



AY2019 Q2

MA08

# Applied Algebra, 応用代数

(Abstract Algebra, 抽象代数学)

# Class Information

**Lectures:** Period 1, 2 Monday and Period 1, 2 Thursday

**Grades:** 20% Assignments (10, Attendance  $> 2/3$ )

30% Middle Examination

50% Final Examination

+5 Bonus Points from Quizzes

**Office hours:** Period 3, 4 Monday and Thursday; @研究棟#247C

**Textbook:** [Eng] **Abstract Algebra Theory and Applications, 2018,**

**(教科書)**

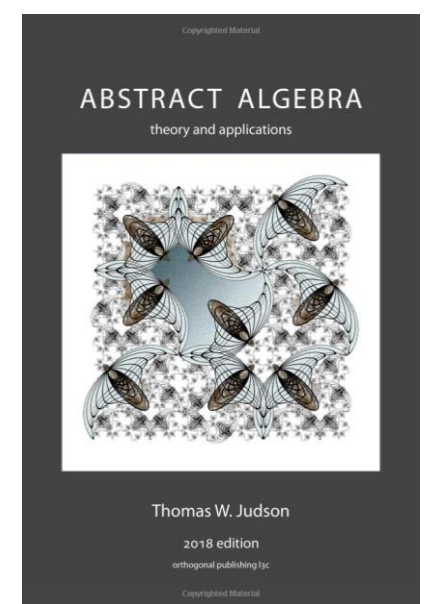
Thomas W. Judson etc.

Free online: <http://abstract.ups.edu/download/aata-20180801-sage-8.2.pdf>


**参考書:** [Eng] **Introduction to Abstract Algebra, 2007, D. S. Malik, John N. Mordeson, M.K. Sen**

Free online: [https://www.researchgate.net/publication/238669835\\_MTH\\_581-582\\_Introduction\\_to\\_Abstract\\_Algebra](https://www.researchgate.net/publication/238669835_MTH_581-582_Introduction_to_Abstract_Algebra)

[Jap] **工学のための応用代数, 1999, 杉原 厚吉, 今井 敏行, 共立出版**



# Hint for Middle & Final Exams

90%  Lecture Slides (Example, Definition, Theorem)  
Assignments

10% Other questions

## About Lecture Notes & Assignments

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

before and after each lecture for slides and assignments.

# What we will cover

## Syllabus on course website

01 promenade to algebraic system

02 remainder of integer and polynomial

03 group(1): Lagrange theorem

04 group(2): quotient group and homomorphism theorem

05 group(3): analysis of group structure

06 applications of group



07 Mid-exam

08 ring and field(1): ideal, quotient ring

09 ring and field(2): polynomial ring

10 ring and field(3): reversible

11 application(1): quotient field and operator theory

12 ring and field(4): extension of field

13 application(2): M-sequence random number generation

14 application(3): error correct coding

# Prerequisites

MA03 Calculus I

\*MA01 Linear Algebra I

Notice: \* is optional.

# Important related courses:

NS03 Quantum Mechanics



# Lecture 1

## Promenade to Algebraic System

# 0.1 Why abstract algebra

## 0.1 Why Abstract Algebra

- **Abstract Algebra** is the study of **algebraic structures** (代数構造).
- **Algebraic structures** include **groups (群)**, **rings (環)**, **fields (体)**, modules, vector spaces, lattices, and algebras.



# 0.1 Why Abstract Algebra

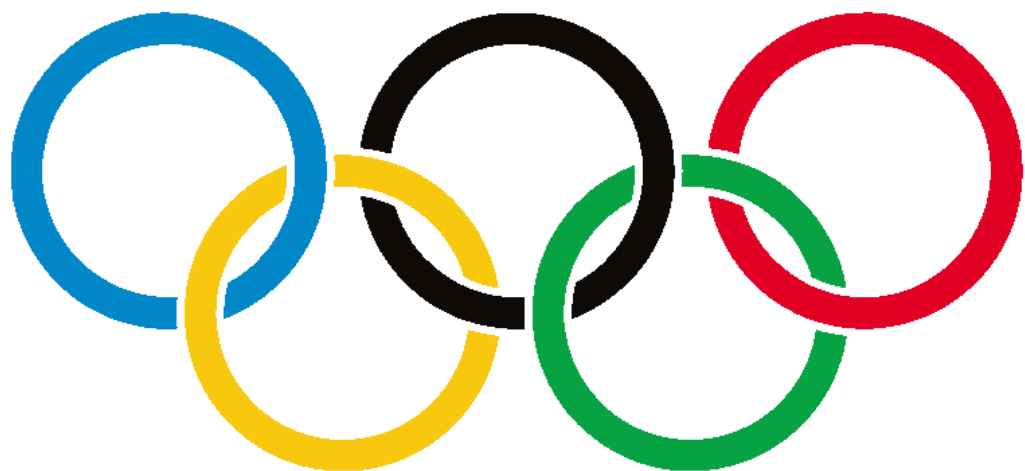
The first time we hear the names of group, ring, field ...



Group (群)

Ring (環)

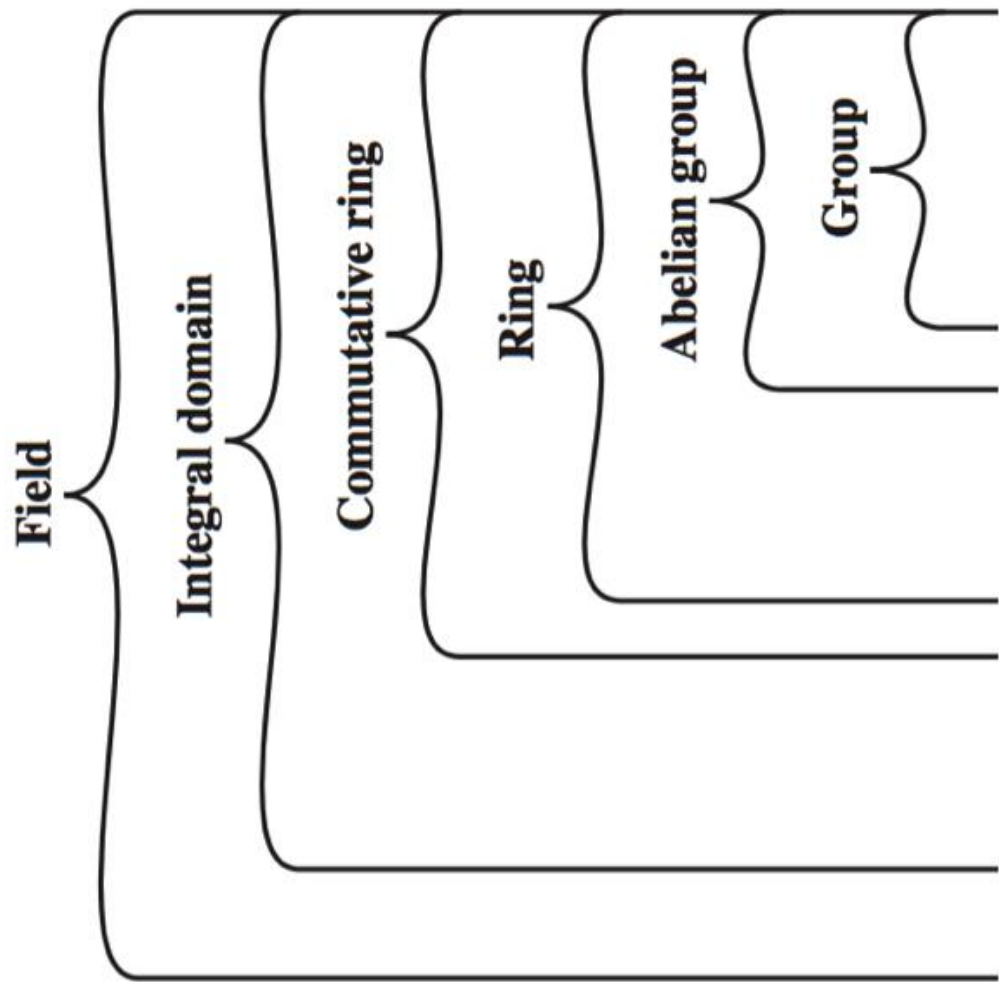
Field (体)



