Set Theory

Discrete Math, Fall 2025

Konstantin Chukharev

Set Theory

- Operations & laws
- Power sets
- Russell's paradox
- ZFC axioms
- Cartesian products
- Cardinality

Binary Relations

- Relation properties
- Equivalence relations
- Functions
- Partial orders
- Lattices
- Well-orders

Boolean Algebra

- Truth tables & laws
- Logic circuits
- Normal forms
- Karnaugh maps
- Binary Decision Diagrams (BDDs)

Formal Logic

- Syntax & semantics
- Natural deduction
- Soundness & completeness
- Categorical logic
- First-order logic

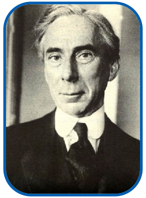
Set Theory

"A set is a Many that allows itself to be thought of as a One."

— Georg Cantor


Georg Cantor


Richard Dedekind


Bertrand Russell


Ernst Zermelo


Abraham Fraenkel

Introduction

Set theory provides a foundational language for all of mathematics. *Everything* from numbers and functions to spaces and relations can be defined using *sets*. This lecture introduces the basic objects and operations of set theory and explores their deep structural and logical consequences.

Topics include:

- Basic concepts: elements, subsets, operations
- Relations and functions as sets
- Infinite sets and cardinality
- Axiomatic foundations
- Applications in logic and computer science

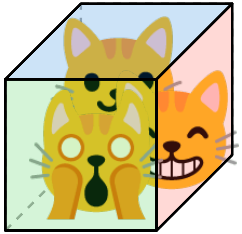
What is a Set?

Definition 1: A *set* is an unordered collection of distinct objects, called *elements*.

Think of a set as a *"box"* or *"bag"* containing objects where:

- The *order* doesn't matter.
- Each object appears *only once* (no duplicates).
- We can check if an object is *directly* inside or not.

Note: A set *can* contain other sets. Nested set is considered a *single* object.



Basic notation: Sets are written within *curly braces*: $\{\ldots\}$.

We use uppercase letters ($A, B, C, \ldots$) to denote sets and lowercase letters ($a, b, c, \ldots$) for their elements.

Example: $A = \{5, \triangle, 🐦\}$ is a set containing *three* distinct elements: the number 5, a triangle, and a birb[1].

[1] A *birb* is a *small bird*. Here, we assume it is distint from the number 5 and triangle.

Examples of Sets

Example (Simple sets):

- $P = \{2, 3, 5, 7, 11, 13\}$ – set of first six prime numbers
- $E = \{2, 4, 6, 8, 10, \ldots\}$ – *infinite* set of even positive integers
- $F = \{$🍏, 🍌, 🍇$\}$ – set of fruits
- $C = \left\{\pi, e, \sqrt{2}, \varphi\right\}$ – set of famous mathematical constants

Example (Special sets):

- $\varnothing = \{\}$ – the *empty set* (contains no elements)
- $\{\varnothing\}$ – *singleton* set containing the empty set as its only element
- $\mathfrak{U} = \{\ldots\}$ – the *universal set* (contains all things in the considered universe)

Example (Nested sets):

- $N = \{\{1, 2\}, \{3, 4\}\}$ – set containing *two* sets as elements
- $M = \{\underbrace{\varnothing}_{1}, \underbrace{\{\text{❤️}\}}_{2}, \underbrace{\{a, \{b, \{c\}\}\}}_{3}\}$ – set with *three* elements: (1) empty set, (2) singleton, (3) nested set

Set Membership

We can check if an object is an *element* of a set or not using the symbols $\in$ and $\notin$.

- $a \in A$ means "a is *an element of* A"
- $a \notin A$ means "a is *not an element of* A"

Example: Let $A = \{42,$ 🐨, 🍞$\}$.

- 🐨 $\in A$ is `true`, since the koala is indeed one of the elements of A.
- 🐧 $\in A$ is `false`, denoted as "🐧 $\notin A$", since there is *no* penguin in A.

Example: Let $B = \{a, \{b\}\}$.

- $a \in B$ is `true` — the element a is directly in B
- $b \in B$ is `false` — the element b is *not* directly in B (it's inside the nested set $\{b\}$)
- $\{b\} \in B$ is `true` — the nested set $\{b\}$ itself is a direct element of B

Note: Membership operator ($\in$) only checks *direct* elements, not what's inside nested sets.

Urelements vs Sets Only

Definition 2: *Urelements*[2] are objects that:

- Are *not* sets themselves.
- Can be *elements* of sets.
- Have no internal structure that set theory can examine.

Examples: numbers, people, physical objects, symbols.

Definition 3: In *pure set theory*:

- *Everything is a set* — no urelements allowed.
- Numbers, functions, relations are all constructed from sets.
- Even "primitive" objects like 0, 1, 2 are defined as specific sets.

[2]From the German prefix *ur-* meaning "primordial" (primitive)

Urelements vs Sets Only [2]

With Urelements:

- $A = \{1, 2, 🐈\}$
- 1 and 2 are numbers (urelements)
- 🐈 represents some object
- Natural and intuitive

Pure Sets Only:

- $0 = \emptyset$
- $1 = \{\emptyset\} = \{0\}$
- $2 = \{\emptyset, \{\emptyset\}\} = \{0, 1\}$
- *Everything* built from $\emptyset$

Note: For this course, we'll often use urelements for intuitive examples, but remember that everything *can* be constructed as pure sets in formal mathematics.

The Extensionality Principle

Definition 4: Two sets are *equal*, denoted $A = B$, if and only if they have exactly the same elements.

