

Set Theory

沈威宇

July 1, 2025

Contents

1	Set Theory (集合論)	1
I	Basic Notations	1
i	Set (集合/集)	1
ii	Specifying a set	1
iii	Empty set (空集合) and singleton (單元素集合)	1
iv	Subset (子集)	1
v	Superset (父集/母集/超集)	1
vi	Intersection (交集)	1
vii	Union (聯集)	2
viii	Complement (差集)	2
ix	Cartesian product (笛卡爾積)	2
x	Power set (冪集合)	2
xi	Set scalar arithmetic operation	2
xii	Kernel (核) of a set of sets	2
II	Zermelo–Fraenkel Set Theory (策梅洛-弗蘭克爾集合論)	2
i	Axiom of extensionality (外延公理)	2
ii	Axiom of regularity (正則公理)	2
iii	Axiom of separation (分類公理)/Axiom schema of specification (規範公理模式)	3
iv	Pairing Axiom (配對公理)	3
v	Union Axiom (聯集公理)	3
vi	Axiom schema of replacement (替代公理模式)	3
vii	Axiom of Infinity (無窮公理)	3
viii	Power Set Axiom (冪集公理)	3
ix	Axiom of Choice (選擇公理)/Axiom of Well-ordering (良序公理)	3
III	Associativity, commutativity, and distributivity of intersection and union	4
IV	Russell's paradox or Russell's antinomy (羅素悖論)	4
V	De Morgan's Law (笛摩根定律)	4
i	Universe (宇集)	4
ii	Complement (補集/餘集)	4
iii	Complement laws	4

	iv De Morgan's Law (笛摩根定律).	5
VI	Ordered Set	5
	i Partially ordered set, poset (偏序集)	5
	ii Upward closure.	5
	iii Totally ordered set (全序集) or linearly ordered set (線性順序集)	5
VII	Number System (數系)	5
	i Natural numbers (自然數)	5
	ii Integers (整數)	7
	iii Rational numbers (有理數).	7
	iv Real numbers (實數)	7
	v Irrational numbers (無理數)	8
	vi Complex numbers (複數)	8
VIII	Cardinality (勢/基數/計數)	9

1 Set Theory (集合論)

I Basic Notations

i Set (集合/集)

A set, sometimes called a collection or family, is a collection of different things. These things are called elements (元素) or members (成員) of the set.

If a is an element of a set S , we say that a belongs to S or is in S , denoted as $a \in S$; if b is not an element of a set S , we say that b does not belong to S or is not in S , denoted as $b \notin S$.

ii Specifying a set

A set may be specified either by listing its elements or by a property that characterizes its elements.

Roster notation or enumeration notation specifies a set by listing its elements between braces $\{ \}$, separated by commas, e.g. $\{ \}$, $\{x\}$, and $\{x, y\}$. When there is a clear pattern for generating all set elements, one can use ellipses \dots for abbreviating the notation.

Set-builder notation specifies a set as being the set of all elements that satisfy some logical formula. More precisely, if $P(x)$ is a logical formula depending on a variable x , which evaluates to true or false depending on the value of x , then

$$\{x \mid P(x)\}$$

or

$$\{x : P(x)\}$$

denotes the set of all x of which $P(x)$ is true, in which the vertical bar \mid or the colon $:$ is read as "such that", and the whole formula can be read as "the set of all x such that $P(x)$ is true".

iii Empty set (空集合) and singleton (單元素集合)

A set with no element in it is called the empty set, denoted as \emptyset . A set with one element in it is called a singleton.