# 0.1 Why Abstract Algebra

理論の土台となる約束事・前提事項。  
( 証明の必要は無い。 )

## Algebra Structure (代数構造)



## Component Axioms (公理)

- (A1) Closure under addition:
- (A2) Associativity of addition:
- (A3) Additive identity:
- (A4) Additive inverse:
- (A5) Commutativity of addition:
- (M1) Closure under multiplication:
- (M2) Associativity of multiplication:
- (M3) Distributive laws:
- (M4) Commutativity of multiplication:
- (M5) Multiplicative identity:
- (M6) No zero divisors:
- (M7) Multiplicative inverse:

## Explanation of Axiom

If  $a$  and  $b$  belong to  $S$ , then  $a + b$  is also in  $S$   
 $a + (b + c) = (a + b) + c$  for all  $a, b, c$  in  $S$   
There is an element  $0$  in  $R$  such that  
 $a + 0 = 0 + a = a$  for all  $a$  in  $S$   
For each  $a$  in  $S$  there is an element  $-a$  in  $S$  such that  $a + (-a) = (-a) + a = 0$   
 $a + b = b + a$  for all  $a, b$  in  $S$   
If  $a$  and  $b$  belong to  $S$ , then  $ab$  is also in  $S$   
 $a(bc) = (ab)c$  for all  $a, b, c$  in  $S$   
 $a(b + c) = ab + ac$  for all  $a, b, c$  in  $S$   
 $(a + b)c = ac + bc$  for all  $a, b, c$  in  $S$   
 $ab = ba$  for all  $a, b$  in  $S$   
There is an element  $1$  in  $S$  such that  
 $a1 = 1a = a$  for all  $a$  in  $S$   
If  $a, b$  in  $S$  and  $ab = 0$ , then either  $a = 0$  or  $b = 0$   
If  $a$  belongs to  $S$  and  $a \neq 0$ , there is an element  $a^{-1}$  in  $S$  such that  $aa^{-1} = a^{-1}a = 1$

Figure 4.2 Groups, Ring, and Field

## 0.1 Why Abstract Algebra

The **three main areas** that were to give rise to **group theory** are:

- **geometry** at the beginning of the 19th Century,  
# studied properties invariant
- **number theory** at the end of the 18th Century,  
# studied modular arithmetic
- **the theory of algebraic equations** at the end of the 18th Century  
# lead to the study of permutations (置換).

Reference: [https://www-history.mcs.st-and.ac.uk/HistTopics/Development\\_group\\_theory.html](https://www-history.mcs.st-and.ac.uk/HistTopics/Development_group_theory.html)



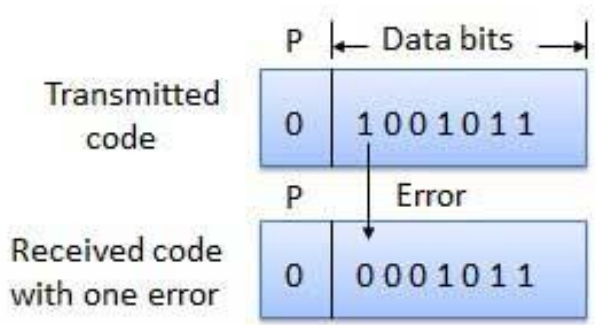
# 0.1 Why Abstract Algebra

Quintic Equation

$$ax^5 + bx^4 + cx^3 + dx^2 + ex + f = 0$$



## Error Correction



2019/6/14

## Rubik's Cube

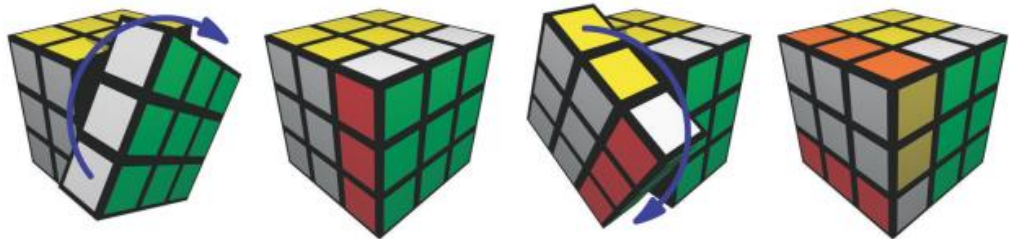


Figure 1.2. The leftmost cube shows the green face rotating 90 degrees clockwise; the next cube shows the result of that move. The third cube shows the white face rotating 90 degrees clockwise; the final cube shows the result of that move.

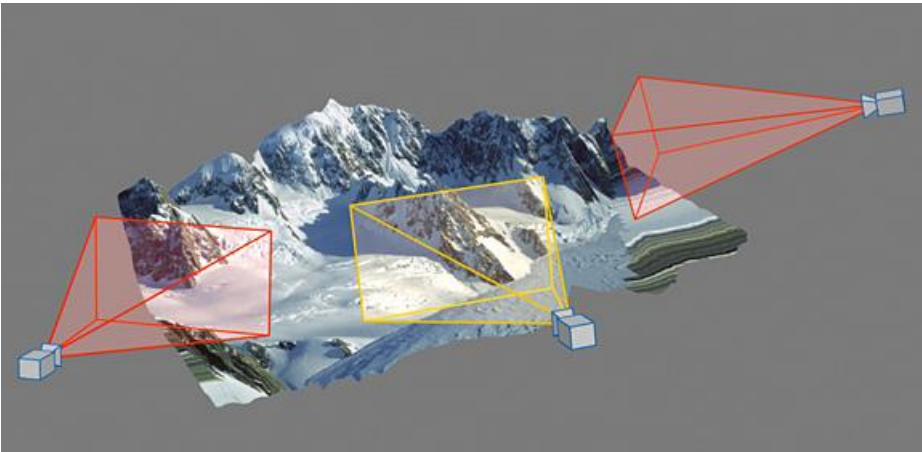
## Fifteen Puzzle



## Standard Model of Elementary Particles

three generations of matter (fermions)			interactions / force carriers (bosons)	
I	II	III		
mass charge spin	$\approx 2.2 \text{ MeV}/c^2$ $\frac{2}{3}$ $\frac{1}{2}$	$\approx 1.28 \text{ GeV}/c^2$ $\frac{2}{3}$ $\frac{1}{2}$	$\approx 173.1 \text{ GeV}/c^2$ $\frac{2}{3}$ $\frac{1}{2}$	$\approx 124.97 \text{ GeV}/c^2$ 0 0 0
<b>u</b> up	<b>c</b> charm	<b>t</b> top	<b>g</b> gluon	<b>H</b> higgs
$\approx 4.7 \text{ MeV}/c^2$ $-\frac{1}{3}$ $\frac{1}{2}$	$\approx 96 \text{ MeV}/c^2$ $-\frac{1}{3}$ $\frac{1}{2}$	$\approx 4.18 \text{ GeV}/c^2$ $-\frac{1}{3}$ $\frac{1}{2}$	0 0 1	
<b>d</b> down	<b>s</b> strange	<b>b</b> bottom	<b>γ</b> photon	
$\approx 0.511 \text{ MeV}/c^2$ -1 $\frac{1}{2}$	$\approx 105.66 \text{ MeV}/c^2$ -1 $\frac{1}{2}$	$\approx 1.7768 \text{ GeV}/c^2$ -1 $\frac{1}{2}$	$\approx 91.19 \text{ GeV}/c^2$ 0 1	
<b>e</b> electron	<b>μ</b> muon	<b>τ</b> tau	<b>Z</b> Z boson	
$< 2.2 \text{ eV}/c^2$ 0 $\frac{1}{2}$	$< 0.17 \text{ MeV}/c^2$ 0 $\frac{1}{2}$	$< 18.2 \text{ MeV}/c^2$ 0 $\frac{1}{2}$	$\approx 80.39 \text{ GeV}/c^2$ $\pm 1$ 1	
<b>ν<sub>e</sub></b> electron neutrino	<b>ν<sub>μ</sub></b> muon neutrino	<b>ν<sub>τ</sub></b> tau neutrino	<b>W</b> W boson	

