# 1 Sets (集合)

## 1.1 Sets

**Definition 1.1** [**Set (集合)** ] A *set* is a collection of objects. The objects that make up a set are called its *elements* (or members). When $a$ is an element of a set $A$, we say that $a$ belongs to $A$ and wirte

$$a \in A \text{ or } A \ni a.$$

If $a$ is not a member of $A$, we write

$$a \notin A \text{ or } A \not\ni a.$$

We consider a set with no elements and call the *empty set*（空集合）, *null set* or *void set*. The empty set is denoted by $\emptyset$ or $\{\ \}$.

The number of elements in a set $S$ is denoted by $|S|$. The $|S|$ is also referred to as the *cardinal number*（基数） or *cardinality*（濃度） of $S$. A set $S$ is *finite* if $|S| = n$ for some nonnegative integer $n$. A set $S$ is *infinite* if it is not finite.

**Example 1.1**

1. $\boldsymbol{N}, \boldsymbol{Z}, \boldsymbol{Q}, \boldsymbol{R}, \boldsymbol{C}$, where $\boldsymbol{N} = \{1, 2, \ldots, \}$, the set of positive integers.
2. $S = \{x : x^2 - 2 = 0\} = \{\sqrt{2}, -\sqrt{2}\}$. Unless it is clear by context, we write $S = \{x : x \in \boldsymbol{R} \text{ and } x^2 - 2 = 0\}$ or $S = \{x \in \boldsymbol{R} : x^2 - 2 = 0\}$. Note that $\{x \in \boldsymbol{Q} : x^2 - 2 = 0\} = \emptyset$.

## 1.2 Inclusion and Set Operations（包含関係と集合演算）

**Definition 1.2**

1. A set $A$ is called a *subset* of a set $B$ if every element of $A$ belongs to $B$. If $A$ is a subset of $B$, then we write $A \subseteq B$ or $B \supseteq A$.
2. Two sets $A$ and $B$ are *equal* and we write $A = B$ if they have exactly same elements. This is equivalent to say that $A = B$ if and only if $A \subseteq B$ and $B \subseteq A$.
3. A set $A$ is a *proper subset*（真部分集合） of a set $B$ if $A \subseteq B$ and $A \neq B$.
4. The *union*（和集合） of two sets $A$ and $B$, denoted by $A \cup B$, is the set of all elements belonging to $A$ or $B$; that is
$$A \cup B = \{x \mid x \in A \text{ or } x \in B\}.$$
5. The *intersection*（共通集合） of two sets $A$ and $B$, denoted by $A \cap B$, is the set of all elements belonging to both $A$ and $B$; that is
$$A \cap B = \{x \mid x \in A \text{ and } x \in B\}.$$
6. If two sets $A$ and $B$ have no elements in common, then $A \cap B = \emptyset$, $A$ and $B$ are said to be *disjoint*（互いに素）.
7. The *difference*（差集合） $A - B$ of two sets $A$ and $B$ (also written as $A \setminus B$ is defined as
$$A - B = \{x \mid x \in A \text{ and } x \notin B\}.$$
8. We are ordinarily concerned with subsets of some specified set $U$, called the *universal set*. In this case for a subset $A$ of $U$, $U - A$ is denoted by $\overline{A}$ and called the *complement*（補集合） of $A$.
9. The set containing of all subsets of a given set $A$ is called the *power set*（冪集合） of $A$ and is denoted by $\mathcal{P}(A)$.

## 1.3 Indexed Collections of Sets（添え字付き集合族）

**Definition 1.3** 1. The union and intersection of the $n \geq 2$ sets $A_1, A_2, \ldots, A_n$ are denoted by

$$A_1 \cup A_2 \cup \cdots \cup A_n = \bigcup_{i=1}^{n} A_i = \{x : x \in A_i \text{ for some } i, 1 \leq i \leq n\}.$$

$$A_1 \cap A_2 \cap \cdots \cap A_n = \bigcap_{i=1}^{n} A_i = \{x : x \in A_i \text{ for all } i, 1 \leq i \leq n\}.$$

2. We also use the notation using an *index set* to describe a collection of sets $\{S_\alpha\}_{\alpha \in I}$. It is called an *indexed collection of sets*. Moreover,

$$\bigcup_{\alpha \in I} A_\alpha = \{x : x \in A_\alpha \text{ for some } \alpha \in I\}, \quad \bigcap_{\alpha \in I} A_\alpha = \{x : x \in A_\alpha \text{ for all } \alpha \in I\}.$$

**Example 1.2**

$$A_n = \left\{x \in \boldsymbol{R} : -\frac{1}{n} \leq x \leq \frac{1}{n}\right\} = \left[-\frac{1}{n}, \frac{1}{n}\right], \quad \bigcup_{n \in \boldsymbol{N}} A_n = [-1, 1], \qquad \bigcap_{n \in \boldsymbol{N}} A_n = \{0\}.$$

## 1.4 Partitions of Sets（集合の分割）

**Definition 1.4** 1. A collection $\mathcal{S}$ of subsets of a set $A$ is called *pairwise disjoint* if every two distinct subsets that belong to $\mathcal{S}$ are disjoint.

2. A partition of $A$ is a collection $\mathcal{S}$ of nonempty subsets of $A$ such that every element of $A$ belongs to exactly one member of $\mathcal{S}$. Equivalently, a partition of a set $A$ is a collection $\mathcal{S}$ of subsets of $A$ satisfying the following three properties:

   (1) $X \neq \emptyset$ for every set $X \in \mathcal{S}$.

   (2) For every two sets $X, Y \in \mathcal{S}$, either $X = Y$ or $X \cap Y = \emptyset$.

   (3) $\displaystyle\bigcup_{X \in \mathcal{S}} X = A$.

**Example 1.3** For $i = 0, 1, 2$, let $A_i = \{3n + i : n \in \boldsymbol{Z}\}$. Then $\{A_0, A_1, A_2\}$ is a partition of $\boldsymbol{Z}$.

## 1.5 Cartesian Product of Sets（集合の直積）

**Definition 1.5** 1. The ordered pair $(x, y)$ is a single element consisting of a pair of elements in which $x$ is the first element (or first coordinate) of the ordered pair $(x, y)$ and $y$ is the second element (or second coordinate). Moreover $(x, y) = (w, z)$ if and only if $x = w$ and $y = z$.

2. The *Cartesian product* (or simply the product) $A \times B$ of two sets $A$ and $B$ is the set consisting of all ordered pairs whose first coordinate belongs to $A$ and whose second coordinate belongs to $B$. In other words,

$$A \times B = \{(a, b) : a \in A \text{ and } b \in B\}.$$

3. If both $A$ and $B$ are finite sets, then $|A \times B| = |A| \cdot |B|$.

**Example 1.4**

$$\{(x, y) \in \boldsymbol{R} \times \boldsymbol{R} : y = 2x + 3\}.$$

**Russel's Paradox (1903):** Let $S$ be the set of all sets. Let

$$C_1 = \{M \in S \mid M \notin M\},\ C_2 = \{M \in S \mid M \in M\}.$$

Both $C_1 \in C_1$ and $C_1 \notin C_1$ imply a contradiction. ■

**Reference:** 「新装版：集合とはなにか (はじめて学ぶ人のために)」竹内外史著、講談社 (BLUE BACKS B1332 ISBN4-06-257332-6, 2001.5.20) を参考にしてください。

### 1.6 Exercises from Chapter 3

**Homework:** Chapter 3. Sets Exercises 45 (indexed), 46 (partition), 63 (product), 69 (list), 73 (cardinality)

**Recitation Problems:** Chapter 3. Sets Exercises 25, 27, 29, 31, 33, 34, 35, 36, 38, 40, 42, 44, 52, 59, 64, 65, 66, 69, 73, 77

## 2 Logic (論理)

### 2.1 Statements（命題）

**Definition 2.1**

1. A *statement* is a declarative sentence or assertion that is true or false (but not both).

   eg. The integer 3 is odd. The integer 57 is prime.

2. Every statement has a *truth value*, namely *true* (denoted by $T$) or *false* (denoted by $F$).

3. An *open sentence* is a declarative sentence when that contains one or more variables, each variable representing a value in some prescribed set, called the *domain* of the variable, and which becomes a statement when values from their respective domains are substituted for these variables.

   eg. $3x = 12$. An integer $x$ is prime.

**Example 2.1** An open sentence

$$P(x) : (x - 3)^2 \leq 1.$$

over the domain $\boldsymbol{Z}$ is a true statement when $x \in \{2, 3, 4\}$, and a false statement otherwise.

### 2.2 Negation, Disjunction, Conjunction and Implication

**Definition 2.2** [Logical Connectives, Compound Statement of Component Statements]

1. Truth table（真理表）

2. The *negation*（否定） of a statement $P$ is the statement 'not $P$' and is denoted by $\sim P$.

3. The *disjunction, i.e, logical or*（離接・論理和） of the statements $P$ and $Q$ is the statement '$P$ or $Q$' and is denoted by $P \vee Q$.

4. The *conjunction, i.e., logical and*（合接・論理積） of the statements $P$ and $Q$ is the statement '$P$ and $Q$' and is denoted by $P \wedge Q$.

5. The *implication*（含意） is the statement 'If $P$, then $Q$' and is denoted by $P \Rightarrow Q$. We also express $P \Rightarrow Q$ in words as '$P$ implies $Q$'.

