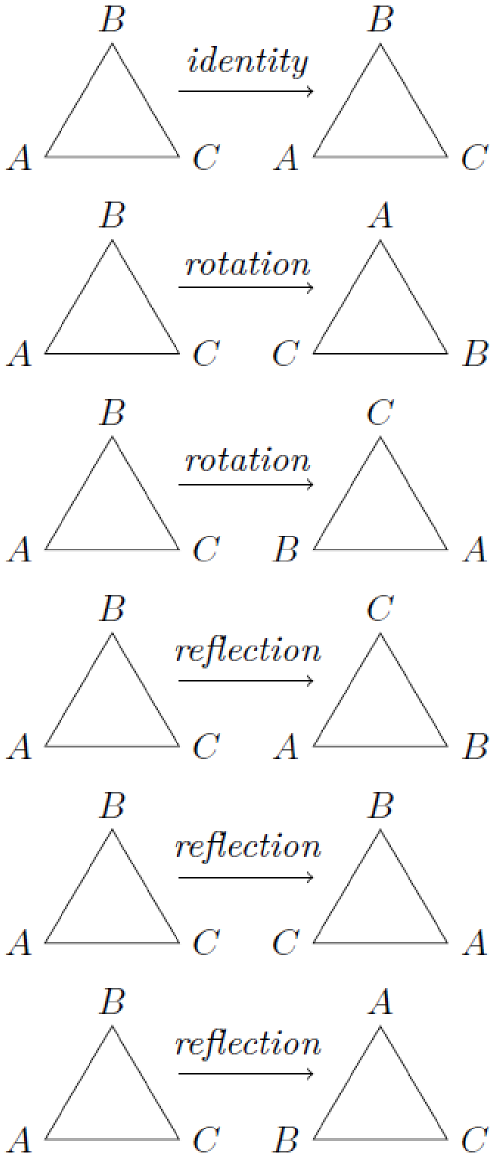
Example 2 of Binary Operation

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.