## 3D Mapping in Computer Vision



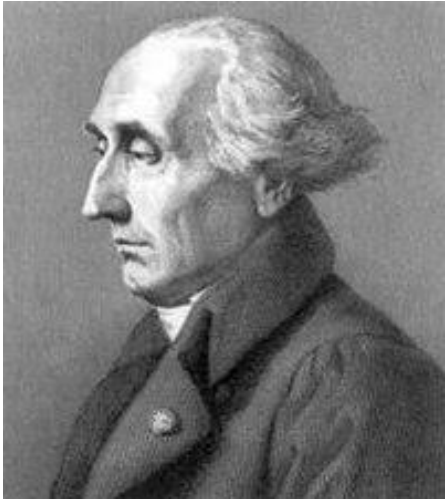
# 0.1 Why Abstract Algebra

## Birth of Group Theory (群論)

### General Quintic Equation

$$ax^5 + bx^4 + cx^3 + dx^2 + ex + f = 0$$

They reveal Non-existence of a formula that is comprised of these coefficients, arithmetic operations and roots for general quintic equation



Joseph-Louis Lagrange  
(ラグランジュ)  
France, 1736 ~ 1813



Évariste Galois (ガロア)  
France, 1811 ~ 1832



Niels Henrik Abel (アーベル)  
Norway, 1802 ~ 1829

# 0.1 Why Abstract Algebra

**Lagrange** firstly studied **Permutations** (置換) in his 1770 paper on the theory of algebraic equations. Lagrange's main object was to find out why cubic (三次) and quartic (四次) equations (方程式) could be solved algebraically.

**Cauchy** played a major role in **developing the theory of permutations**. His first paper on the subject was in 1815 but at this stage Cauchy is motivated by permutations of roots of equations.

**Abel**, in 1824, **gave the first accepted proof of the insolubility of the quantic equation (五次方程式)**, and he used the existing ideas on permutations of roots but little new in the development of group theory.

**Galois** in 1831 was the first to really understand that the algebraic solution of an equation **was related to the structure of a group** le groupe of permutations related to the equation. By 1832 **Galois had discovered that special subgroups (部分群) (now called normal subgroups) are fundamental**. He calls **the decomposition of a group into cosets (剰余類) of a subgroup a proper decomposition if the right and left coset decompositions coincide**. Galois then shows that the non-abelian simple group of smallest order has order 60.

**Galois' work was not known until Liouville published Galois' papers in 1846**. Liouville saw clearly the connection between Cauchy's theory of permutations and Galois' work. However Liouville failed to grasp that the importance of Galois' work lay in the group concept.

Reference: [https://www-history.mcs.st-and.ac.uk/HistTopics/Development\\_group\\_theory.html](https://www-history.mcs.st-and.ac.uk/HistTopics/Development_group_theory.html)

# 0.2 A Short Note on Proofs

In studying **abstract mathematics**, we take what is called an **axiomatic approach**; that is, we **take a collection of objects  $S$  and assume some rules about their structure**.

These rules are called **axioms (公理)**. Using the axioms for  $S$ , we wish to derive other information about  $S$  by using logical arguments.



A **statement** (言明, 命題) in logic or mathematics is an **assertion** (主張) that **is either true (真) or false (偽)**. Consider the following examples:

1.  ~~$3 + 56 - 13 + 8/2.$~~

2. All cats are black.

3.  $2 + 3 = 5.$

4.  $2x = 6$  exactly when  $x = 4.$

5. If  $ax^2 + bx + c = 0$  and  $a \neq 0$ , then

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

6.  ~~$x^3 - 4x^2 + 5x - 6.$~~

All examples except the first and last examples are statements, and must be either true or false.

- A mathematical proof is nothing more than a convincing argument about the accuracy of a statement.

Let us examine different types of statements. A statement could be as simple as " $10/5 = 2$ "

however, mathematicians are usually interested in more complex statements such as "**If  $p$ , then  $q$ ,**" where  $p$  and  $q$  are both statements.

Here  $p$  is called the hypothesis and  $q$  is known as the conclusion.

## 0.2 A Short Note on Proofs

## Proof

Consider the **following statement**: If  $ax^2 + bx + c = 0$  and  $a \neq 0$ , then

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

Here the **hypothesis** is  $ax^2 + bx + c = 0$  and  $a \neq 0$ ; the **conclusion** is

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

Notice that the **statement** says nothing about whether or not the hypothesis is true. However, if this entire statement is true and we can show that  $ax^2 + bx + c = 0$  with  $a \neq 0$  is true, then the conclusion *must* be true. A proof of this statement might simply be a series of equations:

**Proof:**

$$\begin{aligned} ax^2 + bx + c &= 0 \\ x^2 + \frac{b}{a}x &= -\frac{c}{a} && \because a \neq 0 \\ x^2 + \frac{b}{a}x + \left(\frac{b}{2a}\right)^2 &= \left(\frac{b}{2a}\right)^2 - \frac{c}{a} \\ \left(x + \frac{b}{2a}\right)^2 &= \frac{b^2 - 4ac}{4a^2} \\ x + \frac{b}{2a} &= \frac{\pm\sqrt{b^2 - 4ac}}{2a} \\ x &= \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}. \end{aligned}$$

If we can prove a statement true or false, then that statement is called a proposition (命題).

A proposition of major importance is called a theorem (定理).

Sometimes instead of proving a theorem or proposition all at once, we break the proof (証明) down into modules; that is, we prove several supporting propositions, which are called lemmas (補題), and use the results of these propositions to prove the main result.

If we can prove a proposition or a theorem, we will often, with very little effort, be able to derive other related propositions called corollaries (系).

# What you will learn in Lecture 1

## 1.1 Sets (集合)

## 1.2 Relation (関係), Mapping (写像) and Permutation (置換)

## 1.3 Division (除法), Quotient (商), Remainder (剰余), Great Common Divisor (最大公約数)

## 1.4 Equivalence Classes (同値類)

## 1.1 Sets (集合)

## 1.1 Sets (集合)

We will denote sets by capital letters, such as  $X$ .

- A *set*  $X$  is a well-defined collection of objects  
(集合とは、well-defined なモノの集まりのことである。);  
that is, it is defined that we can determine for any given object  $x$  whether or not  $x$  belongs to the set  $X$ .
- The objects that belong to a set are called its *elements* (要素) or *members*.

Given a set  $X$ , we use the notation

$x \in X$  to mean  $x$  is an element of  $X$

$x \notin X$  to mean  $x$  is **not** an element of  $X$

collection of objects

For example, for the set  $X = \{1, 2, 3\}$ , we have  $1 \in X$  and  $4 \notin X$ .