6. For statements (or open sentences) $P$ and $Q$, the implication $Q \Rightarrow P$ is called the *converse*（逆） of $P \Rightarrow Q$.

7. The statement (or open statement) $P$ and $Q$, the conjunction

$$(P \Rightarrow Q) \wedge (Q \Rightarrow P)$$

of the implication $P \Rightarrow Q$ and its converse is called the *biconditional* of $P$ and $Q$ and is denoted by $P \Leftrightarrow Q$. The biconditional $P \Leftrightarrow Q$ is often stated as '$P$ is equivalent to $Q$'（同値な論理命題） or '$P$ if and only if $Q$'. or as '$P$ is a necessary and sufficient condition for $Q$'（必要十分条件）.

8. A compound statement is called a *tautology*（トートロジー・恒真命題） if it is true for all possible combinations of truth values of the component statements.

9. A compound statement is called a *contradiction*（矛盾） if it is false for all possible combinations of truth values（真理値） of the component statements.

$\sim P$, $P \vee Q$, $P \wedge Q$, $P \Rightarrow Q$, $P \Leftrightarrow Q$

| $P$ | $\sim P$ |
|---|---|
| $T$ | $F$ |
| $F$ | $T$ |

| $P$ | $Q$ | $P \vee Q$ | $P \wedge Q$ | $P \Rightarrow Q$ | $P \Leftrightarrow Q$ |
|---|---|---|---|---|---|
| $T$ | $T$ | $T$ | $T$ | $T$ | $T$ |
| $T$ | $F$ | $T$ | $F$ | $F$ | $F$ |
| $F$ | $T$ | $T$ | $F$ | $T$ | $F$ |
| $F$ | $F$ | $F$ | $F$ | $T$ | $T$ |

**Exercise 2.1** Complete the following truth table.

1. $(\sim P) \vee Q$
2. $(\sim Q) \Rightarrow (\sim P)$
3. $(P \wedge Q) \Rightarrow \sim Q$
4. $((\sim P) \vee Q) \Rightarrow P$
5. $((P \Rightarrow Q) \wedge (Q \Rightarrow R)) \Rightarrow (P \Rightarrow R)$

| $P$ | $Q$ | $(\sim P) \vee Q$ | $(\sim Q) \Rightarrow (\sim P)$ | $(P \wedge Q) \Rightarrow \sim Q$ | $((\sim P) \vee Q) \Rightarrow P$ |
|---|---|---|---|---|---|
| $T$ | $T$ | | | | |
| $T$ | $F$ | | | | |
| $F$ | $T$ | | | | |
| $F$ | $F$ | | | | |

| $P$ | $Q$ | $R$ | $((P \Rightarrow Q) \wedge (Q \Rightarrow R)) \Rightarrow (P \Rightarrow R)$ | $P \vee (Q \wedge R)$ | $(P \vee Q) \wedge R$ |
|---|---|---|---|---|---|
| $T$ | $T$ | $T$ | | | |
| $T$ | $T$ | $F$ | | | |
| $T$ | $F$ | $T$ | | | |
| $T$ | $F$ | $F$ | | | |
| $F$ | $T$ | $T$ | | | |
| $F$ | $T$ | $F$ | | | |
| $F$ | $F$ | $T$ | | | |
| $F$ | $F$ | $F$ | | | |

## 2.3 Logical Equivalence

Whenever two (compound（合成）) statements $R$ and $S$ have the same truth values for all combinations of truth values of their component statements, then we say that $R$ and $S$ are *logically equivalent*（論理同値） and indicated by writing $R \equiv S$.

$$(\sim P) \vee Q \equiv (\sim Q) \Rightarrow (\sim P) \equiv P \Rightarrow Q$$

## 2.4 Some Fundamental Properties of Logical Equivalence

**Proposition 2.1** *The following hold.*

(1) $P \vee P \equiv P$.

(2) $P \wedge P \equiv P$.

(3) $\sim(\sim P) \equiv P$.

(4) $P \vee Q \equiv Q \vee P$.

(5) $(P \vee Q) \vee R \equiv P \vee (Q \vee R)$.

(6) $P \wedge Q \equiv Q \wedge P$.

(7) $(P \wedge Q) \wedge R \equiv P \wedge (Q \wedge R)$.

(8) $P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R)$.

(9) $P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R)$.

(10) $\sim(P \vee Q) \equiv (\sim P) \wedge (\sim Q)$.

(11) $\sim(P \wedge Q) \equiv (\sim P) \vee (\sim Q)$.

## 2.5 Quantified Statements

Universal quantifier and existential quantifier. See Section 4 as well.

## 2.6 Characterization of Statements

We say that the concept is *characterized* by $Q(x)$ if

$$\forall x \in S, P(x) \Leftrightarrow Q(x).$$

See Section 4 as well.

## 2.7 Exercises from Chapter 2. Logic

**Homework:** 2.5, 16, 31, 40, 75

**Recitation Problems:** 2.3, 5, 8, 18, 22, 23, 24, 29, 33, 43, 44, 48, 49, 62, 70, 71, 73, 75, 76, 77

# 3 Direct Proof and Proof by Contrapositive

## 3.1 Proof of Implication $P \Rightarrow Q$

$$\forall x \in S, P(x) \Rightarrow Q(x).$$

| $P$ | $Q$ | $P \Rightarrow Q$ | $\sim P \vee Q$ | $\sim Q \Rightarrow \sim P$ |
|---|---|---|---|---|
| $T$ | $T$ | $T$ | $T$ | $T$ |
| $T$ | $F$ | $F$ | $F$ | $F$ |
| $F$ | $T$ | $T$ | $T$ | $T$ |
| $F$ | $F$ | $T$ | $T$ | $T$ |

**Vacuous Proof**

**Example 3.1** 1. $\forall x \in \boldsymbol{R},\ x < 0 \Rightarrow x^2 + 1 > 0$.

$\forall x \in \boldsymbol{R},\ x^2 + 1 > 0$.

2. $\forall x \in \boldsymbol{R},\ x^2 - 2x + 2 \leq 0 \Rightarrow x^3 \geq 8$.

$\forall x \in \boldsymbol{R},\ x^2 - 2x + 2 > 0$.

**Types of Proofs**

1. Direct Proof
2. Proof by Contrapositive
3. Proof by Cases

**Example 3.2** Let $x \in \boldsymbol{Z}$. If $5x - 7$ is even, then $x$ is odd.

**Example 3.3** Let $x \in \boldsymbol{Z}$. Then $x^2$ is even if and only if $x$ is even.

$$\forall x \in \boldsymbol{Z},\ x^2\text{: even } \Leftrightarrow x\text{: even.}$$

*Proof.* We prove in the following two steps.

(1) If $x$ is even, then $x^2$ is even.

(2) If $x$ is odd, then $x^2$ is odd.
($x$ is not even, then $x^2$ is not even.)

This proves the assertion. ■

**Example 3.4** Let $x \in \boldsymbol{Z}$. If $5x - 7$ is odd, then $9x + 2$ is even.

**Example 3.5** For $x, y \in \boldsymbol{Z}$. Then $x$ and $y$ are of the same parity if and only if $x + y$ is even.

**Example 3.6** Let $A$ and $B$ be sets. Then $A \cup B = A$ if and only if $B \subseteq A$.

*Proof.* We prove in the following two steps.

(1) If $A \cup B = A$, then $B \subseteq A$.

(2) If $B \subseteq A$, then $A \cup B = A$.

(1') If $B \not\subseteq A$ then $A \cup B \neq A$.
$\sim (\forall x,\ x \in B \Rightarrow x \in A) \equiv \exists x, x \in B \wedge x \notin A$.

This proves the assertion. ■

## 3.2 Divisibility of Integers

Let $a, b \in \boldsymbol{Z}$. The integer $a$ divides $b$ If there exists $c \in \boldsymbol{Z}$ such that $b = ac$. When $a$ divides $b$, we write $a \mid b$. If $a$ does not divide $b$, we write $a \nmid b$.

$$\forall a \in \boldsymbol{Z}, \forall b \in \boldsymbol{Z}, a \mid b \Leftrightarrow \exists c \in \boldsymbol{Z}, b = ac.$$

**Proposition 3.1** *Let $a, b, c \in \boldsymbol{Z}$.*

(i) *Always* $1 \mid a$, $a \mid 0$ *and* $0 \mid a \Leftrightarrow a = 0$.

(ii) $(a \mid b) \wedge (b \mid c) \Rightarrow a \mid c_\circ$

(iii) $(a \mid b) \wedge (b \mid a) \Leftrightarrow a = \pm b$.

(iv) $(a \mid b) \wedge (a \mid c) \Leftrightarrow a \mid bx + cy$ *for all integers* $x, y$.

## 3.3 Congruence of Integers

Let $m$ be positive integer. For $a, b \in \boldsymbol{Z}$, $a$ is *congruent to $b$ modulo $m$* if $m \mid a - b$. In this case we write $a \equiv b \pmod{m}$.

$$a \equiv b \pmod{m} \Leftrightarrow m \mid a - b.$$

**Lemma 3.2** *The following hold.*

(i) $a \equiv a \pmod{m}$.

(ii) $a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$.