Formally: $A = B$ iff $\forall x.\, (x \in A \iff x \in B)$

Equivalently: $A = B$ iff $A \subseteq B$ and $B \subseteq A$

Note: This is actually one of the fundamental *axioms* of set theory!

Example: All of these represent the *same set*:

$\{a, b\}$	$=$	$\{b, a\}$	$=$	$\{a, b, b\}$	$=$	$\{b, a, b\}$
normal form		different order		with duplicate		reorder + duplicates

The extensionality principle makes set equality *well-defined* and ensures that the representation of a set doesn't affect its identity — only its *content* matters.

Set-Builder Notation

Definition 5: A set can be defined using *set-builder notation* (*set comprehension*):

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

meaning "the set of all x such that the property $P(x)$ holds".

Example: $A = \{x \mid x \in \mathbb{N} \text{ and } x > 5\} = \{6, 7, 8, ...\}$ is the set of natural numbers greater than 5.

Example: $S = \{x^2 \mid x \text{ is prime}\} = \{4, 9, 25, 49, ...\}$ is the set of squares of prime numbers[3].

Example: $\mathbb{Q} = \{a/b \mid a \in \mathbb{Z}, b \in \mathbb{N}, b \neq 0\}$ is the set of rational numbers (fractions).

[3] **Note:** 1 *is not* a prime number.

Some Important Sets

Example: $\mathbb{N} = \{0, 1, 2, ...\}$ is the set of natural numbers.

Example: $\mathbb{Z} = \{..., -2, -1, 0, 1, 2, ...\}$ is the set of integers.

Example: $\mathbb{Q} = \{a/b \mid a \in \mathbb{Z}, b \in \mathbb{N}, b \neq 0\}$ is the set of rational numbers.

Example: $\mathbb{R} = (-\infty, +\infty)$ is the set of real numbers (the continuum).

Example: $\mathbb{B} = \{0, 1\}$ is the set of Boolean values (truth values).

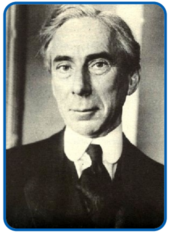
Example: The set A^* of *finite strings* over an alphabet A is defined as:

$$A^* = \{\varepsilon\} \cup \{a_1 a_2 ... a_n \mid n \in \mathbb{N}, a_i \in A\} = \bigcup_{n \in \mathbb{N}} A^n$$

For example, $\mathbb{B}^* = \{\varepsilon, 0, 1, 00, 01, 10, 11, 000, 001, 010, ..., 0000, ...\}$, where ε is the *empty string*.

Example: The set A^ω of *infinite sequences* over A.

Russell's Paradox



Bertrand Russell

Suppose a set can be either *"normal"* or *"unusual"*.

- A set is considered *normal* if it does *not contain itself* as an element. That is, $A \notin A$.
- Otherwise, it is *unusual*. That is, $A \in A$.

Note: being "normal" or "unusual" is a predicate $P(x)$ that can be applied to any set x.

Consider the set of *all normal sets*: $R = \{A \mid A \notin A\}$.

The paradox arises when we ask: **Is R a normal set?**

- Suppose R is *normal*. By its definition, R must be an element of R, so $R \in R$. But elements of R are normal sets, and normal sets do not contain themselves. So $R \notin R$. Contradiction.
- Suppose R is *unusual*. This means R contains itself, so $R \in R$. But the definition of R only includes sets that do *not* contain themselves. So R cannot be a member of R, *i.e.* $R \notin R$. Contradiction.

A contradiction is reached in *both* cases. The only possible conclusion is that **the set R cannot exist**.

This paradox showed that *unrestricted comprehension* — the ability to form a set from any arbitrary property — is logically inconsistent. How can we fix this?..

From Naive to Axiomatic Set Theory

Historical Note

Georg Cantor developed *naive set theory* in the late 19th century, which **David Hilbert** famously called "a paradise from which no one shall expel us". This intuitive approach revolutionized mathematics by providing a foundation for *infinite* sets and real analysis.

However, paradise was short-lived. In 1901, **Bertrand Russell** discovered his famous paradox, showing that unrestricted set formation leads to *contradictions*. This crisis motivated Russell and **Alfred Whitehead** to write *"Principia Mathematica"* (1910-1913), attempting to rebuild mathematics on *logical foundations*.

The modern solution came through *axiomatic set theory*: **Ernst Zermelo** (1908) and **Abraham Fraenkel** (1922) independently developed the *ZFC* axiom system, providing the rigorous foundation we use today. Their work transformed Cantor's intuitive paradise into a mathematically *consistent* framework.

Criterion	**Naive**	**Axiomatic**
Set formation	*Any collection* of objects	From *existing* sets using *axioms*
Comprehension	Unrestricted: $\{x \mid P(x)\}$	Restricted: $\{x \in A \mid P(x)\}$
Distinctions	Simple and intuitive	Mathematically rigorous
Consistency	Leads to *paradoxes*	Axiomatically *consistent*

ZFC Axioms

1. **Extensionality**: Sets with the same elements are equal.
2. **Empty Set**: There exists a set $\emptyset$ with no elements.
3. **Pairing**: For any a and b, there exists a set $\{a, b\}$.
4. **Union**: For any collection of sets, their union exists.
5. **Power Set**: For any set A, the power set $\mathcal{P}(A)$ exists.
6. **Infinity**: There exists an infinite set (containing $\mathbb{N}$).
7. **Separation**: From any set A and property P, we can form $\{x \in A \mid P(x)\}$.
8. **Replacement**: If F is a function-like relation, then for any set A, the image $F[A]$ exists.
9. **Foundation**: Every non-empty set has a minimal element (prevents self-membership).
10. **Choice**: Every collection of non-empty sets has a choice function.