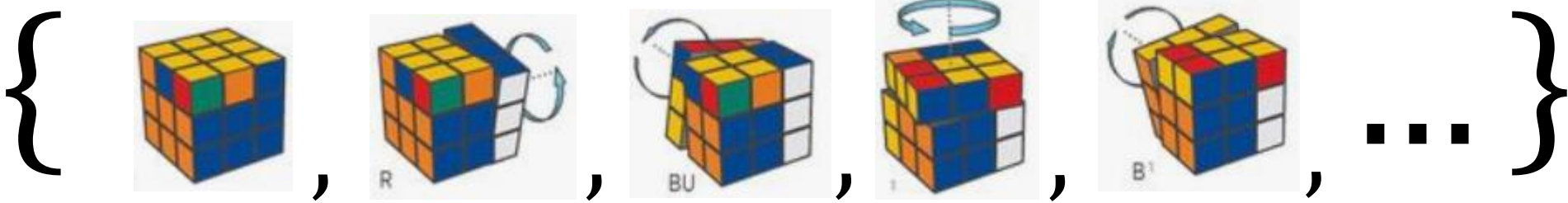
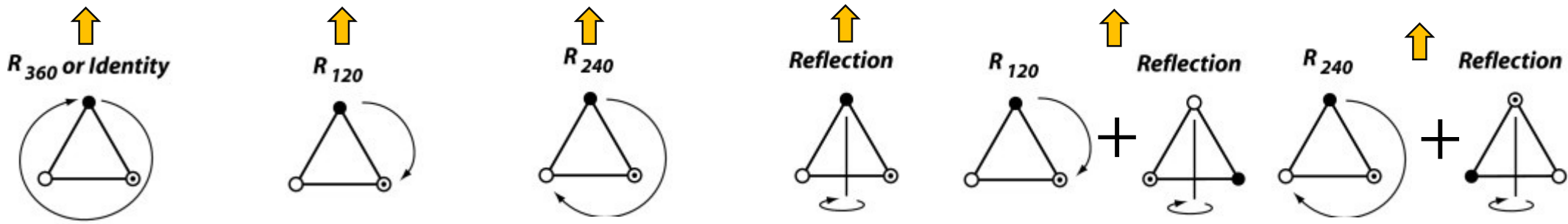
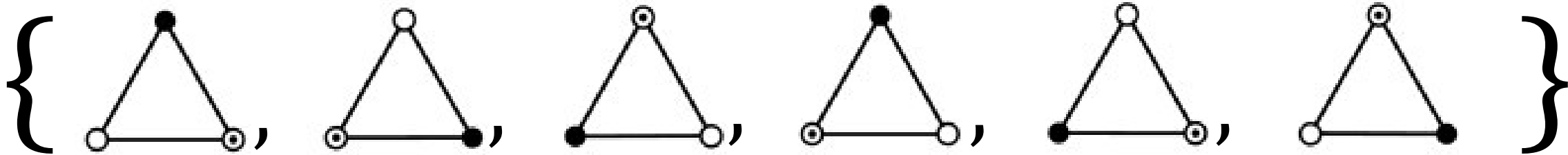
object, i.e. element or member

1.1 Sets (集合)

Example of Sets

{1, 2, 3, 4, 5, ... }

{..., -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, ... }





- A set  $X$  is a well-defined collection of objects;  
that is, it is defined that we can determine for any given object  $x$  whether or not  $x$  belongs to the set  $X$ .

A set  $X$  is **well-defined (ちゃんと定義になっている)**, meaning that if  $X$  is a set and  $x$  is some object, then either  $x$  is definitely in  $X$ , denoted by  $x \in X$ , or  $x$  is definitely not in  $X$ , denoted by  $x \notin X$ .

Thus, we should never say, "Consider the set  $S$  of some positive integers," , because it is **not definite** whether  $2 \in S$  or  $2 \notin S$ .

On the other hand, we can consider the set of all **even** positive integers, because every positive integer is definitely either even or odd. Thus  $2 \in S$  and  $3 \notin S$ .

A set is usually specified by

(1) listing all of its elements inside a pair of braces

$$X = \{x_1, x_2, \dots, x_n\}$$

for a set containing elements  $x_1, x_2, \dots, x_n$ ;

(2) stating the characterizing property that determines whether or not an object  $x$  belongs to the set

$$X = \{x \mid x \text{ satisfies } P(x)\} \quad \text{or} \quad X = \{x : x \text{ satisfies } P(x)\}$$

if each  $x$  in  $X$  satisfies a certain property  $P(x)$ .

The notation  $X = \{x \mid x \text{ satisfies } P(x)\}$  is often called "set-builder notation"

## 1.1 Sets (集合)

## Important Sets

If  $S$  is the set of even positive integers, we can describe  $S$  by writing either

$$S = \{2, 4, 6, \dots\} \text{ or } S = \{x \mid x \text{ is an even integer and } x > 0\}$$

We write  $2 \in S$  when we want to say that 2 is in the set  $S$ , and  $3 \notin S$  to say that 3 is not in the set  $S$ .

- Some of the more **important sets** that we will consider are the following:

$$\mathbb{N} = \{n \mid n \text{ is a natural number}\} = \{1, 2, 3, \dots\}$$

$$\mathbb{Z} = \{z \mid z \text{ is an integer}\} = \{\dots, -2, -1, 0, 1, 2, \dots\}$$

$$\mathbb{Q} = \{r \mid r \text{ is a rational number}\} = \{p/q \mid p, q \in \mathbb{Z} \text{ where } q \neq 0\}$$

$$\mathbb{R} = \{x \mid x \text{ is a real number}\}$$

$$\mathbb{C} = \{z \mid z \text{ is a complex number}\}$$

A set  $A$  is said to be a **subset** (部分集合) of a set  $S$  if every element of  $A$  is an element of  $S$ . In this case, we write  $A \subseteq S$  and say that  $A$  is contained in  $S$ .

If  $A \subseteq S$ , but  $A \neq S$ , then we write  $A \subset S$  and say that  $A$  is properly contained in  $S$ . Or we say  $A$  is a **proper subset** (真部分集合) of  $S$ .

As an example, we have  $\{1, 2, 3\} \subseteq \{1, 2, 3\}$  and  $\{1, 2\} \subset \{1, 2, 3\}$ .

If every element of  $A$  is a element of  $B$  and every element of  $B$  is a element of  $A$ , then we say that  $A$  and  $B$  are the same or equal.

In this case, we write  $A = B$ .

Then, we can easily have the following theorem

### Theorem 1.1

Let  $A$  and  $B$  be sets. Then  $A = B$  if and only if  $A \subseteq B$  and  $B \subseteq A$ .

The **empty set** (空集合) or **null set** is the set with no elements.

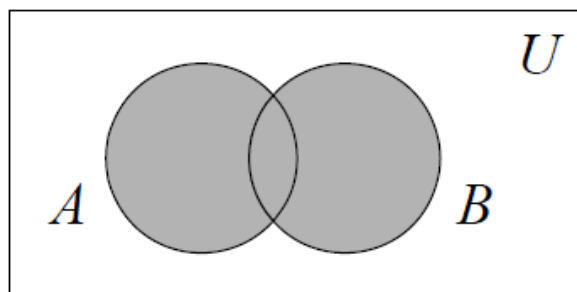
- We usually denote the empty set by  $\emptyset$ .
- For any set  $A$ , we have  $\emptyset \subseteq A$ .

## Definition 1.1

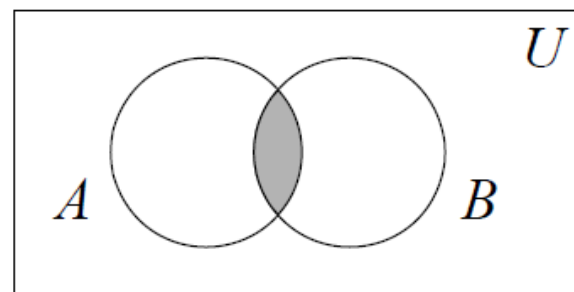
The **union** (和集合) of two sets  $A$  and  $B$ , written  $A \cup B$ , is defined to be the set  $A \cup B = \{x \mid x \in A \text{ or } x \in B\}$ .

## Definition 1.2

The **intersection** (積集合, 共通部分) of two sets  $A$  and  $B$ , written  $A \cap B$ , is defined to be the set  $A \cap B = \{x \mid x \in A \text{ and } x \in B\}$ .