iv Subset (子集)

$$A \subseteq B \iff (x \in A \implies x \in B)$$

v Superset (父集/母集/超集)

$$B \supseteq A \iff (x \in A \implies x \in B)$$

vi Intersection (交集)

$$A \cap B := \{x \mid x \in A \wedge x \in B\}$$

$$\bigcap_{i=1}^n A_i := \left\{ x \mid \bigwedge_{i=1}^n x \in A_i \right\}$$

vii Union (聯集)

$$A \cup B := \{x \mid x \in A \vee x \in B\}$$

$$\bigcup_{i=1}^n A_i := \left\{ x \mid \bigvee_{i=1}^n x \in A_i \right\}$$

viii Complement (差集)

$$A \setminus B := \{x \mid x \in A \wedge x \notin B\}$$

ix Cartesian product (笛卡爾積)

$$A \times B := \{(a, b) \mid a \in A \wedge b \in B\}$$

x Power set (冪集合)

$$2^A := \{B \mid B \subseteq A\}$$

xi Set scalar arithmetic operation

- If $\forall a \in A$, sa is defined, $sA := \{sa : a \in A\}$.
- If $\forall a \in A$, $a + v$ is defined, $A + v := \{a + v : a \in A\}$.

xii Kernel (核) of a set of sets

The kernel of a set $B \neq \emptyset$ of sets is defined to be:

$$\ker(B) := \bigcap_{B \in \mathcal{B}} B.$$

II Zermelo–Fraenkel Set Theory (策梅洛-弗蘭克爾集合論)

Set theory, or more specifically, Zermelo–Fraenkel set theory, has been the standard way to provide rigorous foundations for all branches of mathematics since the first half of the 20th century. Zermelo–Fraenkel set theory with the axiom of choice included is abbreviated ZFC and denoted \vdash_{ZFC} ; Zermelo–Fraenkel set theory with the axiom of choice excluded is abbreviated ZF and denoted \vdash_{ZF} ; sometimes, either of them is denoted \vdash .

i Axiom of extensionality (外延公理)

$$\forall x \forall y [\forall z (z \in x \Leftrightarrow z \in y) \Rightarrow x = y]$$

ii Axiom of regularity (正則公理)

$$\forall x (x \neq \emptyset \Rightarrow \exists y (y \in x \wedge y \cap x = \emptyset))$$

iii Axiom of separation (分類公理)/Axiom schema of specification (規範公理模式)

Let φ be any formula in the language of ZFC with all free variables among x, z, w_1, \dots, w_n so that y is not free in φ . Then:

$$\forall z \forall w_1 \forall w_2 \dots \forall w_n \exists y \forall x [x \in y \Leftrightarrow ((x \in z) \wedge \varphi(x, w_1, w_2, \dots, w_n, z))]$$

This axiom can be used to prove the existence of the empty set, denoted as \emptyset or \varnothing .

Axiom of empty set (空集公理) :

$$\exists x, \forall y, (y \notin x)$$

The \emptyset is defined as the x above.

iv Pairing Axiom (配對公理)

$$\forall x \forall y \exists z ((x \in z) \wedge (y \in z))$$

v Union Axiom (聯集公理)

$$\forall \mathcal{F} \exists A \forall Y \forall x [(x \in Y \wedge Y \in \mathcal{F}) \Rightarrow x \in A]$$

Although this formula doesn't directly assert the existence of $\cup \mathcal{F}$, the set $\cup \mathcal{F}$ can be constructed from A in the above using the axiom schema of specification:

$$\cup \mathcal{F} = \{x \in A \mid \exists Y (x \in Y \wedge Y \in \mathcal{F})\}$$

vi Axiom schema of replacement (替代公理模式)

Let φ be any formula in the language of ZFC with all free variables among x, z, w_1, \dots, w_n so that B is not free in φ . Then:

$$\forall A \forall w_1 \forall w_2 \dots \forall w_n [\forall x (x \in A \Rightarrow \exists! y \varphi) \Rightarrow \exists B \forall x (x \in A \Rightarrow \exists y (y \in B \wedge \varphi))]$$

vii Axiom of Infinity (無窮公理)

$$\exists X [\exists e (\forall z \neg (z \in e) \wedge e \in X) \wedge \forall y (y \in X \Rightarrow S(y) \in X)]$$

viii Power Set Axiom (冪集公理)

$$\forall A \exists P(A) \forall x (x \in P(A) \leftrightarrow x \subseteq A)$$

The $P(A)$ above is called power set (冪集) and denoted as 2^A .