$$id = \begin{pmatrix} A & B & C \\ A & B & C \end{pmatrix}$$

$$\rho_1 = \begin{pmatrix} A & B & C \\ B & C & A \end{pmatrix}$$

$$\rho_2 = \begin{pmatrix} A & B & C \\ C & A & B \end{pmatrix}$$

$$\mu_1 = \begin{pmatrix} A & B & C \\ A & C & B \end{pmatrix}$$

$$\mu_2 = \begin{pmatrix} A & B & C \\ C & B & A \end{pmatrix}$$

$$\mu_3 = \begin{pmatrix} A & B & C \\ B & A & C \end{pmatrix}$$

Figure 2.3 Symmetries of an equilateral triangle

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 $\triangle ABC$

Assignment

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

References

[1] Thomas W. Judson etc. Abstract Algebra Theory and Applications, 2018

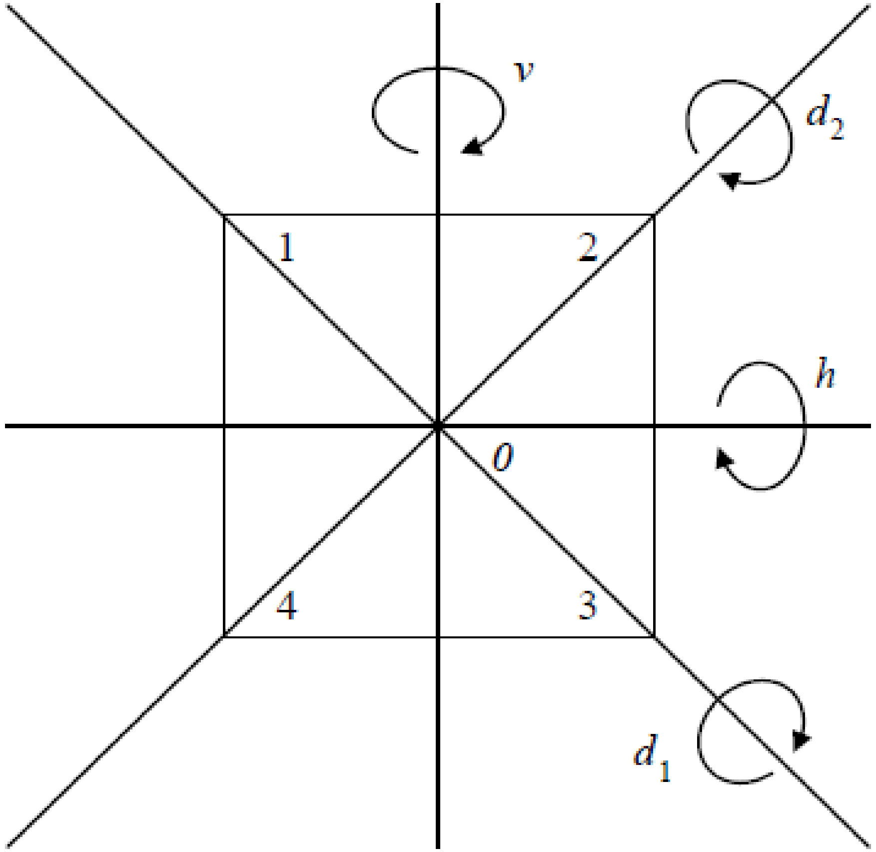
[2] D. S. Malik, John N. Mordeson, M.K. Sen, Introduction to Abstract Algebra, 2007

[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.

Appendix (付録)