$A \cup B$



$A \cap B$

### Example 1.1

Let  $A$  be the set  $\{1, 2, 3, 4\}$  and  $B$  be the set  $\{3, 4, 5, 6\}$ .

Then  $A \cup B = \{1, 2, 3, 4, 5, 6\}$  and  $A \cap B = \{3, 4\}$

If  $C$  is the set  $\{5, 6\}$ , then  $A \cup C = \{1, 2, 3, 4, 5, 6\}$  while  $A \cap C = \emptyset$ .

### Notice:

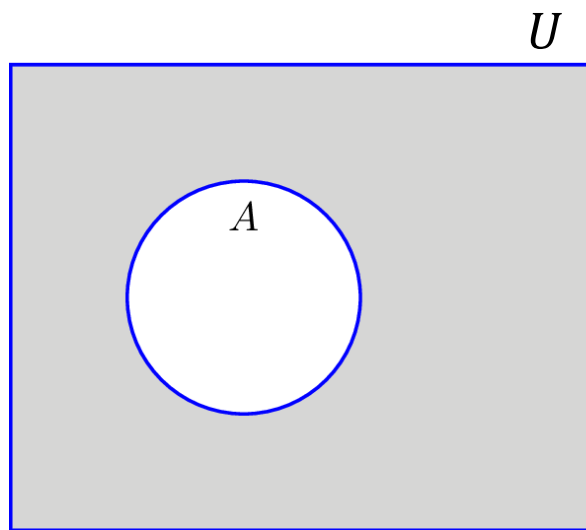
Two sets  $A$  and  $B$  are called **disjoint** (2つの集合が交わりを持たない  
あるいは互いに素) exactly when  $A \cap B = \emptyset$ .



## Definition 1.3

For any set  $A \subset U$ , where  $U$  is **universal set (全体集合)**, we define the **complement (補集合)** of  $A$ , denoted by  $A'$ , to be the set

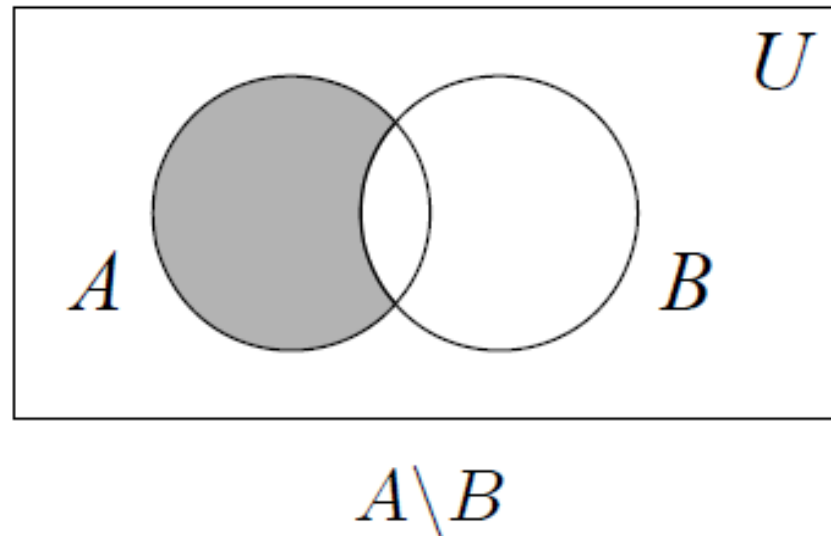
$$A' = \{x \mid x \in U \text{ and } x \notin A\}.$$



### Definition 1.4

Given two sets  $A$  and  $B$ , the **relative complement** of  $B$  in  $A$ , denoted by *the set difference*  $A \setminus B$ , is the set

$$A \setminus B = A \cap B' = \{x \mid x \in A, \text{ but } x \notin B\}.$$



### Example 1.2

Let  $A = \{1, 2, 3, 4\}$  and  $B = \{3, 4, 5, 6\}$ . Then  $A \setminus B = \{1, 2\}$

## 1.1 Sets (集合)

### Remark

Let  $P$  and  $Q$  be statements.

Throughout the class, we will encounter questions in which we will be asked to show that  $P$  if and only if  $Q$ ;

that is, show that statement  $P$  is true if and only if statement  $Q$  is true.

In situations like this,

- we first assume that statement  $P$  is true and show that statement  $Q$  is true.
- Then we assume that statement  $Q$  is true and show that statement  $P$  is true.

The statement  $P$  if and only if  $Q$  is also equivalent to the statement: if  $P$ , then  $Q$ , and if  $Q$ , then  $P$ .

# **1.2 Relation (関係), Mapping (写像) and Permutation (置換)**

### Definition 1.5

Let  $A$  and  $B$  be nonempty sets (空でない集合) and  $x \in A, y \in B$ . The **Cartesian cross product** (Cartesian product, 直積集合) of  $A$  and  $B$ , written  $A \times B$ , is defined to be the set

$$A \times B = \{(x, y) \mid x \in A, y \in B\}.$$

where  $(x, y)$  is called the **ordered pair** (順序対).

### Example 1.3

If  $A = \{x, y\}$ ,  $B = \{1, 2, 3\}$ , and  $C = \emptyset$ ,  
then  $A \times B = \{(x, 1), (x, 2), (x, 3), (y, 1), (y, 2), (y, 3)\}$ .  
and  $A \times C = \emptyset$

We define the **Cartesian product** of  $n$  sets to be

$$A_1 \times \cdots \times A_n = \{(a_1, \dots, a_n) \mid a_i \in A_i \text{ for } i = 1, \dots, n\}.$$


$$a_1 \in A_1, a_2 \in A_2, \dots, \text{ and } a_n \in A_n$$

If  $A_1 = A_2 = \cdots = A_n$ , we often write  $A^n$  for  $A \times \cdots \times A$  (where  $A$  would be written  $n$  times).

For example, the set  $\mathbb{R}^3 = \mathbb{R} \times \mathbb{R} \times \mathbb{R}$  consists of all of 3-tuples of real numbers.

### Definition 1.6

A **binary relation** (二項関係) or simply a **relation**  $\mathcal{R}$  from a set  $A$  to a set  $B$  is a **subset** of  $A \times B$ .

Let  $\mathcal{R}$  be a relation from a set  $A$  into a set  $B$ .

If  $(x, y) \in \mathcal{R}$ , we write  $x\mathcal{R}y$  or  $\mathcal{R}(x) = y$ .

If  $x\mathcal{R}y$ , then sometimes we say that  $x$  is related to  $y$  (or  $y$  is in relation with  $x$ ) with respect to  $\mathcal{R}$  or simply  $x$  is related to  $y$ .



### Definition 1.7

Let  $A$  and  $B$  be nonempty sets. A special type of relation  $f \subset A \times B$  from  $A$  into  $B$  is called a **function** (関数) (or **mapping** (写像)) from  $A$  into  $B$  if

- (i)  $\mathcal{D}(f) = A$ , i.e. the *domain* (定義域) of  $f$  is the set  $A$ ;
- (ii) for all  $(x, y), (x', y') \in f$ , we have that  $x = x'$  implies  $y = y'$ .

When (ii) is satisfied by a relation  $f$ , we say that  $f$  is **well defined** or **single-valued**.

We can also say that for every element in  $A$ ,  $f$  assigns a unique element in  $B$ . We usually write  $f: A \rightarrow B$  or  $A \xrightarrow{f} B$ .

Instead of writing down ordered pairs  $(a, b) \in A \times B$ , we write  $f(a) = b$  or  $f: a \mapsto b$ .

The set  $A$  is called the *domain* (定義域) of  $f$ , denote by  $\mathcal{D}(f) = A$ . The set  $f(A)$  is called the *range* (値域) or *image* of  $f$ , defined by

$$f(A) = \{f(a) \mid a \in A\} \subset B.$$

**Notice** that here  $f(A)$  is a subset of  $B$ .

We can think of the elements in the function's domain as input values and the elements in the function's range as output values.