ix Axiom of Choice (選擇公理)/Axiom of Well-ordering (良序公理)

$$\forall X \left[\emptyset \notin X \Rightarrow \exists f : X \rightarrow \bigcup_{A \in X} A \quad \forall A \in X (f(A) \in A) \right]$$

III Associativity, commutativity, and distributivity of intersection and union

- Intersection has commutativity.
- Union has commutativity.
- Intersection has associativity and distributivity over intersection.
- Union has associativity and distributivity over union.
- Intersection has distributivity over union.
- Union has distributivity over intersection.
- Note: $(A \cap B) \cup C$ is not necessarily equal to $A \cap (B \cup C)$

IV Russell's paradox or Russell's antinomy (羅素悖論)

According to the unrestricted comprehension principle, for any sufficiently well-defined property, there is the set of all and only the objects that have that property. Russell's paradox states that, let

$$R := \{x \mid x \notin x\}$$

then

$$R \in R \iff R \notin R.$$

Statement. $\vdash_{ZFC} \nexists U = \{z \mid z \text{ is a set}\}.$

Proof.

Assume that $\exists U = \{z \mid z \text{ is a set}\}$. Let $A = \{x \in U \mid x \notin x\}$. $A \in A \iff (A \in U \wedge A \notin A)$, but $A \in A \iff \neg A \notin A$, so $A \notin A$, so $\neg(A \in U \wedge A \notin A)$, so $A \notin U$. A is a set, so $A \in U$. $\Rightarrow \Leftarrow$. \square

V De Morgan's Law (笛摩根定律)

i Universe (字集)

The universe is now often defined as "when the sets under discussion are all subsets of a given set, the given set is called the universe", denoted as U .

ii Complement (補集/餘集)

If a set A is a subset of a given universe U , then the complement of A given U is defined as $U \setminus A$, denoted as A' , \bar{A} , or A^C .

iii Complement laws

$$(A')' = A$$

$$A \setminus B = A \cap B'$$

$$A \subseteq B \iff B' \subseteq A'$$

iv De Morgan's Law (笛摩根定律)

$$(A \cup B)' = A' \cap B'$$

$$(A \cap B)' = A' \cup B'$$

VI Ordered Set

i Partially ordered set, poset (偏序集)

A partially ordered set is an ordered pair $P = (X, \leq)$ consisting of a set X (called the ground set of P) and a partial order \leq on X . That is, for all $a, b, c \in X$ it must satisfy:

1. Reflexivity: $a \leq a$, i.e. every element is related to itself.
2. Antisymmetry: $a \leq b \wedge b \leq a \implies a = b$, i.e. no two distinct elements precede each other.
3. Transitivity: $a \leq b \wedge b \leq c \implies a \leq c$.

When the meaning is clear from context and there is no ambiguity about the partial order, the set X itself is sometimes called a poset.

ii Upward closure

Let A be a subset of a poset X , the upward closure of A , denoted as $\uparrow A$, is defined as:

$$\uparrow A := \{x \in X : \exists a \in A \text{ s.t. } a \leq x\}.$$

iii Totally ordered set (全序集) or linearly ordered set (線性順序集)

A totally ordered set is an ordered pair $P = (X, \leq)$ consisting of a set X (called the ground set of P) and a total order (aka, linear order) \leq on X . That is, for all $a, b, c \in X$ it must satisfy:

1. Reflexivity: $a \leq a$, i.e. every element is related to itself.
2. Antisymmetry: $a \leq b \wedge b \leq a \implies a = b$, i.e. no two distinct elements precede each other.
3. Transitivity: $a \leq b \wedge b \leq c \implies a \leq c$.
4. Strongly connectivity or totality: $a \leq b \vee b \leq a$.