(iii) $(a \equiv b \pmod{m}) \wedge (b \equiv c \pmod{m}) \Rightarrow a \equiv c \pmod{m}$.

**Proposition 3.3** *For integers $a, b, c, d$ and a positive integer $n$, suppose $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. Then the following hold.*

(i) $a + c \equiv b + d \pmod{n}$.

(ii) $ac \equiv bd \pmod{n}$.

## 3.4 Exercises from Chapter 4

**Homework:** 4.3, 13, 19, 32, 37

**Recitation Problems:** 7, 10, 18, 20, 24, 26, 35, 36, 38, 40, 47, 51, 54, 55, 60, 61, 63, 64, 66

## 3.5 Exercises from Chapter 5

**Homework:** 5.3, 19, 34, 40, 67

**Recitation Problems:** 4, 8, 10, 16, 20, 22, 26, 28, 32, 46, 56, 58, 60, 66, 70, 85, 89, 96, 99

# 4 Existence Proof and Proof by Contradiction

## 4.1 Quantified Statements

**Open Statement:** $P(x)$. $2x \geq 1$.

**Quantified Statement:** An open statement can be converted to a statement by a quantifier. 限定記号

**Universal Quantifier:** $\forall x \in \boldsymbol{R}, e^x > 0$, $\forall x \in \boldsymbol{R}, e^x \geq 1$. 全称記号・全称命題

**Existential Quantifier:** $\exists x \in \boldsymbol{R}, e^x = 2$, $\exists x \in \boldsymbol{R}, e^x = 0$. 存在記号・存在命題

## 4.2 Counter Example（反例）

$$\sim (\forall x \in S, R(x)) \equiv \exists x \in S, \sim R(x), \quad \sim \left( \bigwedge_{x \in S} R(x) \right) \equiv \bigvee_{x \in S} (\sim R(x)).$$

**Example 4.1** 1. If $x$ is a real number, then $\tan^2 x + 1 = \sec^2 x$.

$$\forall x \in \boldsymbol{R}, \tan^2 x + 1 = \sec^2 x.$$

For $x = \pi/2 + k\pi$, the right hand side is not defined.

Whenever both hand sides are defined, $\tan^2 x + 1 = \sec^2 x$.

2. Let $n \in \boldsymbol{Z}$. If $n^2 + 3n$ is even, then $n$ is odd.

   The number 2 is a counter example. Note that $n^2 + 3n = n(n+3)$ is even for every integer $n$. It is true that every even integer is a counter example. But ....

3. For all non-negative integer $n$, $F(n) = 2^{2^n} + 1$ is a prime.

   $F(0) = 3$, $F(1) = 5$, $F(2) = 17$, $F(3) = 257$, $F(4) = 65537$, $F(5) = 4294967297 = 641 \cdot 6700417$.

4. Mersenne Prime: $M(p) = 2^p - 1$, where $p$ is prime.

**Sage Program**

```
def me(n):
    v = []
    for i in prime_range(2,n):
        if is_prime(2^i-1):
                v.append(i)
    return v

m=me(1000);m
```

```
[2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607]
```

URL http://www.sagemath.org
日本語による SageMath 入門：
URL http://subsite.icu.ac.jp/people/hsuzuki/science/computer/education/sage-j.html

## 4.3 Proof by Contradiction（背理法による証明）

If $R: \forall x \in S, P(x) \Rightarrow Q(x)$, then a proof by contradiction might begin with

> Assume, to the contrary, that there exists some element $x \in S$ for which $P(x)$ is true and $Q(x)$ is false.

**Example 4.2** Let $p$ be a prime. Then $\sqrt{p}$ is irrational.

## 4.4 Existence Proofs（存在証明）

$$\exists x \in S, R(x): \text{ There exists } x \in S \text{ such that } R(x).$$

**Example 4.3** There exist irrational numbers $a$ and $b$ such that $a^b$ is rational.

*Proof.* *Case 1.* $\sqrt{2}^{\sqrt{2}}$ is rational.
Then set $a = b = \sqrt{2}$.
*Case 2.* $\sqrt{2}^{\sqrt{2}}$ is irrational.
Then set $a = \sqrt{2}^{\sqrt{2}}$ and $b = \sqrt{2}$. ■

**Example 4.4** The equation $x^5 + 2x - 5 = 0$ has a unique real number solution between $x = 1$ and $x = 2$.

*Proof.* Let $f(x) = x^5 + 2x - 5$. Then $f(1) = -2$ and $f(2) = 31$. $f(x)$ is continuous. Thus by the Intermediate Value Theore, the assertion holds.

For $1 < a < b < 2$, $a^5 + 2a - 5 < b^5 + 2b - 5$. Or $f'(x) = 5x^4 + 2 > 0$ and $f(x)$ is increasing. So if $a < b$, then $f(a) < f(b)$. ■

**Example 4.5** Let $a$ be a real number. For each integer $Q > 1$, there exist integers $p$, $q$ with $0 < q < Q$ such that $|qa - p| \leq 1/Q$. In this case $|a - \frac{p}{q}| \leq \frac{1}{Q}$.

## 4.5 Principle of Mathematical Induction（数学的帰納法の原理）

**Definition 4.1** A nonempty subset $S$ of real numbers is said to be *well-ordered*（整列集合） if every nonempty subset of $S$ has a least element, which is unique. The least element of a set $T$ is denoted by $\min T$ and

$$m = \min T \Leftrightarrow m \in T, \text{ and } \forall x \in T, m \leq x.$$

**The Well-Ordering Principle:** The set $\boldsymbol{N}$ of positive integers is well-ordered.

Every nonempty subset of a well-ordered set is well-ordered and hence every nonempty finite subset $S$ of real numbers is well-ordered.

**Theorem 4.1 (Theorem 6.2 (The Principle of Mathematical Induction))** *For each positive integer $n$, let $P(n)$ be a statement. If*

(1) *$P(1)$ is true and*

(2) *the implication*

$$\textit{If } P(k), \textit{ then } P(k+1)$$

*is true for every positive integer $k$,*

*then $P(n)$ is true for every positive integer $n$.*

## 4.6 Exercises from Chapter 6

**Homework:** 6.14, 20, 26, 40, 49

**Recitation Problems:** 7, 8, 11, 22, 29, 32, 37, 44, 48, 50, 55, 60, 61, 62, 64

## 4.7 Exercises from Chapter 7

**Homework:** 7.1, 5, 11, 18, 24

**Recitation Problems:** 2, 4, 8, 9, 12, 13, 14, 15, 16, 17, 19, 20, 22, 23, 25

# 5 Mathematical Induction (数学的帰納法)

## 5.1 General Principles of Mathematical Induction

**Definition 5.1** [Review] An nonempty set $S$ of real numbers is said to be *well-ordered* if every nonempty subset of $S$ has a least element $\min S$, i.e.,

$$m = \min S \Leftrightarrow m \in S, \text{ and } \forall x \in S,\ m \le x.$$

**Well-Ordered Set:** For each integer $m \in \boldsymbol{Z}$, the set $S = \{i \in \boldsymbol{Z} : i \ge m\}$ is well-ordered.

**Principle of Mathematical Induction:** $(P(m) \wedge (\forall k \ge m, P(k) \Rightarrow P(k+1)) \Rightarrow (\forall n \ge m, P(n))$.

Every nonempty subset of a well-ordered set is well-ordered and hence every nonempty finite subset $S$ of real numbers is well-ordered.

**Theorem 5.1 (The Strong Principle of Mathematical Induction)** *For a fixed integer $m$, let $S = \{i \in \boldsymbol{Z} : i \ge m\}$. For each integer $n \in S$, let $P(n)$ be a statement. If,*

(1) *$P(m)$ is true and*

(2) *the implication;*

*if $P(k)$ is true <u>for every integer $i$ with $m \le i \le k$</u>, then $P(k+1)$*

*is true for every integer $k \in S$,*

*then $P(n)$ is true for every integer $n \in S$.*

**Example 5.1** 1. For every integer $n \ge 5$, $2^n > n^2$.

*Proof.* For $k \ge 3$, $2^{k+1} = 2 \cdot 2^k > 2k^2 = k^2 + k^2 \ge k^2 + 3k > k^2 + 2k + 1 = (k+1)^2$. Note that we need $n \ge 5$. ■

2. A sequence $\{a_n\}$ is defined recursively by

$$a_1 = 1,\ a_2 = 4, \text{ and } a_n = 2a_{n-1} - a_{n-2} + 2 \text{ for } n \ge 3.$$

Conjecture a formula for $a_n$ and verify that your conjecture is correct.

$$a_1 = 1,\ a_2 = 4,\ a_3 = 9,\ a_4 = 16, \ldots,$$

Conjecture: $a_n = n^2$.

*Proof.* The conjecture is valud when $n = 1, 2$. Now for $k \ge 2$,

$$a_{k+1} = 2a_k - a_{k-1} + 2 = 2k^2 - (k-1)^2 + 2 = 2k^2 - k^2 + 2k - 1 + 1 = (k+1)^2. \quad ■$$

3. Let $a, b, p, q$ be constants. Suppose a sequence $\{a_n\}$ satisfies the following.

$$a_1 = a, a_2 = b,\ a_n = pa_{n-1} + qa_{n-2}, \text{ for } n \ge 3.$$

Let $\alpha, \beta$ be roots of $x^2 - px - q = 0$. Then

$$a_n = \begin{cases} \frac{1}{\beta-\alpha}((\beta^{n-1} - \alpha^{n-1})b + (\alpha^{n-1}\beta - \alpha\beta^{n-1})a & \text{if } \alpha \ne \beta \\ (n-1)\alpha^{n-2}b - (n-2)\alpha^{n-1}a & \text{if } \alpha = \beta. \end{cases}$$

*Proof.* It is clear that $a_1 = a$ and $a_2 = b$ in both cases.