Note: The **Separation** axiom prevents Russell's paradox by only allowing formation of subsets from existing sets, not arbitrary collections.

This is just an introductory course, so we won't delve into the formal axioms here, *yet*.
We'll use an intuitive approach while being aware of the foundations.

Sets: Basic Concepts

Size of Sets

Definition 6: The *size* of a *finite* set X, denoted $|X|$, is the number of elements it contains.

Examples:

- Let $A = \{$🪐, 🦕, 🎻$\}$, then $|A| = 3$, since A contains *exactly 3* elements.
- Let $B = \{$🥝, 🥝, 🥝$\}$, then $|B| = 1$, since B contains *only one unique* element (the kiwi).
- $|\varnothing| = 0$, since the *empty* set contains *no elements*.
- $|\mathbb{N}| = \infty$, since there are *infinitely many* natural numbers.
- $|\mathbb{R}| = \infty$, since there are *infinitely many* real numbers.

Later, we will explore *infinite* sets and different "types of infinity" (*countable* vs *uncountable*) in more detail. For now, we focus on *finite* sets only, or treat infinite sets informally and naively.

Subsets

Definition 7: A set A is a *subset* of B, denoted $A \subseteq B$, if every element of A is also an element of B.

- Formally, $A \subseteq B \iff \forall x.\, (x \in A) \to (x \in B)$.
- If A is not a subset of B, we write $A \nsubseteq B$.
- If $A \subseteq B$ and $A \neq B$, we say A is a *proper* (or *strict*) *subset* of B, denoted $A \subset B$ or $A \subsetneq B$.
- If A is a subset of B, denoted $A \subseteq B$, then B is a *superset* of A, denoted $B \supseteq A$.

Example: Every set is a subset of itself: $A \subseteq A$.

Example: The empty set is a subset of every set: $\varnothing \subseteq A$ for any set A.

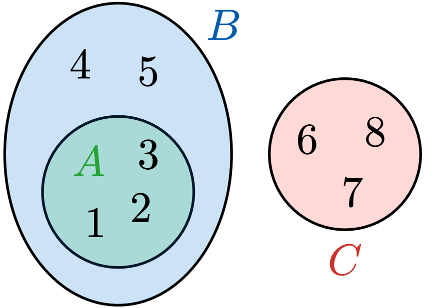
Example: The set of even numbers is a proper subset of the set of integers: $\mathbb{Z}_{\text{even}} \subset \mathbb{Z}$.

Example: $\{a, b\} \subseteq \{a, b, c\}$, but $\{a, b, x\} \nsubseteq \{a, b, c\}$.

Example: $\{0\} \in \{0, \{0\}\}$ *and* $\{0\} \subseteq \{0, \{0\}\}$, that is, $\{0\}$ is an element, and also a subset.

Euler Circles

Definition 8: *Euler diagram* is a graphical representation of sets and their relationships (subset, intersecting, disjoint) using closed shapes (usually circles).



- $A \subseteq B \nsubseteq C$
- $A = \{1, 2, 3\} \subseteq B$ (subset)
- $B = \{1, 2, 3, 4, 5\}$
- $C = \{6, 7, 8\}$
- $B \cap C = \varnothing$ (disjoint)

Set Partitions

Definition 9: Two sets A and B are *disjoint* if they have no elements in common: $A \cap B = \emptyset$.

Definition 10: A collection of sets $\{A_1, A_2, \ldots, A_n\}$ is *pairwise disjoint* if every pair of distinct sets is disjoint: $A_i \cap A_j = \emptyset$ for all $i \neq j$.

Definition 11: A *partition* of a set M is a collection $\mathcal{P} = \{A_1, A_2, \ldots, A_n\}$ of subsets of M such that:

1. Each A_i is *non-empty*: $A_i \neq \emptyset$
2. The sets are *pairwise disjoint*: $A_i \cap A_j = \emptyset$ for $i \neq j$
3. Their *union covers* M: $A_1 \cup A_2 \cup \ldots \cup A_n = M$

Elements of the partition are called *blocks* or *cells*.

Examples of Partitions

Example: $\mathcal{P}_1 = \{\{a\}, \{b, c\}\}$ is a partition of $M = \{a, b, c\}$ into two blocks.

Example: $\mathcal{P}_2 = \{\{2, 4\}, \{1, 3, 5\}\}$ is a partition of $M = \{1, \ldots, 5\}$ into two blocks: *even* and *odd* numbers.

Example: $\mathcal{P}_3 = \{\{$🐄, 🐑, 🐇$\}, \{$🐅, 🦁, 🐺$\}, \{$🐕, 🐖, 🐻$\}\}$ is a partition of given animals into *herbivores*, *carnivores*, and *omnivores*.

Verifying Partitions

Claim 1: $\mathcal{P} = \{\{1,3\},\{2,6\},\{4,5\}\}$ is a partition of $M = \{1,2,3,4,5,6\}$.