## 1.2 Relation, Mapping and Permutation

### Domain & Range

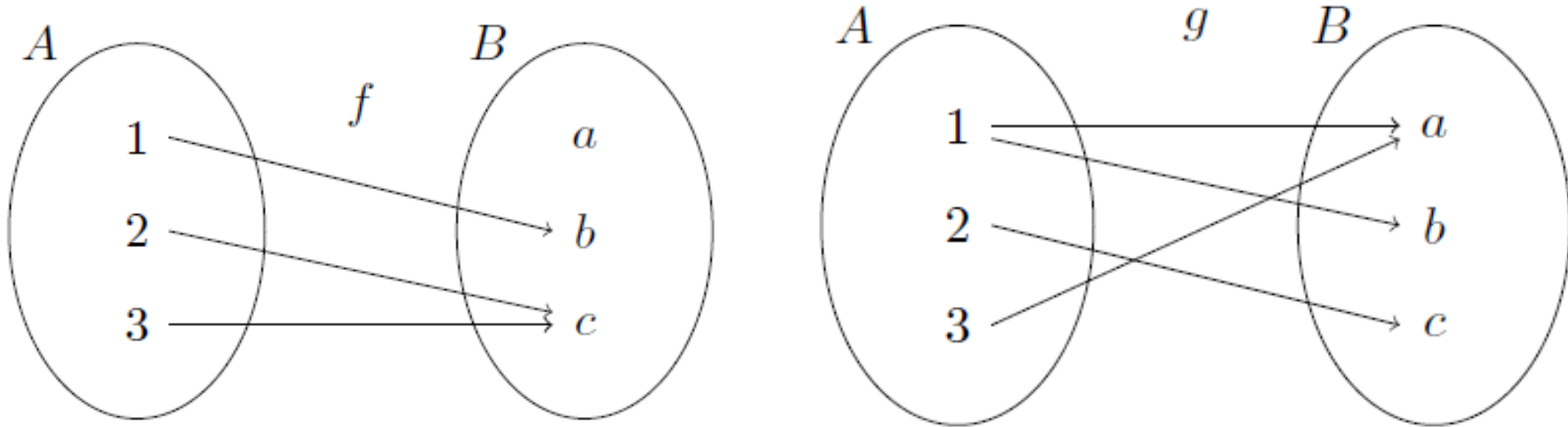


Figure 1.1 Mappings and relations

### Example 1.4

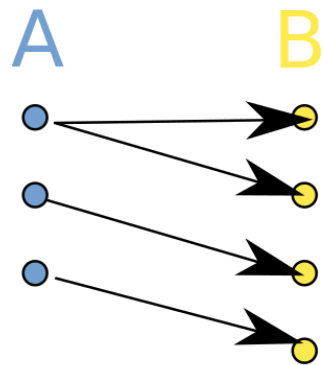
Suppose  $A = \{1, 2, 3\}$ , and  $B = \{a, b, c\}$ . In Figure 1.1 we define relations  $f$  and  $g$  from  $A$  to  $B$ . The relation  $f$  is a mapping, but  $g$  is not, because  $1 \in A$  is not assigned to a unique element in  $B$ ; that is,  $g(1) = a$  and  $g(1) = b$ .

### Definition 1.8

Let  $f$  be a function from a set  $A$  to a set  $B$ . Then

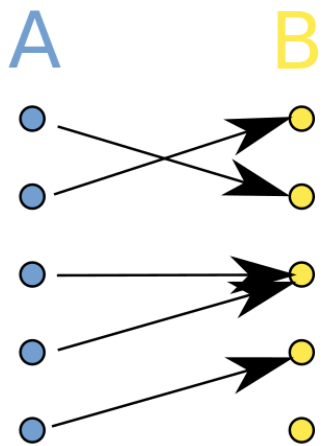
- (i)  $f$  is called *one-to-one* (一対一) or *injective* (単射) if for all  $x, x' \in A$ , we have that  $f(x) = f(x')$  implies  $x = x'$ .
- (ii)  $f$  is called *onto* or *surjective* (全射)  $B$  (or  $f$  maps  $A$  onto  $B$ ) if  $f(A) = B$ .
- (iii) A map is called *bijective* (全単射、あるいは双射) if both *one-to-one* and *onto*.

# 1.2 Relation, Mapping and Permutation



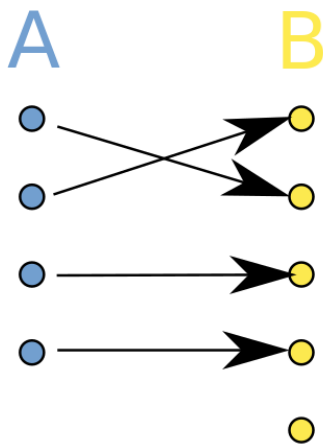
NOT a  
Function

*A has many B*



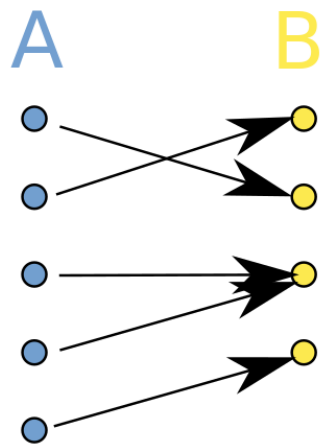
General  
Function

*B can have many A*



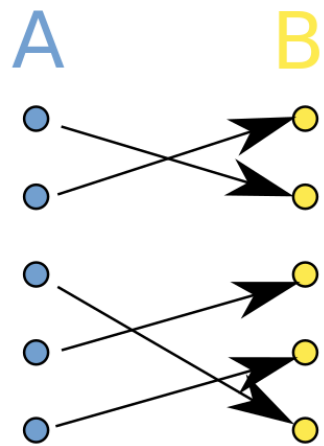
Injective  
(not surjective)

*B can't have many A*



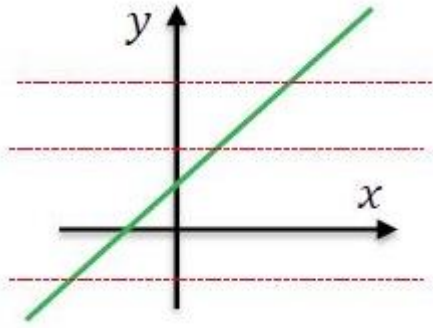
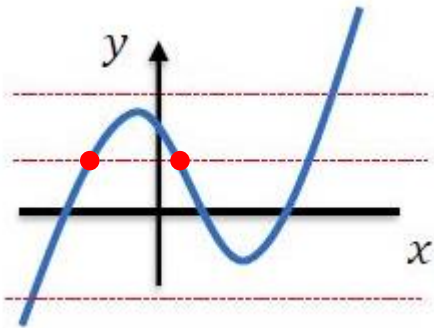
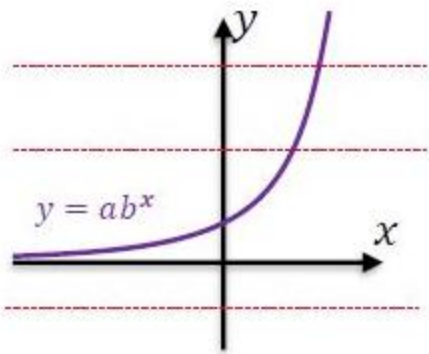
Surjective  
(not injective)

*Every B has some A*



Bijjective  
(injective, surjective)

*A to B, perfectly*



Negative  $y$  is not used  
Applied Algebra (応用代数)

## 1.2 Relation, Mapping and Permutation

### Example 1.5

Let  $A = \{1, 2, 3\}$ ,  $B = \{2, 4, 6\}$ . For the following relation between  $A$  and  $B$  given as a subset of  $A \times B$ , decide whether it is a function mapping  $A$  into  $B$ . If it is a function, decide whether it is *one-to-one* and whether it is *onto*  $B$ .

	is function	is <i>one-to-one</i>	is <i>onto</i> $B$
(a) $\{(1,4),(2,4),(3,6)\}$	Yes	No	No
(b) $\{(1,4),(2,6),(3,2)\}$	Yes	Yes	Yes
(c) $\{(1,4),(1,6),(2,2)\}$	No		

Given two functions, we can construct a new function by using the range of the first function as the domain of the second function.

