# Module 2: Set Theory

## Operational math bootcamp

Statistical Sciences
UNIVERSITY OF TORONTO

Ichiro Hashimoto

University of Toronto

July 9, 2025

# Outline

- Review of basic set theory
- Ordered Sets
- Functions

# Introduction to Set Theory

- We define a *set* to be a collection of mathematical objects.
- If $S$ is a set and $x$ is one of the objects in the set, we say $x$ is an element of $S$ and denote it by $x \in S$.
- The set of no elements is called empty set and is denoted by $\emptyset$.

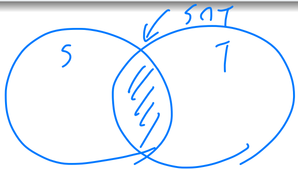
$\emptyset$ is a subset of any set

To show $S = T$, you need to show
1) $s \in S$ implies $s \in T$, 2) $t \in T$ implies $t \in S$.

## Definition (Subsets, Union, Intersection)

Let $S, T$ be sets.

- We say that $S$ is a *subset* of $T$, denoted $S \subseteq T$, if $s \in S$ implies $s \in T$.
- We say that $S = T$ if $S \subseteq T$ and $T \subseteq S$.
- We define the *union* of $S$ and $T$, denoted $S \cup T$, as all the elements that are in *either* $S$ or $T$.
- We define the *intersection* of $S$ and $T$, denoted $S \cap T$, as all the elements that are in *both* $S$ and $T$.
- We say that $S$ and $T$ are *disjoint* if $S \cap T = \emptyset$.




# Some examples

natural numbers

Integers

Real numbers

**Example**

$\mathbb{N} \subseteq \mathbb{N}_0 \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$

$\mathbb{N}_0 = \mathbb{N} \cup \{0\}$

rational numbers

complex numbers

**Example**

Let $a, b \in \mathbb{R}$ such that $a < b$.
Open interval: $(a, b) := \{x \in \mathbb{R} : a < x < b\}$ ($a, b$ may be $-\infty$ or $+\infty$)
Closed interval: $[a, b] := \{x \in \mathbb{R} : a \leq x \leq b\}$
We can also define half-open intervals.

$(a, b] = \{x \in \mathbb{R} : a < x \leq b\}$, $[a, b) = \{x \in \mathbb{R} : a \leq x < b\}$

## Example

Let $A = \{x \in \mathbb{N} : 3|x\}$ and $B = \{x \in \mathbb{N} : 6|x\}$ Show that $B \subseteq A$.

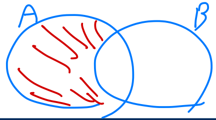
*Proof.* We need to show $x \in B$ implies $x \in A$.

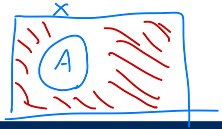
Let $x$ be any element in $B$.

By definition of $B$, there exists $k \in \mathbb{N}$ s.t. $x = 6k$.

Then, $x = 6k = 3\underbrace{(2k)}_{\in \mathbb{N}} \in A$ by definition of $A$.

# Difference of sets




## Definition

Let $A, B \subseteq X$. We define the *set-theoretic difference* of $A$ and $B$, denoted $A \setminus B$ (sometimes $A - B$) as the elements of $X$ that are in $A$ but *not* in $B$.
The complement of a set $A \subseteq X$ is the set $A^c := X \setminus A$.

## Example

Let $X \subseteq \mathbb{R}$ be defined as $X = \{x \in \mathbb{R} : 0 < x \leq 40\} = (0, 40]$. Then

$X^c =$ $(-\infty, 0] \cup (40, \infty)$

Recall that for sets $S$, $T$:

- the *union* of $S$ and $T$, denoted $S \cup T$, is all the elements that are in *either* $S$ and $T$
- and the *intersection* of $S$ and $T$, denoted $S \cap T$, is all the elements that are in *both* $S$ and $T$.

We extend the definition of union and intersection to an arbitrary family of sets as follows:

## Definition

Let $S_\alpha$, $\alpha \in A$, be a family of sets. $A$ is called the *index set*. We define

$$\bigcup_{\alpha \in A} S_\alpha := \{x : \exists \alpha \text{ such that } x \in S_\alpha\},$$

$$\bigcap_{\alpha \in A} S_\alpha := \{x : x \in S_\alpha \text{ for all } \alpha \in A\}.$$