Suppose $\alpha \neq \beta$ and $n \geq 3$. Then by induction hypothesis,

$$\begin{aligned}
a_n &= \frac{1}{\beta-\alpha}(p((\beta^{n-2}-\alpha^{n-2})b+(\alpha^{n-2}\beta-\alpha\beta^{n-2})a)+q(\beta^{n-3}-\alpha^{n-3})b+(\alpha^{n-3}\beta-\alpha\beta^{n-3})a) \\
&= \frac{1}{\beta-\alpha}((p\beta+q)\beta^{n-3}-(p\alpha+q)\alpha^{n-3})b+((p\alpha+q)\alpha^{n-3}\beta-(p\beta+q)\alpha\beta^{n-3})a) \\
&= \frac{1}{\beta-\alpha}((\beta^{n-1}-\alpha^{n-1})b+(\alpha^{n-1}\beta-\alpha\beta^{n-1})a.
\end{aligned}$$

The other case is similar and left as your exercise. ■

**Example 5.2** Every positive number $n \geq 2$ is either a prime[1] or a product of primes.

*Proof.* Let $n$ be an integer at least 2. Suppose $n$ is not a prime. Then there exist positive integers $2 \leq m_1, m_2 \leq n$ such that $n = m_1 m_2$, Since $m_1, m_2 < n$, each of these is a prime or a product of primes. ■

**Example 5.3** For each integer $n \geq 8$, there are nonnegative integers $a$ and $b$ such that $n = 3a + 5b$.

*Proof.* (i) OK for $n = 8, 9, 10$. Assume $k + 1 \geq 11$, Then $k - 2 \geq 8$ hence,

$$k + 1 = (k - 2) + 3 = 3a + 5b + 3 = 3(a + 1) + 5b. \quad ■$$

**Example 5.4** Let $a, b \in \boldsymbol{Z}$. Then there is an integer $d$ satisfying the following three conditions.

$$\text{(i) } d \geq 0, \quad \text{(ii) } d \mid a \text{ and } d \mid b, \quad \text{(iii) } c \mid a \text{ and } c \mid b \text{ implies } c \mid d.$$

The integer $d$ is uniquely determined and it is called the *greatest common divisor* of $a$ and $b$. The greatest common divisor $d$ of $a$ and $b$ is denoted by $d = \gcd\{a, b\}$. In this case, there are $x, y \in \boldsymbol{Z}$ such that $d = ax + by$.

*Proof.* In the following we show that there is an integer $d = ax + by$ ($x, y \in \boldsymbol{Z}$) satisfying (i), (ii), (iii).

If $a = b = 0$, then $d = 0$ with $x = y = 0$ satisfies the condition. So assume that $a \neq 0$ or $b \neq 0$. Let

$$S = \{ax + by > 0 \mid x \in \boldsymbol{Z},\ y \in \boldsymbol{Z}\} \subseteq \boldsymbol{N}.$$

Since $a \neq 0$ or $b \neq 0$, for $x = a$, $y = b$ $ax + by = a^2 + b^2 > 0$ and $S \neq \emptyset$. Thus by well-ordered principle applied to $\boldsymbol{N}$, $S$ has a least element $d$. Since $d > 0$, it satisfies (i). By definition of $S$ there is an expression $d = ax + by$ with $x, y \in \boldsymbol{Z}$. Suppose $c \mid a$ and $c \mid b$. Since $d = ax + by$, $c \mid d$, and we have (iii). Suppose $d \nmid a$. Then we have $a = dq + r$ for some integers $q$ and $r$ with $0 < r < d$. Now $r = a - dq = a - (ax + by)q = a(1 - qx) + b(-qy)$, and by the definition of $S$ $r \in S$. This is absurd as $r < d$ and $d$ is the least element of $S$. Therefore $d \mid a$. Similarly, $d \mid b$. Thus $d$ satisfies (ii) and $d$ has desirable properties.

Suppose $d'$ satisfies the same conditions. Since $d'$ satisfies (ii) and $d$ satisfies (iii), $d' \mid d$. Similarly, $d \mid d'$. By (i), we have $d = d'$. Thus the integer satisfying (i), (ii), (iii) is unique. ■

**Exercise 5.1** Let $a, b$ be integers with $\gcd(a, b) = 1$. Then for each $\ell \geq ab$, there are nonnegarive integers $x, y$ such that $\ell = ax + by$.

## 5.2 Exercises from Chapter 7

**Homework:** 7.26, 30, 41, 44, 45

**Recitation Problems:** 27, 31, 32, 33, 40, 42, 43, 46, 52, 53, 57, 62, 63, 64, 67,

## 5.3 Exercises from Chapter 8

**Homework:** 8.16, 56, 70, 76, 78

**Recitation Problems:** 1, 2, 3, 5, 6, 7, 8, 29, 54, 58, 67, 68, 81, 88, 92

[1] A prime number $p$ is a positive integer at least 2 such that 1 and $p$ are the only positive divisors.

# 6 Relations (関係)

## 6.1 Relations

**Definition 6.1** Let $A$ and $B$ be two sets. By a *relation $R$ from $A$ to $B$* we mean a subset of $A \times B$, i.e., $R \subseteq A \times B$. If $(a, b) \in R$, then we say that $a$ is *related* to $b$ by $R$ and write $aRb$. If $(a, b) \notin R$, then $a$ is not related to $b$ by $R$.

Let $R$ be a relation from $A$ to $B$. Then the *domain* and the *range* are defined as follows.

$$\mathrm{dom}R = \{a \in A : (a, b) \in R \text{ for some } b \in B\}, \text{ and}$$

$$\mathrm{ran}R = \{b \in B : (a, b) \in R \text{ for some } a \in A\}.$$

By a *relation on a set* $A$, we mean a relation from $A$ to $A$.

Let $R$ be a relation on a set $A$.

(R) $(\forall a \in A)[aRa]$ (反射律, reflexive law).

(S) $(\forall a \in A)(\forall b \in A)[aRb \Rightarrow bRa]$ (対称律, symmetric law)

(A) $(\forall a \in A)(\forall b \in A)[(aRb \wedge bRa) \Rightarrow a = b]$ (反対称律, antisymmetric law)

(T) $(\forall a \in A)(\forall b \in A)(\forall c \in A)[(aRb \wedge bRc) \Rightarrow aRc]$ (推移律, transitive law)

**Example 6.1** The following are relations on a set.

1. $(\boldsymbol{Z}, \leq)$: $R_{\leq} = \{(a, b) \in \boldsymbol{Z} \times \boldsymbol{Z} : a \leq b\}$.
2. For a set $X$, $(\mathcal{P}(X), \subseteq)$.

Reflexive, antisymmetric and transitive relation is called an *ordering relation*（順序関係）. A set with an ordering relation is called a *poset* or a *partially ordered set*（半順序集合）.

## 6.2 Equivalence Relation

**Definition 6.2** A reflexive, symmetric and transitive relation on a set $A$ is called an *equivalence relation*. For a relation $\sim$ on a set $A$,

(i) $a \sim a$ for all $a \in A$.

(ii) $a \sim b$ implies $b \sim a$ for all $a, b \in A$.

(iii) $a \sim b$ and $b \sim c$ implies $a \sim c$ for all $a, b, c \in A$.

**Example 6.2** 1. Let $X$ be a set and let $Y$ be a subset of $X$. For $A, B \in \mathcal{P}(X)$, $A \cap Y = B \cap Y$ if and only if $A \sim_Y B$.

2. Let $X$ be the set of all lines on a plane. For $\ell, m \in X$, $\ell \parallel m$ if and only if $\ell$ is equal to $m$ or parallel to $m$.

3. Let $X$ be the set of all triangles on a plane. For $S, T \in X$, $S \propto T$ ($S \equiv T$) if and only if $S$ and $T$ are similar (or congruent).

4. Let $m$ be positive integer. For $a, b \in \boldsymbol{Z}$, $a$ is *congruent to $b$ modulo $m$* if $m \mid a - b$. In this case we write $a \equiv b \pmod{m}$.

$$a \equiv b \pmod{m} \Leftrightarrow m \mid a - b.$$

**Lemma 6.1** *The following hold.*

(i) $a \equiv a \pmod{m}$.

(ii) $a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$.

(iii) $(a \equiv b \pmod{m}) \wedge (b \equiv c \pmod{m}) \Rightarrow a \equiv c \pmod{m}$.

## 6.3 Equivalence Classes

Let $\sim$ be an equivalence relation defined on a set $A$. For $a \in A$ let

$$[a] = [a]_\sim = \{x \mid (x \in A) \wedge (x \sim a)\}.$$

The set $[a]$ is called the equivalence class of $a$（$a$ を含む同値類）.

**Proposition 6.2** *The following hold.*

(i) $(\forall a \in A)[a \in [a]]$.