Verification:

1. **Non-empty:** Each block $\{1,3\}$, $\{2,6\}$, $\{4,5\}$ contains at least one element ✓
2. **Pairwise disjoint:**
   - $\{1,3\} \cap \{2,6\} = \varnothing$ ✓
   - $\{1,3\} \cap \{4,5\} = \varnothing$ ✓
   - $\{2,6\} \cap \{4,5\} = \varnothing$ ✓
3. **Union covers M:** $\{1,3\} \cup \{2,6\} \cup \{4,5\} = \{1,2,3,4,5,6\} = M$ ✓

Therefore, $\mathcal{P}$ is indeed a partition of M. □

Non-Examples of Partitions

Example *(Non-partitions)*: **Why these are NOT partitions of $\boldsymbol{M = \{1, 2, 3, 4\}}$:**

- $\{\{1, 2\}, \{2, 3\}, \{4\}\}$ – blocks $\{1, 2\}$ and $\{2, 3\}$ are not disjoint
- $\{\{1\}, \{2, 3\}\}$ – union is $\{1, 2, 3\} \neq M$ (missing element 4)
- $\{\{1, 2\}, \emptyset, \{3, 4\}\}$ – contains empty set

Power Sets

Definition 12: The *power set* of a set A, denoted 2^A or $\mathcal{P}(A)$, is the set of all subsets of A.

$$\mathcal{P}(A) = \{S \mid S \subseteq A\}$$

Example: If $A = \{a, b\}$, then $\mathcal{P}(A) = \{\varnothing, \{a\}, \{b\}, \{a, b\}\}$.

Example: If $A = \{1, 2, 3\}$, then $\mathcal{P}(A) = \{\varnothing, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$.

Example: The power set of the empty set is $\mathcal{P}(\varnothing) = \{\varnothing\}$, a *non-empty* set containing the empty set.

Theorem 2: $|\mathcal{P}(A)| = 2^{|A|}$ for any finite set A.

Proof *(combinatorial)*: For each of the n elements in the set, we can either include it in a subset or not. These n independent binary choices yield 2^n possible subsets by the multiplication principle.

$$\underbrace{2 \times 2 \times \ldots \times 2}_{n \text{ times}} = 2^n \qquad \square$$

Power Sets [2]

Proof: By *induction* on $n = |A|$, the cardinality of the set A.

Base case: If $n = 0$, then $A = \emptyset$ and $\mathcal{P}(A) = \{\emptyset\}$. Thus, $|\mathcal{P}(A)| = 1 = 2^0$.

Inductive step: Assume the formula holds for any set of size k. Let A be a set with $|A| = k + 1$. Choose an arbitrary element $a \in A$ and let $A' = A \setminus \{a\}$, so $|A'| = k$.

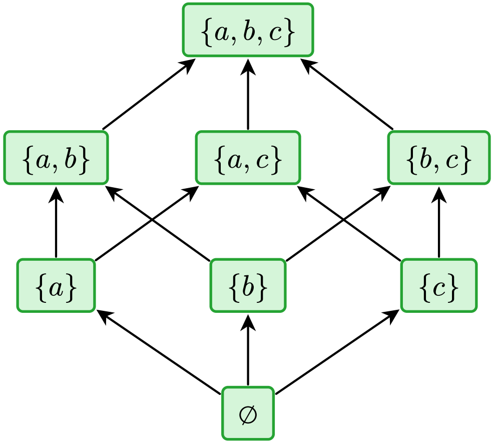
The power set $\mathcal{P}(A)$ can be partitioned into two *disjoint* collections:

1. Subsets of A that *do not* contain a. This collection is exactly $\mathcal{P}(A')$. By the inductive hypothesis, it has $|\mathcal{P}(A')| = 2^k$ elements.
2. Subsets of A that *do* contain a. Each such subset is of the form $S \cup \{a\}$ where $S \subseteq A'$. This establishes a bijection with $\mathcal{P}(A')$, so this collection also has 2^k elements.

The total number of subsets of A is the *sum* of their sizes: $|\mathcal{P}(A)| = 2^k + 2^k = 2 \cdot 2^k = 2^{k+1} = 2^{|A|}$. $\square$

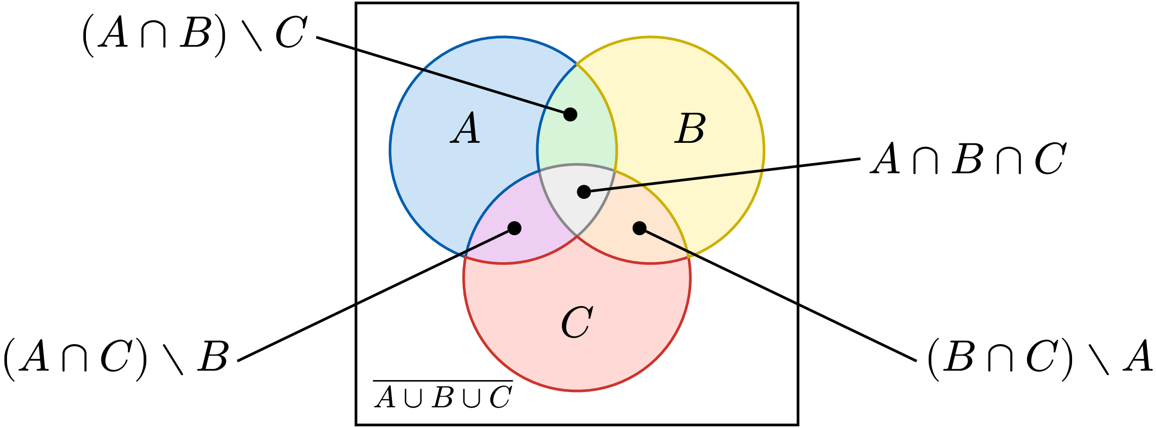
Hasse Diagram of Power Set

The elements of the power set of $\{a, b, c\}$ ordered with respect to inclusion ($\subseteq$):

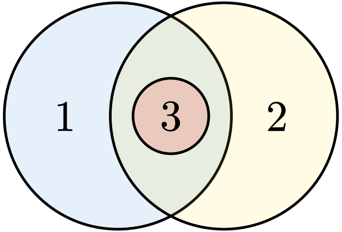


Venn Diagrams

Definition 13: A *Venn diagram* is a visual representation of sets and their relationships using overlapping circles. Each circle represents a set, and overlapping regions show intersections.