### Definition 1.9

Let  $f: A \rightarrow B$  and  $g: B \rightarrow C$  be mappings.  
Define the *composition of mapping* (合成写像) of  $f$  and  $g$  from  $A$  to  $C$ , by  $(g \circ f)(x) = g(f(x))$ .

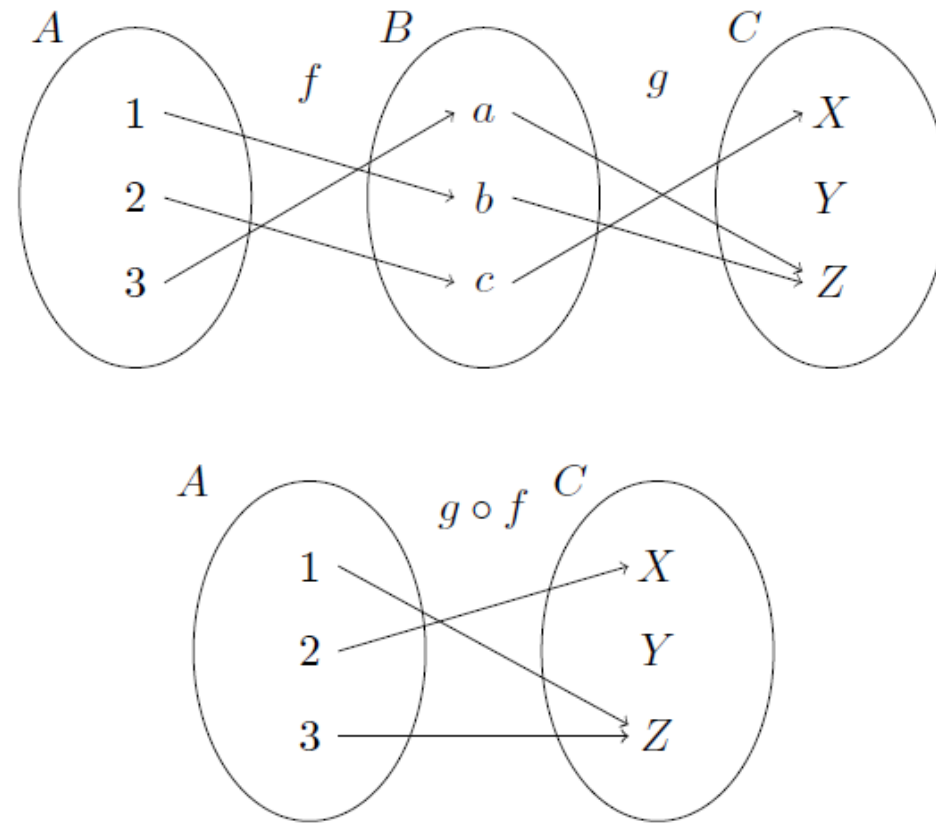


Figure 1.2 Composition of maps

**Example 1.6** Consider the functions  $f: A \rightarrow B$  and  $g: B \rightarrow C$  that are defined in Figure 1.2 (top). The composition of these functions,  $g \circ f: A \rightarrow C$ , is defined in Figure 1.2 (bottom).



### Example 1.7

Let  $f(x) = x^2$  and  $g(x) = 2x + 5$ . Then

$$(f \circ g)(x) = f(g(x)) = (2x + 5)^2 = 4x^2 + 20x + 25$$

and

$$(g \circ f)(x) = g(f(x)) = 2x^2 + 5$$

In general, order (順序) makes a difference; that is, in most cases

$$f \circ g \neq g \circ f.$$

### Example 1.8

Sometimes it has the case that  $f \circ g = g \circ f$ . Let  $f(x) = x^3$  and  $g(x) = \sqrt[3]{x}$ . Then

$$(f \circ g)(x) = f(g(x)) = f(\sqrt[3]{x}) = (\sqrt[3]{x})^3 = x$$

and

$$(g \circ f)(x) = g(f(x)) = g(x^3) = \sqrt[3]{(x^3)} = x$$

### Example 1.9

Suppose that  $S = \{1, 2, 3\}$ . Define a map  $\pi: S \rightarrow S$  by  $\pi(1) = 2, \pi(2) = 1, \pi(3) = 3$ .

This is a *bijective* map. An alternative way to write  $\pi$  is

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

\*This notation is due to Cauchy and is called the **two-row notation**.

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

If  $S$  is any set, we will use  $id_S$  or  $id$  to denote the *identity mapping* (恒等写像) from  $S$  to itself. Define this map by  $id_S(s) = s$  for all  $s \in S$ .

### Definition 1.10

Let  $A$  and  $B$  be sets and  $f: A \rightarrow B$ .

(i)  $f$  is called **left invertible** (左可逆) if there exists  $g: B \rightarrow A$  such that  $g \circ f = id_A$ .

(ii)  $f$  is called **right invertible** (右可逆) if there exists  $h: B \rightarrow A$  such that  $f \circ h = id_B$ .

A function  $f: A \rightarrow B$  is called **invertible** (可逆) if  $f$  is both left and right invertible.

### Example 1.10

The function  $f(x) = x^3$  has inverse  $f^{-1}(x) = g(x) = \sqrt[3]{x}$ .

Because left invertible

$$(g \circ f)(x) = g(f(x)) = g(x^3) = \sqrt[3]{(x^3)} = x = id_X$$

and right invertible

$$(f \circ g)(x) = f(g(x)) = f(\sqrt[3]{x}) = (\sqrt[3]{x})^3 = x = id_X$$

### Theorem 1.2

A mapping is **invertible** (可逆) if and only if it is ***bijjective*** (全单射), i.e. both ***one-to-one*** and ***onto***.

# **1.3 Division (除法), Quotient (商), Remainder (剰余), Great Common Divisor (最大公約数)**

## Theorem 1.3 Division Algorithm

Let  $x$  and  $y$  be integers, with  $y \neq 0$ . Then there exist unique integers  $q$  and  $r$  such that  $x = yq + r$  where  $0 \leq r < |y|$ .

The integer  $q$  is called the **quotient (商)** of  $x$  and  $y$  on dividing  $x$  by  $y$  and  
the integer  $r$  is called the **remainder (剰余)** of  $x$  and  $y$  on dividing  $x$  by  $y$ .



### Definition 1.11

Let  $x, y \in \mathbb{Z}$  with  $x \neq 0$ . Then  $x$  is said to divide  $y$  or  $x$  is a **divisor** (約数) (or **factor** (因子)) of  $y$ , written  $x|y$ , provided there exists  $q \in \mathbb{Z}$  such that  $y = qx$ . When  $x$  does not divide  $y$ , we sometimes write  $x \nmid y$ .

### Definition 1.12

Let  $x, y \in \mathbb{Z}$ . A nonzero integer  $c$  is called a **common divisor** (公約数) of  $x$  and  $y$  if  $c|x$  and  $c|y$ .

### Definition 1.13

A nonzero integer  $d$  is called a **greatest common divisor** (gcd) (最大公約数) of the integers  $x$  and  $y$  if

- (i)  $d|x$  and  $d|y$ ,
- (ii) for all  $c \in \mathbb{Z}$  if  $c|x$  and  $c|y$ , then  $c|d$ .