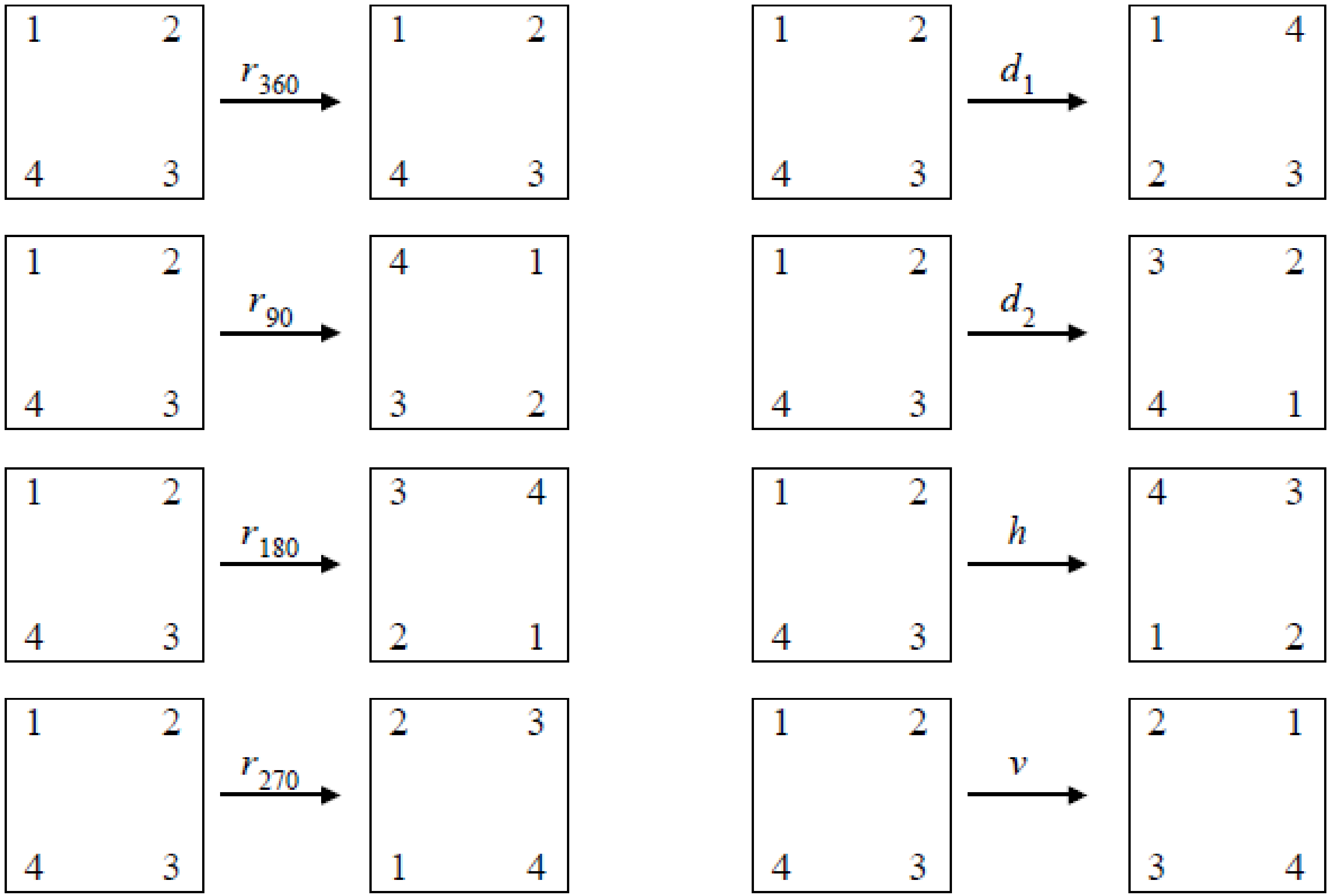
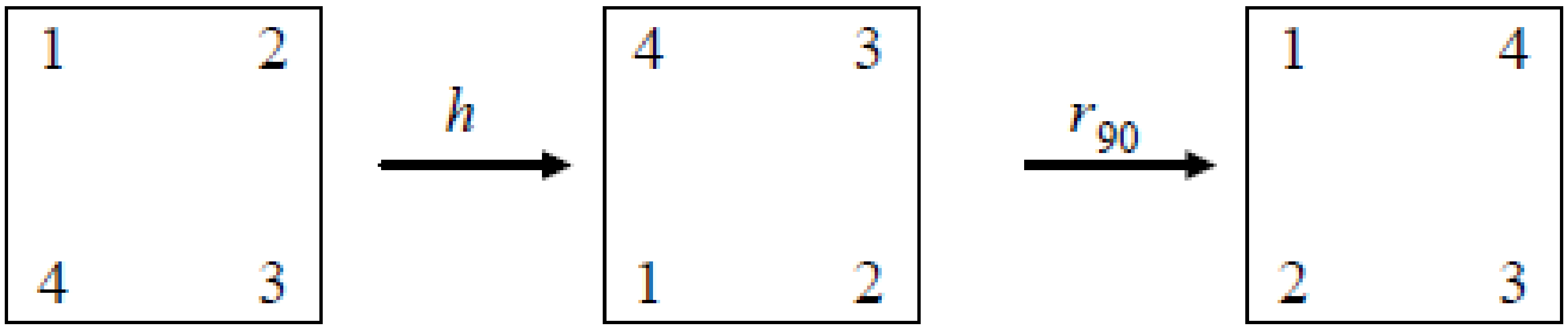


Figure. Rigid motions of a square

Appendix (付録)

$$r_{90} \circ h$$



Appendix (付録)

The complete operation table for the operation $\circ$ is as following

$\circ$	r_{360}	r_{90}	r_{180}	r_{270}	h	v	d_1	d_2
r_{360}	r_{360}	r_{90}	r_{180}	r_{270}	h	v	d_1	d_2
r_{90}	r_{90}	r_{180}	r_{270}	r_{360}	d_1	d_2	v	h
r_{180}	r_{180}	r_{270}	r_{360}	r_{90}	v	h	d_2	d_1
r_{270}	r_{270}	r_{360}	r_{90}	r_{180}	d_2	d_1	h	v
h	h	d_2	v	d_1	r_{360}	r_{180}	r_{270}	r_{90}
v	v	d_1	h	d_2	r_{180}	r_{360}	r_{90}	r_{270}
d_1	d_1	h	d_2	v	r_{90}	r_{270}	r_{360}	r_{180}
d_2	d_2	v	d_1	h	r_{270}	r_{90}	r_{180}	r_{360}