(ii) $(\forall a \in A)(\forall b \in A)[b \in [a] \Rightarrow [a] = [b]]$.

(iii) $(\forall a \in A)(\forall b \in A)[[a] \cap [b] \neq \emptyset \Rightarrow [a] = [b]]$. (iii') $(\forall a \in A)(\forall b \in A)[[a] \neq [b] \Rightarrow [a] \cap [b] = \emptyset]$.

(iv) $A = \bigcup_{a \in A} [a]$.

**Example 6.3** Let $\equiv_3$ be the congruence relation modulo 3 on the set of integers $\boldsymbol{Z}$. Then $[0] = [3] = [6] = [-3]$, $[1] = [4] = [-2]$. We have $\boldsymbol{Z} = [0] \cup [1] \cup [2]$.

Recall the following.

**Proposition 6.3** *For integers $a, b, c, d$ and a positive integer $n$, suppose $a \equiv b \pmod n$ and $c \equiv d \pmod n$. Then the following hold.*

(i) $a + c \equiv b + d \pmod n$.

(ii) $ac \equiv bd \pmod n$.

**Proposition 6.4** *Let $[a] = \{x \in \boldsymbol{Z} : x \equiv a \pmod n\}$ for $a \in \boldsymbol{Z}$. The the following are well-defined.*

(i) $[a] + [b] = [a + b]$.

(ii) $[a][b] = [ab]$.

**Exercise 6.1** 1. If $n$ is an odd integer, $n^2 \equiv 1 \pmod 8$.

2. Let $n$ be an integer. Then $4n + 3$ cannot be written as a sum of two squares of integers.

3. If there is an integer $n$ satisfying $n^2 \equiv a \pmod 7$, $a \equiv 0, 1, 2, 4 \pmod 7$.

4. If $x$, $y$, and $z$ are integers satisfying $x^2 + y^2 = 6z^2$, then $x = y = z = 0$.

## 6.4 Exercises from Chapter 9

**Homework:** 9.1, 11, 25, 38, 45, 51, 58, 61, 65, 83

**Recitation Problems:** 24, 28, 30, 31, 32, 33, 34, 39, 40, 42, 53, 54, 57, 59, 71, 75, 76, 80, 81, 82

# 7 Functions (写像・関数)

## 7.1 The Definition of a Function

**Definition 7.1** Let $A$ and $B$ be nonempty sets. By a *function* (写像・関数) $f$ from $A$ to $B$, written $f : A \to B$, we mean a relation from $A$ to $B$ with the property that every element $a$ in $A$ is related to exactly one element in $A$.

$$f: \text{ a function from } A \text{ to } B \Leftrightarrow f \subseteq A \times B \text{ and } \forall a \in A, \exists_1 b \in B, (a, b) \in f.$$

When $f \subseteq A \times B$ is a function, we write

$$f : A \to B \ (a \mapsto f(a)),$$

where $(a, f(a)) \in f$, i.e., $f(a)$ is the unique element in $B$ such that $(a, f(a)) \in f$ and $b = f(a)$ is called the *image* (像) of $a$. We also say that $a$ is mapped to $b = f(a)$ or $f$ maps $a$ into $b$. $A$ is called the *domain* (定義域) of $f$ and $B$ the *codomain* (終域) of $f$.

$$\text{dom} f = \{a \in A : (a, b) \in f \text{ for some } b \in B\} = A, \text{ and}$$

$$\text{ran} f = \{b \in B : (a, b) \in f \text{ for some } a \in A\} = \{f(x) : x \in A\} = f(A).$$

is the range of $f$.

Two functions $f : A \to B$ and $g : C \to D$ are equal whenever $A = C$, $B = D$ and $f(x) = g(x)$ for all $x \in A$.

**Example 7.1**
1. $f = \{(x, x^2) : x \in \boldsymbol{R}\} \subseteq \boldsymbol{R} \times \boldsymbol{R}$. We also write $f : \boldsymbol{R} \to \boldsymbol{R} \ (x \mapsto x^2)$.
2. $g = \{(x, x^2) : x \in \boldsymbol{R}\} \subseteq \boldsymbol{R} \times \boldsymbol{R}^{\geq 0}$. We also write $g : \boldsymbol{R} \to \boldsymbol{R}^{\geq 0} \ (x \mapsto x^2)$.
3. $h = \{(x, x^2) : x \in \boldsymbol{R}^{\geq 0}\} \subseteq \boldsymbol{R}^{\geq 0} \times \boldsymbol{R}^{\geq 0}$. We also write $h : \boldsymbol{R}^{\geq 0} \to \boldsymbol{R}^{\geq 0} \ (x \mapsto x^2)$.

**Example 7.2**
1. $f : \boldsymbol{R} \to \boldsymbol{R} \ (x \mapsto e^x)$.
2. $f : \boldsymbol{R} \to \boldsymbol{R}^{\geq 0} \ (x \mapsto e^x)$.
3. $g : \boldsymbol{R} \to \boldsymbol{R} \ (x \mapsto \ln x)$. .................................................... This is not a function.
4. $h : \boldsymbol{R}^{>0} \to \boldsymbol{R} \ (x \mapsto \ln x)$.

**Example 7.3** [Dirichlet Function] $f : \boldsymbol{R} \to \boldsymbol{R} \ (x \mapsto f(x))$

$$f(x) = \begin{cases} 1 & \text{if } x \text{ is rational} \\ 0 & \text{if } x \text{ is irrational.} \end{cases}$$

**Example 7.4** Let $n$ be a positive integer.

$$f : \boldsymbol{Z}_n \to \boldsymbol{Z}_n \ ([x] \mapsto [3x]), \quad [x] = [y] \Rightarrow [3x] = [3y]?$$

## 7.2 One-to-one and Onto Function

**$B^A$:** The set of all functions from $A$ to $B$ is denoted by $B^A$ or $\text{Map}(A, B)$. Then $|B^A| = |B|^{|A|}$.

**One-to-one Function (Injection 単射):** A function $f : A \to B$ is *one-to-one* (or injection) if whenever $f(x) = f(y)$, where $x, y \in A$, then $x = y$.

$$\forall x \in A, \forall y \in A, f(x) = f(y) \Rightarrow x = y$$

**Onto Function (Surjection 全射):** A function $f : A \to B$ is *onto* (or surjection) if every element of $B$ is the image of an element of $A$, $\mathrm{ran}(f) = f(A) = B$.

$$\forall y \in B, \exists x \in A, f(x) = y.$$

**Bijection (全単射・双射):** A function $f : A \to B$ is said to be a *bijection* (one-to-one onto mapping) if it is both injective and surjective.

**Permutation (置換):** A bijection $f : A \to A$ is said to be a permutation on $A$.

**Image (像):** Let $f : A \to B$ be a function and $C \subseteq A$. Then $f(C) = \{f(c) : c \in C\}$.

**Preimage (原像):** Let $f : A \to B$ be a function and $C \subseteq B$. Then $f^{-1}(C) = \{x \in A : f(x) \in C\}$. When $C = \{c\}$, we write $f^{-1}(C)$ as $f^{-1}(c)$.

**Composition (合成):** Let $f : A \to B$, $g : B \to C$ be functions. Then the function $h$ from $A$ to $C$ defined by $h(x) = g(f(x))$ is called the compotion of $f$ and $g$. It is denoted by $h = g \circ f$.

**Identity (恒等写像):** $i_A : A \to A$ $(x \mapsto x)$ is called the *identity function* on $A$.

**Inverse (逆写像):** For functions $f : A \to B$, and $g : B \to A$, suppose $g \circ f = i_A$, and $f \circ g = i_B$. Then $g$ is called the *inverse* of $f$ and write $g = f^{-1}$.

**Example 7.5** 1. The function $f : \boldsymbol{Z}_4 \to \boldsymbol{Z}_6$ defined by $f([x]) = [3x + 1]$ is a well defined function.
If $x - y = 4m$, then $(3x + 1) - (3y + 1) = 12m$.

2. The function $g : \boldsymbol{Z}_6 \to \boldsymbol{Z}_4$ defined by $g([x]) = [3x + 1]$ is not well-defined.
$g([2]) = [3] \neq [1] = g([8])$.

**Example 7.6** 1. The functions

$$f : \boldsymbol{R} - \{2\} \to \boldsymbol{R} - \{3\} \ (x \to \frac{3x}{x-2} = 3 + \frac{6}{x-2}),\ g : \boldsymbol{R} - \{3\} \to \boldsymbol{R} - \{2\} \ (x \to \frac{2x}{x-3})$$

Suppose $f(x) = f(y)$. Then $3x(y - 2) = 3y(x - 2)$ and $x = y$. Hence $f$ is one-to-one. Set $f(x) = y$. Then $x = 2y/(y - 3)$. Hence if $y \neq 3$, then $f(x) = y$. Thus $\mathrm{ran}(f) = \boldsymbol{R} - \{3\}$. Since $f'(x) = -6/(x - 2)^2 < 0$, $f$ is decreasing. $\lim_{x \to \pm 2} f(x) = \pm\infty$.

2. $f(x) = \dfrac{x}{x^2 + 1}$. $\mathrm{ran}(f) = [-1/2, 1/2]$.