### Theorem 1.4

Let  $x, y \in \mathbb{Z}$  with either  $x \neq 0$  and  $y \neq 0$ . Then  $x$  and  $y$  have a positive greatest common divisor  $\gcd(x, y) = d$ . Moreover, there exist integers  $s, t \in \mathbb{Z}$  such that

$$\gcd(x, y) = d = sx + ty.$$

### Example 1.11

Consider the  $\gcd(45, 126)$ .

$$126 = 2 \cdot 45 + 36$$

$$45 = 1 \cdot 36 + 9$$

$$36 = 4 \cdot 9 + 0$$

$$\text{Thus, } \gcd(45, 126) = 9$$

Also,

$$9 = 45 - 1 \cdot 36$$

$$= 45 - 1 \cdot [126 - 2 \cdot 45]$$

$$= 3 \cdot 45 + (-1) \cdot 126.$$

Here  $s = 3$  and  $t = -1$ .

### Definition 1.14

- (i) An integer  $p > 1$  is called **prime** (素数) if the only divisors of  $p$  are  $\pm 1$  and  $\pm p$ .
- (ii) Two integers  $x$  and  $y$  are called **relatively prime** (互いに素) if  $\gcd(x, y) = 1$ .

## 1.4 Equivalence Classes (同値類)

## 1.4 Equivalence Classes (同値類)

### Definition 1.15

Let  $\mathcal{R}$  be a binary relation on a set  $X$ , i.e.  $\mathcal{R} \subset X \times X$ . Then  $\mathcal{R}$  is called

- (i) **reflexive** (反射的) if for all  $x \in X$ ,  $(x, x) \in \mathcal{R}$  (i.e.  $x\mathcal{R}x$ );
- (ii) **symmetric** (対称的) if for all  $x, y \in X$ ,  $(x, y) \in \mathcal{R}$  implies  $(y, x) \in \mathcal{R}$  (i.e.  $x\mathcal{R}y$  implies  $y\mathcal{R}x$ );
- (iii) **Transitive** (推移的) if for all  $x, y, z \in X$ ,  $(x, y)$  and  $(y, z) \in \mathcal{R}$  implies  $(x, z) \in \mathcal{R}$  (i.e.  $x\mathcal{R}y$  and  $y\mathcal{R}z$  imply  $x\mathcal{R}z$ ).

### Definition 1.16

A binary relation  $\mathcal{R}$  on a set  $X$  is called an **equivalence relation** (同値関係) on  $X$  if  $\mathcal{R}$  is reflexive, symmetric, and transitive.

## Definition 1.17

Let  $\mathcal{R}$  be an **equivalence relation** on a set  $A$ . For all  $x \in A$ , let  $[x]$  denote the set

$$[x] = \{y \in A \mid y\mathcal{R}x\}.$$

The set  $[x]$  is called the **equivalence class** (with respect to  $\mathcal{R}$ ) of  $x$ .

## Theorem 1.5

Let  $\mathcal{R}$  be an equivalence relation on the set  $A$ . Then

- (i) for all  $x \in A$ ,  $[x] \neq \emptyset$ ,
- (ii) if  $y \in [x]$ , then  $[x] = [y]$ , where  $x, y \in A$ ,
- (iii) for all  $x, y \in A$ , either  $[x] = [y]$  or  $[x] \cap [y] = \emptyset$ ,
- (iv)  $A = \bigcup_{x \in A} [x]$ , i.e.,  $A$  is the union of all equivalence classes with respect to  $\mathcal{R}$ .

## 1.4 Equivalence Classes (同値類)

Let  $r$  and  $s$  be two integers and suppose that  $n \in \mathbb{N}$ .

We say that  $r$  is *congruent* (合同) to  $s$  *modulo* (剰余演算)  $n$ , or  $r$  is congruent to  $s \bmod n$ , if  $r - s$  is evenly divisible by  $n$ ; that is,  $r - s = nk$  for some  $k \in \mathbb{Z}$ .

In this case we write  $r \equiv s \pmod{n}$ .

### Example 1.12

$41 \equiv 17 \pmod{8}$  since  $41 - 17 = 24$  is divisible by 8.

We claim that congruence modulo  $n$  forms an **equivalence relation** of  $\mathbb{Z}$ .

Certainly any integer  $r$  is equivalent to itself since  $r - r = 0$  is divisible by  $n$ .



## 1.4 Equivalence Classes (同値類)

We will now show that the relation is symmetric. If  $r \equiv s \pmod{n}$ , then  $r - s = -(s - r)$  is divisible by  $n$ . So  $s - r$  is divisible by  $n$  and  $s \equiv r \pmod{n}$ . Now suppose that  $r \equiv s \pmod{n}$  and  $s \equiv t \pmod{n}$ . Then there exist integers  $k$  and  $m$  such that  $r - s = kn$  and  $s - t = mn$ .

To show transitivity, it is necessary to prove that  $r - t$  is divisible by  $n$ . However,

$$r - t = r - s + s - t = kn + mn = (k + l)n$$

and so  $r - t$  is divisible by  $n$ .

## 1.4 Equivalence Classes (同値類)

If we consider the equivalence relation established by the integers modulo 3, then

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

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

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

Notice that  $[0] \cup [1] \cup [2] = \mathbb{Z}$  and also that these sets are **disjoint**. The sets  $[0]$ ,  $[1]$ , and  $[2]$  form a **partition** (分割) of the integers.

### Notice:

The **integers modulo  $n$**  are a very important example in the study of abstract algebra and will become quite useful in our investigation of various algebraic structures such as **groups** and **rings**.

# Review for Lecture 1

- Sets
- Relation, Mapping
- Invertible
- Quotient, Remainder, Greatest Common Divisor
- Equivalence Classes
- Modulo

# 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)

## Definition

The union of  $A_1, A_2, \dots, A_n$ , denoted by  $\bigcup_{i=1}^n A_i$  or  $A_1 \cup A_2 \cup \dots \cup A_n$ , is the set of all elements  $x$  such that  $x$  is an element of some  $A_i$ , where  $1 \leq i \leq n$ .

The intersection of  $A_1, A_2, \dots, A_n$ , denoted by  $\bigcap_{i=1}^n A_i$  or  $A_1 \cap A_2 \cap \dots \cap A_n$ , is the set of all elements  $x$  such that  $x \in A_i$  for all  $1 \leq i \leq n$ .

# Appendix (付録)

## Definition

Let  $A$  be a set and  $\mathcal{P}$  be a collection of nonempty subsets of  $A$ . Then  $\mathcal{P}$  is called a **partition** (分割) of  $A$  if the following properties are satisfied:

- (i) for all  $B, C \in \mathcal{P}$ , either  $B = C$  or  $B \cap C = \emptyset$ .
- (ii)  $A = \bigcup_{B \in \mathcal{P}} B$ .

# Appendix (付録)

## Definition

For any set  $X$ , the **power set of  $X$** , written  $\mathcal{P}(X)$ , is defined to be the set  $\{A \mid A \text{ is a subset of } X\}$ .

## Example

Let  $X = \{1, 2, 3\}$ . Then

$$\mathcal{P}(X) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}.$$

Here  $\mathcal{P}(X)$  has  $2^3$  elements.

# Appendix (付録)

## Theorem

Let  $f: A \rightarrow B$ ,  $g: B \rightarrow C$ , and  $h: C \rightarrow D$ . Then

1. The composition of mappings is associative; that is,  $(h \circ g) \circ f = h \circ (g \circ f)$ ;
2. If  $f$  and  $g$  are both *one-to-one*, then the mapping  $g \circ f$  is *one-to-one*;
3. If  $f$  and  $g$  are both *onto*, then the mapping  $g \circ f$  is *onto*;
4. If  $f$  and  $g$  are *bijective*, then so is  $g \circ f$ .