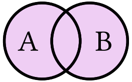
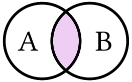
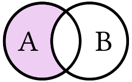
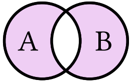
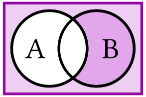


Venn Diagrams vs Euler Circles



(1) people who know what a Venn diagram is
(2) people who know what an Euler diagram is
(3) people who know the difference

Operations on Sets

Operation	Notation	Formal definition	Venn diagram
Union	$A \cup B$	$\{x \mid x \in A \lor x \in B\}$	
Intersection	$A \cap B$	$\{x \mid x \in A \land x \in B\}$	
Difference	$A \setminus B$	$\{x \mid x \in A \land x \notin B\}$	
Symmetric diff.	$A \triangle B$	$(A \setminus B) \cup (B \setminus A)$	
Complement	$\overline{A}$ or A^c	$\{x \mid x \notin A\}$	

Laws of Set Operations

For any sets A, B, C, and the universal set U:

Commutative Laws:

- $A \cup B = B \cup A$
- $A \cap B = B \cap A$

Associative Laws:

- $(A \cup B) \cup C = A \cup (B \cup C)$
- $(A \cap B) \cap C = A \cap (B \cap C)$

Distributive Laws:

- $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
- $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

De Morgan's Laws:

- $\overline{A \cap B} = \overline{A} \cup \overline{B}$
- $\overline{A \cup B} = \overline{A} \cap \overline{B}$

Identity Laws:

- $A \cup \emptyset = A$, $A \cap U = A$
- $A \cap \emptyset = \emptyset$, $A \cup U = U$

Complement Laws:

- $A \cup \overline{A} = U$, $A \cap \overline{A} = \emptyset$
- $\overline{\overline{A}} = A$ (double complement)

Proving Set Identities

Theorem 3 (Distributive Law): $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

We can prove set identities using various methods, such as:

- Element-membership approach
- Logical equivalences
- Venn diagrams (informal)

Here, we demonstrate the *element-membership approach*.

Proof: We show that $x \in A \cup (B \cap C) \iff x \in (A \cup B) \cap (A \cup C)$.

Step 1 ($\Rightarrow$): Suppose that $x \in A \cup (B \cap C)$.

- Then $x \in A$ *or* $x \in (B \cap C)$. (definition of union)
  - **Case 1:** If $x \in A$, then $x \in (A \cup B)$ and $x \in (A \cup C)$, so $x \in (A \cup B) \cap (A \cup C)$.
  - **Case 2:** If $x \in (B \cap C)$, then $x \in B$ and $x \in C$, so $x \in (A \cup B)$ and $x \in (A \cup C)$, hence $x \in (A \cup B) \cap (A \cup C)$.
- In either case, $x \in (A \cup B) \cap (A \cup C)$. (definition of intersection)

Proving Set Identities [2]

Step 2 ($\Leftarrow$): Suppose that $x \in (A \cup B) \cap (A \cup C)$.

- Then $x \in (A \cup B)$ *and* $x \in (A \cup C)$. (definition of intersection)
- Since $x \in (A \cup B)$, we have $x \in A$ or $x \in B$.
- Since $x \in (A \cup C)$, we have $x \in A$ or $x \in C$.
  - **Case 1:** If $x \in A$, then $x \in A \cup (B \cap C)$.
  - **Case 2:** If $x \notin A$, then from the conditions above, we must have $x \in B$ and $x \in C$, so $x \in (B \cap C)$, hence $x \in A \cup (B \cap C)$.
- In either case, $x \in A \cup (B \cap C)$.

Therefore, $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$. $\square$

Proving Set Identities [3]

Theorem 4 (De Morgan's Law): $\overline{A \cap B} = \overline{A} \cup \overline{B}$

Here, we use the *set inclusion approach* (double containment).

Proof: We prove $\overline{A \cap B} \subseteq \overline{A} \cup \overline{B}$ and $\overline{A} \cup \overline{B} \subseteq \overline{A \cap B}$.

Step 1 ($\subseteq$): Show $\overline{A \cap B} \subseteq \overline{A} \cup \overline{B}$.

Let $x \in \overline{A \cap B}$. We must show $x \in \overline{A} \cup \overline{B}$.

- Since $x \in \overline{A \cap B}$, we have $x \notin A \cap B$.
- This means x is *not in both* A and B simultaneously.
- Therefore, either $x \notin A$ *or* $x \notin B$ (or both).
  - If $x \notin A$, then $x \in \overline{A}$, so $x \in \overline{A} \cup \overline{B}$.
  - If $x \notin B$, then $x \in \overline{B}$, so $x \in \overline{A} \cup \overline{B}$.
- In either case, $x \in \overline{A} \cup \overline{B}$.

Step 2 ($\supseteq$): Show $\overline{A} \cup \overline{B} \subseteq \overline{A \cap B}$.

Let $x \in \overline{A} \cup \overline{B}$. We must show that $x \in \overline{A \cap B}$.

- Since $x \in \overline{A} \cup \overline{B}$, we have $x \in \overline{A}$ or $x \in \overline{B}$.
- **Case 1:** If $x \in \overline{A}$, then $x \notin A$, so $x \notin A \cap B$.
- **Case 2:** If $x \in \overline{B}$, then $x \notin B$, so $x \notin A \cap B$.
- In either case, $x \notin A \cap B$, so $x \in \overline{A \cap B}$.