**Proposition 7.1** *Let $f : X \to Y$ be a function, and $A, B \subseteq X$, $C, D \subseteq Y$. Then*

(i) *$f(A \cup B) = f(A) \cup f(B)$, and $f(A \cap B) \subseteq f(A) \cap f(B)$. Equality holds if $f$ is one-to-one.*

(ii) *$f^{-1}(C \cup D) = f^{-1}(C) \cup f^{-1}(D)$, and $f^{-1}(C \cap D) = f^{-1}(C) \cap f^{-1}(D)$.*

(iii) *$A \subseteq f^{-1}(f(A))$, and equality holds if $f$ is one-to-one.*

(iv) *$f(f^{-1}(C)) \subseteq C$, and equality holds if $f$ is onto.*

**Theorem 7.2** *Let $f : A \to B$, $g : B \to C$ and $h : C \to D$ be functions.*

(i) *If $f$ and $g$ are one-to-one, then so is $g \circ f$.*

(ii) *If $f$ and $g$ are onto, then so is $g \circ f$.*

(iii) *If $f$ and $g$ are bijective, then so is $g \circ f$.*

(iv) *$(h \circ g) \circ f = h \circ (g \circ f)$.*

**Theorem 7.3** *Let $f : A \to B$, $g : B \to C$ be functions.*

(i) *If $g \circ f$ is one-to-one, then so is $f$.*

(ii) *If $g \circ f$ is onto, then so is $g$.*

(iii) *If $g \circ f$ is bijective, then $f$ is one-to-one and $g$ is onto.*

## 7.3 Exercises from Chapter 10

**Homework:** 10.5, 22, 24, 26, 32, 35, 42, 54, 56, 61

**Recitation Problems:** 10.4, 6, 9, 11, 12, 17, 19, 25, 29, 31, 33, 43, 45, 48, 51, 55, 58, 63, 67, 68, 70, 72, 74, 76, 77, 78, 81, 82, 83,

# 8 Cardinality of Sets (集合の濃度)

## 8.1 Numerically Equivalent Sets

**Definition 8.1** Two sets $A$ and $B$ are said to have the *same cardinality* (同じ濃度), written $|A| = |B|$, if either $A$ and $B$ are both empty or there is a bijective function $f$ from $A$ to $B$. Two sets having the same cardinality are also referred to as *numerically equivalent sets*.

**Proposition 8.1** *Let $\mathcal{S}$ be a nonempty collection of nonempty sets. For $A, B \in \mathcal{S}$, $A \sim B$ if and only if $A$ and $B$ are numerically equivalent. Then this is an equivalent relation.*

**Note.**

1. For $m, n \in \boldsymbol{N}$, the sets $\{1, 2, \ldots, m\}$ and $\{1, 2, \ldots, n\}$ are numerically equivalent if and only if $m = n$. So we write $|\{1, 2, \ldots, n\}| = n$ and say that the *cardinality* (基数、濃度) of the set $\{1, 2, \ldots, n\}$ is $n$.
2. The cardinality of $\boldsymbol{N}$ is called *aleph null* and is written $|\boldsymbol{N}| = \aleph_0$. (We will wirte $|\boldsymbol{R}| = \aleph$ or $c$ (*continuum*).

**Definition 8.2** A set $A$ is called *denumerable* if $|A| = |\boldsymbol{N}|$. A denumerable set is also called *countably infinite* (可算無限). A set is countable (可算) if it is either finite or denumerable. A set is called *uncountable* (非可算) if it is not countable.

**Example 8.1** 1. $|2\boldsymbol{Z}| = |\boldsymbol{Z}|$.

2. $|\boldsymbol{N}| = |\boldsymbol{Z}^{\geq 0}| = |\boldsymbol{Z}^{<0}|$.
3. $|\boldsymbol{Z}| = |\boldsymbol{N}|$.
$$f : \boldsymbol{N} \to \boldsymbol{Z} \ \left(n \mapsto \frac{1 + (-1)^n(2n-1)}{4}\right)$$
$f(1) = 0, f(2) = 1, f(3) = -1,\ f(2n) = n,\ f(2n+1) = -n.$
4. $|\boldsymbol{N}| = |\boldsymbol{N} \times \boldsymbol{N}|$. If $|A| = |B| = \aleph_0$ then $|A \times B| = \aleph_0$. (10.5)
$$h(m, n) = \frac{(m+n-1)(m+n-2)}{2} + n.$$
$h(1,1) = 1, h(2,1) = 2, h(1,2) = 3, h(3,1) = 4, h(2,2) = 5, h(1,3) = 6, \ldots.$
5. $|\boldsymbol{Q}^{>0}| = |\boldsymbol{N}|$, $|\boldsymbol{Q}| = |\boldsymbol{N}|$. (10.6), (10.7)
6. $|[a, b]| = |[0, 1]|$ and $|(a, b)| = |(0, 1)|$ for all $a < b$. Hence $|[a, b]| = |[c, d]|$.
7. $|(0, 1)| = |\boldsymbol{R}|$.
$$g : (0, 1) \to \boldsymbol{R} \ \left(x \mapsto \frac{1-2x}{x^2 - x} = -\frac{1}{x} - \frac{1}{x-1}\right)$$
$$h : (0, 1) \to \boldsymbol{R} \ \left(x \mapsto \tan \pi \left(x - \frac{1}{2}\right)\right)$$

**Proposition 8.2** *Suppose $A$, $B$, $C$, $D$ be sets with $A \sim C$ and $B \sim D$. Then the following hold.*

(i) *If $A \cap B = \emptyset = C \cap D$, then $A \cup B \sim C \cup D$.*

(ii) $A \times B \sim C \times D$.

(iii) $P(A) \sim P(C)$.

(iv) $\mathrm{Map}(A, B) \sim \mathrm{Map}(C, D)$.

**Proposition 8.3** *The following hold.*

(i) *Every infinite subset of a denumerable set is denumerable.*
*If there is a one-to-one function from an infinite set $A$ to a denumerable set $B$, then $|A| = \aleph_0$.*

(ii) *If there is an onto function from a denumerable set $B$ to an infinite set $A$, then $|A| = \aleph_0$.*

(iii) *If $A$ and $B$ are denumerable, then $A \times B$ is denumerable.*

**Proposition 8.4** $P(A) \sim \mathrm{Map}(A, \{0,1\})$.

**Proposition 8.5** *The open interval $(0,1)$ of real numbers is uncountable.*

*Proof.* Let $f : \boldsymbol{N} \to (0,1)$ be a bijection and write $f(n) = a_n = 0.a_{n1}a_{n2}\ldots$. Write $0.40\ldots$ rather than $0.399\ldots$. $b = 0.b_1b_2\ldots$,

$$b_i = \begin{cases} 4 & \text{if } a_{ii} = 5 \\ 5 & \text{if } a_{ii} \neq 5. \end{cases}$$

Then $b \notin f(\boldsymbol{N})$. ■

## 8.2 Comparing Cardinality of Sets

**Definition 8.3** Let $A$ and $B$ be set. We write $|A| \leq |B|$ if $A = \emptyset$ or there is a one-to-one function from $A$ to $B$. If $|A| \leq |B|$ and there is not bijective function from $A$ to $B$ we write $|A| < |B|$.

**Theorem 8.6 (Cantor)** *If $X$ be a set, then $|X| < |\mathcal{P}(X)|$.*

*Proof.* The fact that $|X| \leq |P(X)|$ is clear.

Let $\varphi$ be a function from $X$ to $P(X)$. For each $x \in X$, $\varphi(x) = A_x \subseteq X$. Set $B = \{x \mid (x \in X) \wedge (x \notin A_x)\}$. Then $B \subset X$. Let $z \in X$. Then either $z \in A_z$ or $z \in B$. So $\varphi(z) = A_z \neq B$. Thus there is no $z \in X$ such that $\varphi(z) = B$. In particular, there is not bijective function from $X$ to $P(X)$. Since there is a one-to-one function from $X$ to $P(X)$, $|X| < |P(X)|$. ■

## 8.3 Schröder Bernstein Theorem

**Theorem 8.7 (Schröder Bernstein Theorem)** *If $|A| \leq |B|$ and $|B| \leq |A|$, then $|A| = |B|$.*

## 8.4 Exercises from Chapter 11

**Homework:** 11.3, 7, 10, 12, 14, 16, 22, 26, 27, 33

**Recitation Problems:** 11.4, 6, 8, 11, 15, 17, 18, 19, 20, 23, 24, 25, 28, 30, 32, 34, 35, 36, 37, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49

## Challenge Problem

Let $X$, $Y$, $Z$ be sets. Then

$$\mathrm{Map}(X, \mathrm{Map}(Y, Z)) \sim \mathrm{Map}(X \times Y, Z).$$

# 9 Three Topics of Set Theory

**Review**

**Comparison of Cardinalities:** Let $A$ and $B$ be set. We write $|A| \leq |B|$ if $A = \emptyset$ or there is a one-to-one function from $A$ to $B$. If $|A| \leq |B|$ and there is not bijective function from $A$ to $B$ we write $|A| < |B|$.