## Example

$$\bigcup_{n=1}^{\infty} [-n, n] = (-\infty, \infty) = \mathbb{R}$$

$$\bigcap_{n=1}^{\infty} \left(-\frac{1}{n}, \frac{1}{n}\right) = \{0\}$$

## Theorem (De Morgan's Laws)

*Let $\{S_\alpha\}_{\alpha\in A}$ be an arbitrary collection of sets. Then*

$$\left(\bigcup_{\alpha\in A} S_\alpha\right)^c = \bigcap_{\alpha\in A} S_\alpha^c \quad \textit{and} \quad \left(\bigcap_{\alpha\in A} S_\alpha\right)^c = \bigcup_{\alpha\in A} S_\alpha^c$$

*Proof.*

$$\bigcup_{\alpha\in A} S_\alpha = \{x : \underbrace{\exists \alpha \in A \text{ s.t. } x \in S_\alpha}_{\downarrow \text{ negate.}}\}$$

$$\left(\bigcup_{\alpha\in A} S_\alpha\right)^c = \{x : \forall \alpha\in A,\ x \notin S_\alpha\} = \{x : \forall \alpha\in A,\ x \in S_\alpha^c\}$$

by definition of intersection →

$$= \bigcap_{\alpha\in A} S_\alpha^c$$

To prove the second result, we can reduce it to the first one.

By the first result,

$$\left( \bigcup_{\alpha \in A} S_\alpha^c \right)^c = \bigcap_{\alpha \in A} (S_\alpha^c)^c = \bigcap_{\alpha \in A} S_\alpha$$

Taking complement of both sides, we have

$$\bigcup_{\alpha \in A} S_\alpha^c = \left( \bigcap_{\alpha \in A} S_\alpha \right)^c.$$

Since a set is itself a mathematical object, a set can itself contain sets.

### Definition

The power set $\mathcal{P}(S)$ of a set $S$ is the set of all subsets of $S$.

### Example

Let $S = \{a, b, c\}$.
Then $\mathcal{P}(S) =$ $\phi, \{a\}, \{b\}, \{c\}, \{a, b\}, \{b, c\}, \{c, a\}, \{a, b, c\}$

$|P(S)| = 8 = 2^3 = 2^{|S|}$

$A \cup B$ , $A \cap B$ can be considered only when $A, B \subset X$

Another way of building a new set from two old ones is the Cartesian product of two sets.

## Definition

Let $S$, $T$ be sets. The *Cartesian product* $S \times T$ is defined as the set of tuples with elements from $S$, $T$, i.e

$$S \times T = \{(s, t) : \; s \in S \; \text{and} \; t \in T\}.$$

This can also be extended inductively to a finite family of sets.

$$\mathbb{R}^2 = \underbrace{\mathbb{R} \times \mathbb{R}}_{\substack{\cup \\ (x,y)}}$$

# Ordered set

## Definition

A *relation* $R$ on a set $X$ is a subset of $X \times X$. A relation $\leq$ is called a *partial order* on $X$ if it satisfies

1. reflexivity: $x \leq x$,
2. transitivity: if $x \leq y$ and $y \leq z$, then $x \leq z$,
3. anti-symmetry: if $x \leq y$ and $y \leq x$, then $x = y$.

The pair $(X, \leq)$ is called a *partially ordered set*.

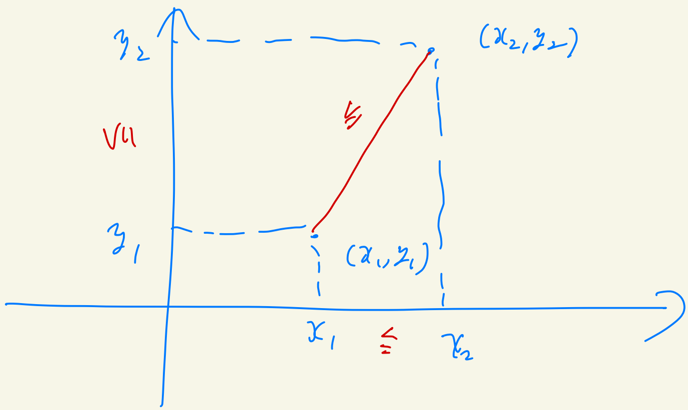
A *chain* or *totally ordered set* $C \subseteq X$ is a subset with the property $x \leq y$ or $y \leq x$ for any $x, y \in C$.