Since both inclusions hold, $\overline{A \cap B} = \overline{A} \cup \overline{B}$. $\square$

Proving Set Identities [4]

Theorem 5 (Absorption Law): $A \cup (A \cap B) = A$

Here, we use an *algebraic approach* with set identities.

Proof: We apply known set laws step by step:

$$
\begin{aligned}
& A \cup (A \cap B) = \\
& = (A \cap U) \cup (A \cap B) && \text{// identity law: } A = A \cap U \\
& = A \cap (U \cup B) && \text{// distributive law} \\
& = A \cap U && \text{// since } U \cup B = U \text{ for any set } B \\
& = A && \text{// identity law: } A \cap U = A
\end{aligned}
$$

Therefore, $A \cup (A \cap B) = A$. □

Proving Set Identities [5]

Theorem 6 (Triple Equivalence): For any sets A, B, and C:

$$A \subseteq B \cup C \quad \Longleftrightarrow \quad A \setminus C \subseteq B \quad \Longleftrightarrow \quad A \cap \overline{B} \subseteq C$$

Here, we use *circular reasoning* to prove the triple equivalence: $(1) \to (2) \to (3) \to (1)$.

Proof: We prove the equivalence by showing three implications in a cycle.

Step 1 ($1 \to 2$): Show $A \subseteq B \cup C \to A \setminus C \subseteq B$.

Suppose $A \subseteq B \cup C$.

Let $x \in A \setminus C$ (left side of the conclusion). We must show $x \in B$ (right side of the conclusion).

- By definition of set difference, $x \in A$ and $x \notin C$.
- Since $A \subseteq B \cup C$, we have $x \in B \cup C$.
- Since $x \in B \cup C$ and $x \notin C$, we must have $x \in B$.

Therefore, $A \setminus C \subseteq B$.

Proving Set Identities [6]

Step 2 ($2 \to 3$): Show $A \setminus C \subseteq B \to A \cap \overline{B} \subseteq C$.

Suppose $A \setminus C \subseteq B$. Let $x \in A \cap \overline{B}$. We must show $x \in C$.

- By definition of intersection, $x \in A$ and $x \in \overline{B}$.
- Since $x \in \overline{B}$, we have $x \notin B$.
- Since $x \in A$ and $x \notin B$, we have $x \notin A \setminus C$ (otherwise $x \in B$ by our assumption).
- Since $x \in A$ but $x \notin A \setminus C$, we must have $x \in C$.

Therefore, $A \cap \overline{B} \subseteq C$.

Proving Set Identities [7]

Step 3 (3 → 1): Show $A \cap \overline{B} \subseteq C \rightarrow A \subseteq B \cup C$.

Suppose $A \cap \overline{B} \subseteq C$. Let $x \in A$. We must show $x \in B \cup C$.

- Either $x \in B$ or $x \notin B$.
  - **Case 1:** If $x \in B$, then $x \in B \cup C$.
  - **Case 2:** If $x \notin B$, then $x \in \overline{B}$, so $x \in A \cap \overline{B}$. By our assumption, $x \in C$, hence $x \in B \cup C$.

In both cases, $x \in B \cup C$. Therefore, $A \subseteq B \cup C$.

Since we have shown $(1) \rightarrow (2) \rightarrow (3) \rightarrow (1)$, all three statements are equivalent. $\square$

The *order of implications* in circular proofs is flexible. We could equally prove $(1) \rightarrow (3) \rightarrow (2) \rightarrow (1)$ or any other permutation. The key is forming a *complete cycle* where each statement implies the next.

Proof Writing Guidelines

- Always state what you want to prove clearly.
- Choose appropriate method (element-membership, logical equivalences, *etc.*).
- *Justify* each step with definitions or previously proven results.
- Handle all *cases* systematically.
- Use clear logical connectives (and, or, if-then).
- End with a clear *conclusion* ($\square$ or QED).

Tuples, Pairs, and Products

Tuples

Definition 14: A *tuple* is a finite ordered collection of elements, denoted $(a_1, a_2, ..., a_n)$.

A tuple of length n is called an *n-tuple*.

Example: (42, 🦀, 😾, 🥝) is a 4-tuple.

Definition 15: Two tuples are *equal*, denoted $(a_1, a_2, ..., a_n) = (b_1, b_2, ..., b_m)$, if and only if they have the same length ($n = m$) and corresponding elements are equal ($a_i = b_i$ for all $1 \leq i \leq n$).

Example: (🦉, 🦉) ≠ (🦉, 🦉, 🦉), these tuples are *not equal* because they have *different lengths*.

Example: (🐏, 🐐, 🐑) ≠ (🐑, 🐏, 🐐), these tuples are *not equal* because the *order* of elements *matters*.

Example: (🦊, 🦊) ≠ (🦊,) ≠ 🦊 ≠ {🦊}, these are *all different* objects: a 2-tuple, a 1-tuple, an urelement, and a singleton set.

Ordered Pairs

Definition 16: An ordered pair $\langle a, b \rangle$ is a special 2-tuple, defined[4] as:

$$\langle a, b \rangle \overset{\text{def}}{=} \{\{a\}, \{a, b\}\}$$

Example: ⟨🎃, 🧙⟩ ≠ ⟨🧙, 🎃⟩, these are different ordered pairs.

Example: ⟨🌵, 🌵⟩ ≠ (🌵,) ≠ 🌵 ≠ {🌵}, these are all different objects: an ordered pair, a 1-tuple, an urelement, and a singleton set.