**There is a Set with Greater Cardinality:** $|X| < |\mathcal{P}(X)|$.

**$|\boldsymbol{R}| > \aleph_0$:** $|\boldsymbol{R}| = |(0,1)| > |\boldsymbol{N}|$.

## 9.1 Proof of Schröder(-Cantor)-Bernstein's Theorem

**Theorem 9.1** *If $|A| \leq |B|$ and $|B| \leq |A|$, then $|A| = |B|$.*

*Proof.* Let $f : X \to Y$ and $g : Y \to X$ be one-to-one functions. Assume that neither $f$ nor $g$ is onto. Element of $X \setminus g(Y)$ and $Y \setminus f(X)$ are called *primitive*

**Fist Kind** With finite steps of taking ascendants it reaches a primitive element of $X$.

**Second Kind** With finite steps of taking ascendants it reaches a primitive element of $Y$.

**Third Kind** There is an infinite sequence of taking parents.

The descendants of $i$th elements are $i$th elements.

$f(X_1) = Y_1,\ g(Y_2 \cup Y_3) = X_2 \cup X_3,\ X = X_1 \cup X_2 \cup X_3$ (disjoint), $Y = Y_1 \cup Y_2 \cup Y_3$ (disjoint). Now we define a bijection from $X = X_1 \cup X_2 \cup X_3$ to $Y = Y_1 \cup Y_2 \cup Y_3$ as follows.

$$h : X = X_1 \cup X_2 \cup X_3 \to Y = Y_1 \cup Y_2 \cup Y_3 \quad \left( x \mapsto h(x) = \begin{cases} f(x) & \text{if } x \in X_1, \\ g^{-1}(x) & \text{if } x \in X_2 \cup X_2. \end{cases} \right)$$

This establishes the assertion. ■

## 9.2 Base-$b$ Numeral System

Let $b \geq 2$ be an integer. Let $a$ be a nonnegative real number and write $a = [a] + \{a\}$, where $[a]$ is the largest integer at most $a$, i.e., $[a] \leq a < [a] + 1$, and $\{a\} = a - [a]$. Then $0 \leq \{a\} < 1$.

For a nonnegative integer $n$, we define $a_n$ recursively as follows. Let $q_0 = [a]$, $q_i = bq_{i+1} + a_i$. So if $b^n \leq [a] < b^{n+1}$,

$$\begin{aligned} [a] &= bq_1 + a_0 = b(bq_2 + a_1) + a_0 = b(b(bq_3 + a_2) + a_1) + a_0 = \cdots \\ &= a_n b^n + a_{n-1} b^{n-1} + \cdots + a_1 b^1 + a_0 b^0. \end{aligned}$$

$a = p_0$, $a_i = [bp_i]$ and $p_{i+1} = \{bp_i\} < 1$. Hence we have $bp_i = a_{-1-i} + p_{i+1}$ and $p_i = a_{-1-i} b^{-1} + p_{i+1} b^{-1}$. So

$$\begin{aligned} \{a\} &= a_{-1} b^{-1} + p_1 b^{-1} \\ &= a_{-1} b^{-1} + (a_{-2} b^{-1} + p_2 b^{-1}) b^{-1} \\ &= a_{-1} b^{-1} + (a_{-2} b^{-1} + (a_{-3} b^{-1} + p_3 b^{-1}) b^{-1}) b^{-1} \\ &= a_{-1} b^{-1} + a_{-2} b^{-2} + a_{-3} b^{-3} + \cdots + a_{-n} b^{-n} + p_n b^{-n}. \end{aligned}$$

Thus by letting $c_m = a_{-1} b^{-1} + a_{-2} b^{-2} + a_{-3} b^{-3} + \cdots + a_{-m} b^{-m}$

$$\{a\} - c_m = \{a\} - (a_{-1} b^{-1} + a_{-2} b^{-2} + a_{-3} b^{-3} + \cdots + a_{-m} b^{-m}) = p_m b^{-m} < b^{-m}.$$

Therefore $\lim_{m \to \infty} c_m = \{a\}$ and we can write $a$ as follows.

$$a = [a] + \{a\} = \sum_{i=0}^{n} a_i b^i + \sum_{j=1}^{\infty} a_{-j} b^{-j}.$$

## 9.3 The Set of Real Numbers

**Proposition 9.2** *The set of reals $\boldsymbol{R}$ and $\mathcal{P}(\boldsymbol{N})$ are numerically equivalent.*

*Proof.* Let $I = (0.1) = \{x \in \boldsymbol{R} : 0 < x < 1\}$. It suffices to show that there are one-to-one mapping from $I$ to $\mathcal{P}(\boldsymbol{N})$ and from $\mathcal{P}(\boldsymbol{N})$ to $I$, (choosing terminating expression when applicable)

$$\phi : I \to \mathcal{P}(\boldsymbol{N}) \left( \sum_{i=1}^{n} \frac{a_i}{2^i} \mapsto \{j \in \boldsymbol{N} : a_j = 1\} \right).$$

$$\psi : \mathcal{P}(\boldsymbol{N}) \to I \left( S \mapsto \sum_{i \in S} \frac{5}{10^i} \right).$$

Thus $I \sim \mathcal{P}(\boldsymbol{N})$ and $|\boldsymbol{R}| = |\mathcal{P}(\mathcal{N})|$. ■

**Note.** The proposition above also shows that $|\boldsymbol{R}| > \aleph_0$.

## 9.4 Axiom of Choice

The following statement is called the Axiom of Choice (選択公理).

> For every collection of of pairwise disjoint nonempty sets, there exists at least one set that contains exactly one element of each of these nonempty set. (Equivalently, suppose $\{S_y : y \in Y\} \subset \mathcal{P}(X)$ is a collection of nonempty mutually disjoint subsets of $X$. Then there is a set $\{s_y : y \in Y\}$, such that each $s_y \in S_y$.)
>
> Let $f : X \to Y$ be an onto function. Then there is a function $g : Y \to X$ such that $f \circ g = i_Y$.

**Proposition 9.3** *Suppose there is an onto function from a set $X$ to a set $Y$. Then $|Y| \leq |X|$.*

*Proof.* We need Axiom of Choice. ■

**Corollary 9.4** *Suppose there is an onto function from a set $X$ to a set $Y$. Then $|Y| \leq |X|$.*

**Definition 9.1** Let $(A, \leq)$ be a (nonempty) partially ordered set. A subset $S$ of $A$ is called a *chain* if $a \leq b$ or $b \leq a$ for all $a, b \in A$. $A$ is said to be *inductive* if every nonempty chain in $A$ has an upper bound in $A$.

**Zorn's Lemma:** Every inductive set has a maximal element.

## 9.5 Exercises from Chapter 12

**Homework:** 12.1, 9, 11, 15, 21, 30, 37, 38, 40, 65

**Recitation Problems:** 12.29, 36, 41, 43, 54, 58, 60, 64, 66, 70, 73, 78, 81, 83, 84

# 10 Proofs in Number Theory (整数論の証明)

## 10.1 Review: Divisibility Properties of Integers

Let $a, b \in \boldsymbol{Z}$. The integer $a$ divides $b$ If there exists $c \in \boldsymbol{Z}$ such that $b = ac$. When $a$ divides $b$, we write $a \mid b$. If $a$ does not divide $b$, we write $a \nmid b$.

$$\forall a \in \boldsymbol{Z}, \forall b \in \boldsymbol{Z}, a \mid b \Leftrightarrow \exists c \in \boldsymbol{Z}, b = ac.$$

Note that if $a \mid b$, then $|b| = |a||c|$ and $|a| \leq |b|$ unless $b = 0$.

**Proposition.** Let $a, b, c \in \boldsymbol{Z}$.

(i) Always $1 \mid a$, $a \mid 0$ and $0 \mid a \Leftrightarrow a = 0$.

(ii) $(a \mid b) \wedge (b \mid c) \Rightarrow a \mid c$。

(iii) $(a \mid b) \wedge (b \mid a) \Leftrightarrow a = \pm b$.

(iv) $(a \mid b) \wedge (a \mid c) \Leftrightarrow a \mid bx + cy$ for all integers $x, y$.

**Congruence of Integers** Let $m$ be positive integer. For $a, b \in \boldsymbol{Z}$, $a$ is *congruent to $b$ modulo $m$* if $m \mid a - b$. In this case we write $a \equiv b \pmod{m}$.

**Lemma.** The following hold, i.e., *the relation of integers $a \equiv b \pmod{m}$ defined by $m \mid a - b$ is an equivalence relation.*

(i) $a \equiv a \pmod{m}$.

(ii) $a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$.

(iii) $(a \equiv b \pmod{m}) \wedge (b \equiv c \pmod{m}) \Rightarrow a \equiv c \pmod{m}$.

**Proposition.** For integers $a, b, c, d$ and a positive integer $n$, suppose $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. Then the following hold.

$$\text{(i)} \quad a + c \equiv b + d \pmod{n}. \quad \text{(ii)} \quad ac \equiv bd \pmod{n}.$$

**Proposition.** Let $[a] = \{x \in \boldsymbol{Z} : x \equiv a \pmod{n}\}$ for $a \in \boldsymbol{Z}$. The the following are well-defined.

$$\text{(i)} \quad [a] + [b] = [a + b]. \quad \text{(ii)} \quad [a][b] = [ab].$$

Let $\boldsymbol{Z}_n = \{[a] : a \in \boldsymbol{Z}\}$. Then the following functions are well-defined.

$$\phi : \boldsymbol{Z}_n \times \boldsymbol{Z}_n \to \boldsymbol{Z}_n \ (([a], [b]) \mapsto [a + b]), \quad \psi : \boldsymbol{Z}_n \times \boldsymbol{Z}_n \to \boldsymbol{Z}_n \ (([a], [b]) \mapsto [ab]),$$

**Well-ordered Property and Mathematical Induction**

**Definition.** [Review] An nonempty set $S$ of real numbers is said to be *well-ordered* if every nonempty subset of $S$ has a least element $\min S$, i.e.,

$$m = \min S \Leftrightarrow m \in S, \text{ and } \forall x \in S, \ m \leq x.$$

For each integer $m \in \boldsymbol{Z}$, the set $S = \{i \in \boldsymbol{Z} : i \geq m\}$. is well-ordered.