When the meaning is clear from context and there is no ambiguity about the total order, the set X itself is sometimes called a totally ordered set.

VII Number System (數系)

i Natural numbers (自然數)

The natural numbers \mathbb{N} are defined as positive integers, that is, 1, 2, 3, and so on, denoted as \mathbb{N}^* , \mathbb{N}_1 , or \mathbb{N}^+ , or non-negative integers, that is, 0, 1, 2, 3, and so on, denoted as \mathbb{N}^0 or \mathbb{N}_0 .

The **Peano axioms (皮亞諾公理)**, **Dedekind–Peano axioms**, or **Peano postulates (皮亞諾公設)** provide a formal definition of the natural numbers \mathbb{N} . Below, we define the natural numbers to include

zero; the definition of natural numbers to exclude zero can be constructed by simply replace 0 with 1 in the following axioms.

- 0 is a natural number.

The next four axioms describe the equality relation. Since they are logically valid in first-order logic with equality, they are not considered to be part of "the Peano axioms" in modern treatments.

- For every natural number x , $x = x$. That is, equality is reflexive.
- For all natural numbers x and y , if $x = y$, then $y = x$. That is, equality is symmetric.
- For all natural numbers x , y , and z , if $x = y$ and $y = z$, then $x = z$. That is, equality is transitive.
- For all a and b , if b is a natural number and $a = b$, then a is also a natural number. That is, the natural numbers are closed under equality.

The remaining axioms define the arithmetical properties of the natural numbers. The naturals are assumed to be closed under a single-valued "successor" function S .

- For every natural number n , $S(n)$ is a natural number. That is, the natural numbers are closed under S .
- For all natural numbers m and n , if $S(m) = S(n)$, then $m = n$. That is, S is an injection.
- For every natural number n , $S(n) = 0$ is false. That is, there is no natural number whose successor is 0.

Axioms 1, 6, 7, 8 define a unary representation of the intuitive notion of natural numbers: the number 1 can be defined as $S(0)$, 2 as $S(S(0))$, etc. However, considering the notion of natural numbers as being defined by these axioms, axioms 1, 6, 7, 8 do not imply that the successor function generates all the natural numbers different from 0. The intuitive notion that each natural number can be obtained by applying successor sufficiently many times to zero requires an additional axiom, which is sometimes called the **axiom of induction**:

- If K is a set such that:

0 is in K , and

for every natural number n , n being in K implies that $S(n)$ is in K ,

then K contains every natural number.

The axiomatization of arithmetic provided by Peano axioms is commonly called **Peano arithmetic** (皮亞諾算術).

- **Addition** is a function that maps two natural numbers to another one. It is defined recursively as:

$$a + 0 = a,$$

$$a + S(b) = S(a + b).$$

- **Multiplication** is a function mapping two natural numbers to another one. Given addition, it is defined recursively as:

$$a \cdot 0 = 0,$$

$$a \cdot S(b) = a + (a \cdot b).$$

- **Total order:** The field \mathbb{N} is ordered, meaning that there is a total order \leq such that for all natural numbers x, y and z :

- Preservation of order under addition:

$$\forall x, y, z \in \mathbb{N} : x \leq y \implies x + z \leq y + z.$$

- Preservation of order under multiplication:

$$\forall x, y \in \mathbb{N} : 0 \leq x \wedge 0 \leq y \implies 0 \leq xy.$$

ii Integers (整數)

The set of integers \mathbb{Z} can be constructive as follows. First construct the set of natural numbers excluding 0 according to the Peano axioms, call this P . Then construct a set P^- which is disjoint from P and in one-to-one correspondence with P via a function ψ . Finally let 0 be some object not in P or P^- . Then the integers are defined to be the union $P \cup P^- \cup \{0\}$.

iii Rational numbers (有理數)