Note: ⟨🌵, 🌵⟩ = {{🌵}}, using Kuratowski's definition:

$$\langle \text{🌵}, \text{🌵} \rangle = \left\{ \{\text{🌵}\}, \{\underbrace{\text{🌵}}_{\text{same}}, \underbrace{\text{🌵}}_{\text{same}}\} \right\} = \left\{ \overbrace{\{\text{🌵}\}}^{\text{equal}}, \overbrace{\{\underline{\text{🌵}}\}}^{\text{equal}} \right\} = \left\{ \overbrace{\{\text{🌵}\}} \right\}$$

[4]Kuratowski's definition is the most cited and now-accepted definition of an ordered pair. For others, see wiki.

n-Tuples as Nested Ordered Pairs

Definition 17: An *n-tuple* $(a_1, a_2, ..., a_n)$ can be defined recursively using ordered pairs:

- The 0-tuple (empty tuple) is represented by the empty set $\varnothing$.
- An n-tuple, for $n > 0$, is an ordered pair of its first element and the remaining $(n-1)$-tuple:

$$(a_1, a_2, ..., a_n) \stackrel{\text{def}}{=} \langle a_1, (a_2, ..., a_n) \rangle$$

This gives the following *recursive structure*:

$$(a_1, a_2, ..., a_n) = \langle a_1, \langle a_2, \langle ..., \langle a_n, \varnothing \rangle ... \rangle \rangle \rangle$$

Examples:

- $(1, 2, 3) = \langle 1, \langle 2, \langle 3, \varnothing \rangle \rangle \rangle$
- (😾, 🙀, 😻, 😸) = ⟨😾, ⟨🙀, ⟨😻, ⟨😸, ∅⟩⟩⟩⟩

Note: *Alternatively*, we could "peel off" the *last* element instead of the first:

$$(a_1, a_2, ..., a_n) \stackrel{\text{def}}{=} \langle (a_1, a_2, ..., a_{n-1}), a_n \rangle$$

Cartesian Product

Definition 18: The *Cartesian product* of two sets A and B, denoted $A \times B$, is defined as:

$$A \times B = \{\langle a, b\rangle \mid a \in A \text{ and } b \in B\}$$

Example: If $A = \{1, 2\}$ and $B = \{x, y, z\}$, then their product is

$$A \times B = \{\langle 1, x\rangle, \langle 1, y\rangle, \langle 1, z\rangle, \langle 2, x\rangle, \langle 2, y\rangle, \langle 2, z\rangle\}$$

Definition 19: The *n-fold Cartesian product* (also known as *Cartesian power*) of a set A is defined as:

$$A^n = \underbrace{A \times A \times \ldots \times A}_{n \text{ times}} = \{(a_1, a_2, \ldots, a_n) \mid a_i \in A\}$$

Example: $\{a, b\}^3 = \{(a, a, a), (a, a, b), (a, b, a), (a, b, b), (b, a, a), (b, a, b), (b, b, a), (b, b, b)\}$

Example: $\{$🦅$\}^3 = \{($🦅, 🦅, 🦅$)\}$, the singleton set containing the 3-tuple of three eagles.

Example: $A^0 = \{()\}$, the singleton set containing the empty tuple.

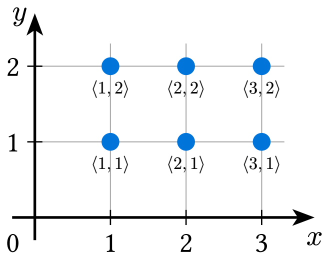
Geometric Interpretation of Cartesian Product

The Cartesian product $A \times B$ can be visualized as a region on the coordinate plane $\mathbb{R}^2$, where each point $\langle a, b \rangle$ represents an element of the product.

Example: Let $A = \{1, 2, 3\}$ and $B = \{1, 2\}$, then $A \times B$ consists of six points:

$$A \times B = \{1, 2, 3\} \times \{1, 2\} = \{\langle 1, 1 \rangle, \langle 1, 2 \rangle, \langle 2, 1 \rangle, \langle 2, 2 \rangle, \langle 3, 1 \rangle, \langle 3, 2 \rangle\}$$

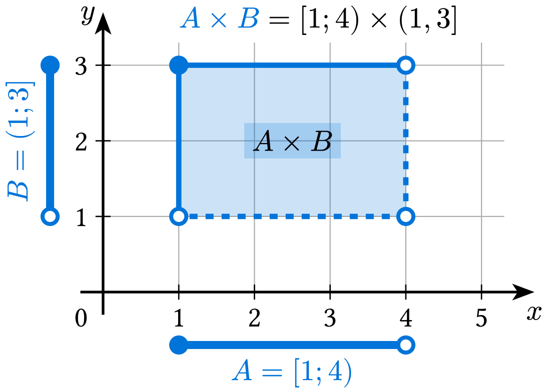
Visually, these points can be arranged in a *grid pattern*:



Geometric Interpretation of Cartesian Product [2]