**Principle of Mathematical Induction:** $(P(m) \wedge (\forall k > m, P(k-1) \Rightarrow P(k)) \Rightarrow (\forall n \geq m, P(n))$.

**Strong Principle of Mathematical Induction:** $(P(m) \wedge (\forall k > m, (m \leq \forall i < k, P(i)) \Rightarrow P(k))) \Rightarrow (\forall n \geq m, P(n))$.

**Example.** Every positive number $n \geq 2$ is either a prime[2] or a product of primes.

**Example.** Let $a, b \in \boldsymbol{Z}$. Then there is an integer $d$ satisfying the following three conditions.

$$\text{(i) } d \geq 0, \quad \text{(ii) } d \mid a \text{ and } d \mid b, \quad \text{(iii) } c \mid a \text{ and } c \mid b \text{ implies } c \mid d.$$

The integer $d$ is uniquely determined and it is called the *greatest common divisor* of $a$ and $b$. The greatest common divisor $d$ of $a$ and $b$ is denoted by $d = \gcd\{a, b\}$. In this case, there are $x, y \in \boldsymbol{Z}$ such that $d = ax + by$.

## 10.2 Division Algorithm

**Proposition 10.1** *For integers $a$ and $b$ with $a \neq 0$, there exist unique integers $q$ and $r$ such that $b = aq+r$ with $0 \leq r < |a|$.*

*Proof.* We assume $a, b > 0$. For general case, see Exercise 11.12. Consider the set $S = \{b - ax : x \in \boldsymbol{Z} \text{ and } b - ax \geq 0\}$.

By letting $x = 0$, we find $b \in S$ and $S \neq \emptyset$. Since $\boldsymbol{Z}^{\geq 0}$ is a well-ordered set, $S$ has a smallest element, say $r \geq 0$. Since $r \in S$, there is some integer $q \in \boldsymbol{Z}$ such that $b = aq + r$. If $r \geq a$, then

$$0 \leq r - a = b - aq - a = b - a(q + 1) \in S,$$

while $r - a < r$. A contradiction. Thus $0 \leq r < a$.

Assume that $b = aq + r = aq' + r'$ with $0 \leq r \leq r' < a$. Then $a(q - q') = r' - r$. So $a \mid r - r'$ and $0 \leq r' - r < a$. Thus $r' = r$. Therefore $q = q'$ as $a \neq 0$. ■

**Lemma 10.2** *Let $a$ and $b$ be positive integers. If $b = aq + r$ for some integers $q$ and $r$, then $\gcd(a, b) = \gcd(r, a)$. Moreover if $d = rx + ay$, then $d = a(y - qx) + bx$.*

**Example 10.1** $d = \gcd(374, 946) = 22$ and $22 = 374 \cdot (-5) + 946 \cdot 2$.

**Proposition 10.3** *Let $a$ and $b$ be integers not both zero. Then $\gcd(a, b) = 1$ if and only if there exist integers $s$ and $t$ such that $1 = as + bt$.*

**Corollary 10.4 (Euclid's Lemma)** *Let $a$, $b$ and $c$ be integers. If $a \mid bc$ and $\gcd(a, b) = 1$, then $a \mid c$. In particular, if $p$ is a prime, and $p \mid bc$, then $p \mid b$ or $p \mid c$.*

**Corollary 10.5** *Let $a, b, c \in \boldsymbol{Z}$, where $a$ and $b$ are relatively prime. If $a \mid c$ and $b \mid c$, then $ab \mid c$.*

*Proof.* Let $as + bt = 1$. $c = ax$ and $c = by$. Now $c = c(as + bt) = absy + abtx = ab(sy + tx)$. ■

## 10.3 The Fundamental Theorem of Arithmetic

**Theorem 10.6** *Every integer $n \geq 2$ is either prime or can be expressed as a product of primes, that is $n = p_1 p_2 \cdots p_m$, where $p_1, p_2, \ldots, p_m$ are primes.*

*Moreover, such expression is unique up to the ordering. That is if $n = p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_\ell$ are both products of primes, then $m = \ell$ and there is a permutation $j_1, j_2, \ldots, j_\ell$ of $1, 2, \ldots, \ell$ such that $p_1 = q_{j_1}, p_2 = q_{j_2}, \ldots, p_m = q_{j_m}$.*

## 10.4 Exercises from Chapter 12

**Homework:** 12.1, 9, 11, 15, 21, 30, 37, 38, 40, 65

**Recitation Problems:** 12.29, 36, 41, 43, 54, 58, 60, 64, 66, 70, 73, 78, 81, 83, 84

[2] A prime number $p$ is a positive integer at least 2 such that 1 and $p$ are the only positive divisors.

# 11 Two Topics

## 11.1 Base-$b$ Numeral System

Let $b \geq 2$ be an integer. Let $a$ be a nonnegative real number and write $a = [a] + \{a\}$, where $[a]$ is the largest integer at most $a$, i.e., $[a] \leq a < [a] + 1$, and $\{a\} = a - [a]$. Then $0 \leq \{a\} < 1$.

For a nonnegative integer $n$, we define $a_n$ recursively as follows. Let $q_0 = [a]$, $q_i = bq_{i+1} + a_i$. So if $b^n \leq [a] < b^{n+1}$,

$$\begin{aligned} [a] &= bq_1 + a_0 = b(bq_2 + a_1) + a_0 = b(b(bq_3 + a_2) + a_1) + a_0 = \cdots \\ &= a_n b^n + a_{n-1} b^{n-1} + \cdots + a_1 b^1 + a_0 b^0. \end{aligned}$$

$a = p_0$, $a_i = [bp_i]$ and $p_{i+1} = \{bp_i\} < 1$. Hence we have $bp_i = a_{-1-i} + p_{i+1}$ and $p_i = a_{-1-i}b^{-1} + p_{i+1}b^{-1}$. So

$$\begin{aligned} \{a\} &= a_{-1}b^{-1} + p_1 b^{-1} = a_{-1}b^{-1} + (a_{-2}b^{-1} + p_2 b^{-1})b^{-1} = a_{-1}b^{-1} + (a_{-2}b^{-1} + (a_{-3}b^{-1} + p_3 b^{-1})b^{-1})b^{-1} \\ &= a_{-1}b^{-1} + a_{-2}b^{-2} + a_{-3}b^{-3} + \cdots + a_{-n}b^{-n} + p_n b^{-n}. \end{aligned}$$

Thus by letting $c_m = a_{-1}b^{-1} + a_{-2}b^{-2} + a_{-3}b^{-3} + \cdots + a_{-m}b^{-m}$

$$\{a\} - c_m = \{a\} - (a_{-1}b^{-1} + a_{-2}b^{-2} + a_{-3}b^{-3} + \cdots + a_{-m}b^{-m}) = p_m b^{-m} < b^{-m}.$$

Therefore $\lim_{m\to\infty} c_m = \{a\}$ and we can write $a$ as follows.

$$a = [a] + \{a\} = \sum_{i=0}^{n} a_i b^i + \sum_{j=1}^{\infty} a_{-j} b^{-j}.$$

## 11.2 Axiom of Choice and Zorn's Lemma

The following statement is called the Axiom of Choice (選択公理).

**Axiom of Choice:** For every collection of of pairwise disjoint nonempty sets, there exists at least one set that contains exactly one element of each of these nonempty set. (Equivalently, suppose $\{S_y : y \in Y\} \subset \mathcal{P}(X)$ is a collection of nonempty mutually disjoint subsets of $X$. Then there is a set $\{s_y : y \in Y\}$, such that each $s_y \in S_y$.)

**Proposition 11.1** *Let $f : X \to Y$ be an onto function. Then there is a function $g : Y \to X$ such that $f \circ g = i_Y$.*

*Proof.* We need Axiom of Choice. ■

**Corollary 11.2** *Suppose there is an onto function from a set $X$ to a set $Y$. Then $|Y| \leq |X|$.*

**Definition 11.1** Let $(A, \leq)$ be a (nonempty) partially ordered set. A subset $S$ of $A$ is called a *chain* if $a \leq b$ or $b \leq a$ for all $a, b \in A$. $A$ is said to be *inductive* if every nonempty chain in $A$ has an upper bound in $A$.

**Zorn's Lemma:** Every inductive set has a maximal element.

# References


[1] Gary Chartrand, Albert D. Polimeni, and Ping Zhang, *Mathematical Proofs, A Transition to Advanced Mathematics, Second Edition*, Pearson International Edition, 2008.

[2] Gaishi Takeuchi, *Shugo to-ha Nani-ka*, (in Japanese), Kodan-sha, 2001.