The set of rational numbers (aka, the rationals) \mathbb{Q} can be constructed as equivalence classes of ordered pairs of integers. Let $(\mathbb{Z} \times (\mathbb{Z} \setminus \{0\}))$ be the set of the pairs (m, n) of integers such that $n \neq 0$ and denoted as $\frac{m}{n}$. An equivalence relation is defined on this set by

$$(m_1, n_1) = (m_2, n_2) \iff m_1 n_2 = m_2 n_1.$$

Addition and multiplication can be defined by the following rules:

$$(m_1, n_1) + (m_2, n_2) \equiv (m_1 n_2 + n_1 m_2, n_1 n_2),$$

$$(m_1, n_1) \times (m_2, n_2) \equiv (m_1 m_2, n_1 n_2).$$

iv Real numbers (實數)

Let \mathbb{R} denote the set of all real numbers. Then:

- **Addition and multiplication:** The set \mathbb{R} is a field under addition and multiplication. In other words,

- Associativity of addition and multiplication:

$$\forall x, y, z \in \mathbb{R} : x + (y + z) = (x + y) + z \wedge x \cdot (y \cdot z) = (x \cdot y) \cdot z.$$

- Commutativity of addition and multiplication:

$$\forall x, y \in \mathbb{R} : x + y = y + x \wedge x \cdot y = y \cdot x.$$

- Distributivity of multiplication over addition:

$$\forall x, y, z \in \mathbb{R} : x \cdot (y + z) = (x \cdot y) + (x \cdot z).$$

- Existence of additive identity:

$$\forall x \in \mathbb{R} : x + 0 = x.$$

- Existence of multiplicative identity:

$$0 \neq 1,$$

$$\forall x \in \mathbb{R} : x \times 1 = x.$$

- Existence of additive inverses:

$$\forall x \in \mathbb{R} : \exists (-x) \in \mathbb{R} \text{ s.t. } x + (-x) = 0.$$

- Existence of multiplicative inverses:

$$\forall x \in \mathbb{R} \wedge x \neq 0 : \exists x^{-1} \in \mathbb{R} \text{ s.t. } x \cdot x^{-1} = 1.$$

- **Total order:** The field \mathbb{R} is ordered, meaning that there is a total order \leq such that for all real numbers x, y and z :

- Preservation of order under addition:

$$\forall x, y, z \in \mathbb{R} : x \leq y \implies x + z \leq y + z.$$

- Preservation of order under multiplication:

$$\forall x, y \in \mathbb{R} : 0 \leq x \wedge 0 \leq y \implies 0 \leq xy.$$

- The order is Dedekind-complete, meaning that every nonempty subset S of \mathbb{R} with an upper bound in \mathbb{R} has a least upper bound (aka, supremum) in \mathbb{R} . This property applies to the real numbers but not to the rational numbers. For example, $\{x \in \mathbb{Q} : x^2 < 2\}$ has a rational upper bound (e.g., 1.42), but no least rational upper bound, because $\sqrt{2}$ is not rational.

v Irrational numbers (無理數)

$$\mathbb{R} \setminus \mathbb{Q}.$$

vi Complex numbers (複數)

$$\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R} \wedge i = \sqrt{-1}\}.$$

VIII Cardinality (勢/基數/計數)

The cardinality is a measure of the size of a set, denoted as $|A|$ or $n(A)$.

- The cardinality of a finite set is the number of its elements.
- Two sets have the same cardinality if there exists a one-to-one correspondence between them.
- The cardinality of \mathbb{N} is called the cardinality of countable infinity (可數無限勢), denoted as \aleph_0 . A set with the same cardinality of \mathbb{N} is called to be countable infinite (可數無限的).
- The cardinality of \mathbb{R} is called the cardinality of continuity (連續勢), denoted as c . A set with the same cardinality of \mathbb{R} is called to be uncountable infinite (不可數無限的).