Example: If $A = [1, 4)$ and $B = (1, 3]$, then $A \times B$ represents the *rectangular region*:

$$\{\langle x, y\rangle \mid 1 \leq x < 4 \text{ and } 1 < y \leq 3\}$$

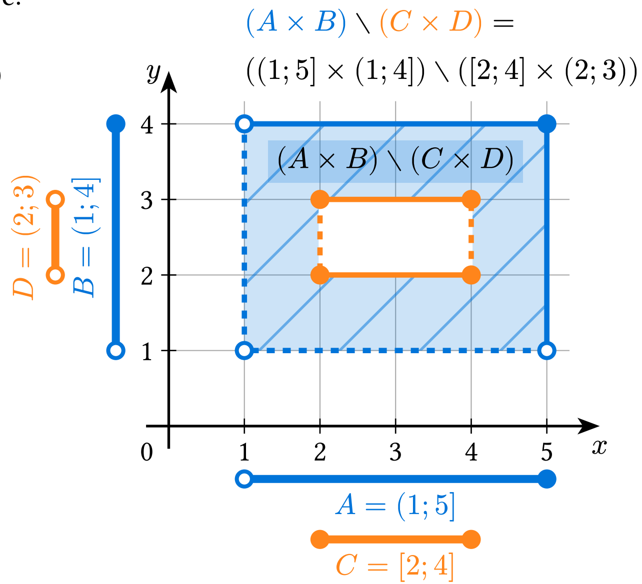


Geometric Interpretation of Cartesian Product [3]

Example: The set difference $(A \times B) \setminus (C \times D)$ where:

- $A \times B = [1;5] \times [1;4]$ (outer rectangle)
- $C \times D = (2;4) \times (2;3]$ (inner rectangle to subtract)

The resulting set is visualized on the right as the blue-shaded area with blue (outer) and orange (inner) boundaries.



Axiomatic Set Theory

The ZFC Axiom System

The *Zermelo-Fraenkel axioms with Choice* (ZFC) form the standard foundation of modern set theory:

Ernst Zermelo

Abraham Fraenkel

Definition 20 (Extensionality): Sets with the same elements are equal.

$$\forall A, B. \left[\left(\forall x. \left(x \in A \Longleftrightarrow x \in B\right)\right) \to (A = B)\right]$$

The ZFC Axiom System [2]

Definition 21 (Empty Set): There exists a set $\varnothing$ with no elements:

$$\exists \varnothing.\, \forall x.\, (x \notin \varnothing)$$

Definition 22 (Pairing): For any objects a and b, there exists a set C containing exactly them:

$$\forall a, b.\, \exists C.\, \forall x.\, \left[(x \in C) \Longleftrightarrow (x = a) \lor (x = b)\right]$$

Definition 23 (Union): For any family of sets $\mathcal{F}$, their union U exists:

$$\forall \mathcal{F}.\, \exists U.\, \forall x.\, \left[(x \in U) \Longleftrightarrow \exists A \in \mathcal{F}.\, (x \in A)\right]$$

The ZFC Axiom System [3]

Definition 24 (Power Set): For any set A, the set of all its subsets $\mathcal{P}(A)$ exists:

$$\forall A.\, \exists \mathcal{P}(A).\, \forall X.\, \left[X \in \mathcal{P}(A) \iff X \subseteq A\right]$$

Definition 25 (Infinity): There exists an infinite set (intuitively, containing natural numbers):

$$\exists S.\, \left[(\varnothing \in S) \land \forall x \in S.\, (x \cup \{x\} \in S)\right]$$

Definition 26 (Separation (Subset)): From any set A and property P, we can form the subset B of elements satisfying that property:

$$\forall A.\, \forall P.\, \exists B.\, \forall x.\, \left[(x \in B) \iff (x \in A) \land P(x)\right]$$

Note: This axiom prevents Russell's paradox by only allowing formation of subsets from existing sets.

The ZFC Axiom System [4]

Definition 27 (Replacement): If F is a function-like relation, then for any set A, the image $F[A]$ exists.

Definition 28 (Foundation (Regularity)): Every non-empty set A has a *minimal element*:

$$\forall A. \left[(A \neq \emptyset) \to \exists x \in A. (A \cap x = \emptyset)\right]$$

Note: This axiom prevents sets from containing themselves and forbids *infinite descending membership chains* like $\ldots \in x_2 \in x_1 \in x_0$. It ensures a *well-founded* hierarchy of sets.

Definition 29 (Choice): Every collection of non-empty sets $\mathcal{F}$ has a *choice function* f selecting one element from each set:

$$\forall \mathcal{F}. \left[(\emptyset \notin \mathcal{F}) \to \exists f. \forall A \in \mathcal{F}. (f(A) \in A)\right]$$

TODO

- Advanced topics in set theory:
  - Cardinal arithmetic and operations
  - Ordinal numbers and transfinite induction
  - The Continuum Hypothesis
  - Large cardinals
- Applications of set operations in:
  - Database theory (relational algebra)
  - Boolean algebra and logic circuits
  - Probability theory (events and sample spaces)
  - Computer science (formal verification)
- Further exploration of axiomatic foundations:
  - Independence results (Cohen forcing)
  - Alternative axiom systems (NBG, MK)
  - Constructive set theory

Looking Ahead: Binary Relations

The next lecture will explore *binary relations*, which provide the mathematical framework for:

- Modeling relationships between objects
- Understanding equivalence and ordering structures
- Developing function theory
- Database design and query optimization

Key topics will include:

- Relations as sets of ordered pairs
- Properties of relations (reflexive, symmetric, transitive)
- Equivalence relations and partitions
- Partial and total orders
- Closure operations on relations

Preview: Functions and Beyond

Following relations, we will study *functions* as special relations, covering:

- Function properties (injective, surjective, bijective)
- Function composition and inverse functions
- Cardinality and different types of infinity
- Applications to combinatorics and algorithm analysis

This progression from sets $\rightarrow$ relations $\rightarrow$ functions provides the foundation for:

- Boolean algebra and digital logic
- Formal logic and proof systems
- Graph theory and discrete structures
- Advanced topics in discrete mathematics

Set theory is the mathematical *lingua franca* — every mathematical concept can be defined in terms of sets. Mastering these fundamentals leads to a deeper understanding of all areas of mathematics.