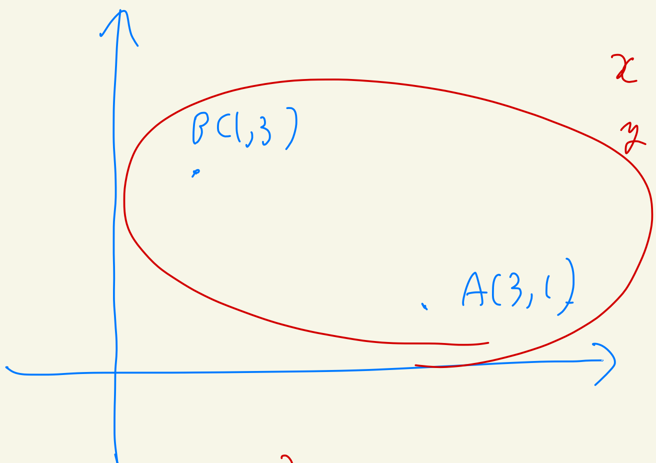
Statistical Sciences
UNIVERSITY OF TORONTO

example. On $\mathbb{R}^2$ we can define relation by

$$(x_1, y_1) \leq (x_2, y_2)$$

$$\overset{\text{def}}{\Longleftrightarrow} \quad x_1 \leq x_2 \text{ and } y_1 \leq y_2$$



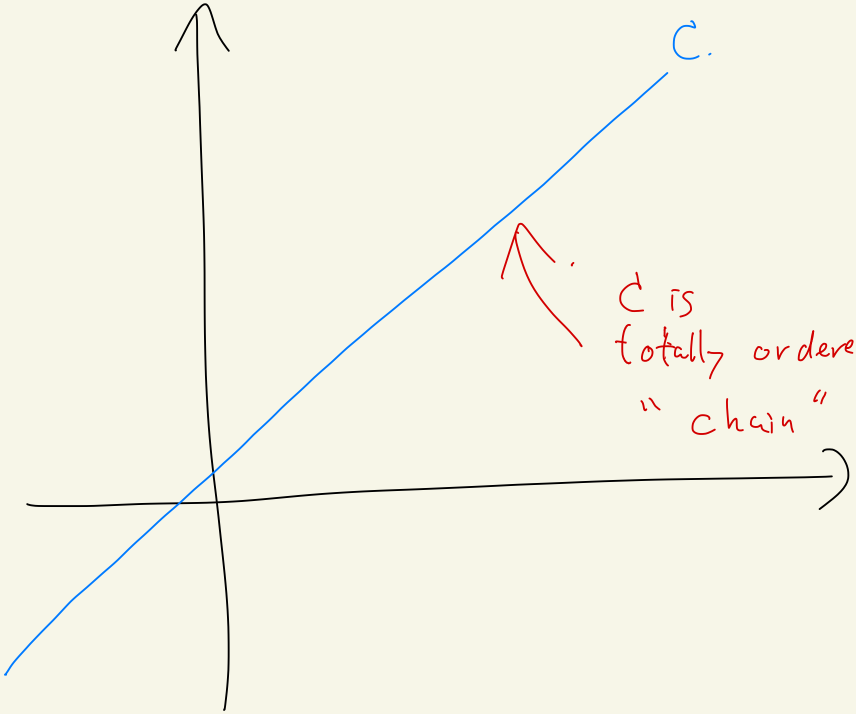

B A

$x: 1 \leq 3$

$y: 3 \nleq 1$

No order between A and B.

$\mathbb{R}^2$ is not totally ordered




C is totally ordered subset

"chain"

### Example

The real numbers with the usual ordering, $(\mathbb{R}, \leq)$ are totally ordered.

### Example

The power set of a set $X$ with the ordering given by $\subseteq$, $(\mathcal{P}(X), \subseteq)$ is a partially ordered set.

consider "$\subseteq$" as order "$\leq$"

$\mathcal{P}(X)$ is not totally ordered.

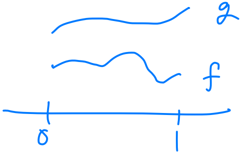
e.g. $X = \{a, b, c\}$, then $\{a\}$, $\{b, c\}$ do not have order

## Example

Let $X = \{a, b, c, d\}$. What is $\mathcal{P}(X)$? Find a chain in $\mathcal{P}(X)$.

$\mathcal{P}(X) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{d\}, \{a, b\}, \{b, c\}, \{c, d\}, \{b, d\}, \{a, c\}, \{a, d\}, \{a, b, c\}, \{b, c, d\}, \{a, b, d\}, \{a, c, d\}, X\}$

$$\underbrace{\emptyset \subset \{a\} \subset \{a, b\} \subset \{a, b, c\} \subset X}_{\text{a chain}}$$




$f \leq g$

## Example

Consider the set $C([0,1],\mathbb{R}) := \{f : [0,1] \to \mathbb{R} : f \text{ is continuous}\}$.

For two functions $f, g \in C([0,1],\mathbb{R})$, we define the ordering as $f \leq g$ if $f(x) \leq g(x)$ for $\forall$ $x \in [0,1]$. Then $(C([0,1],\mathbb{R}), \leq)$ is a partially ordered set.

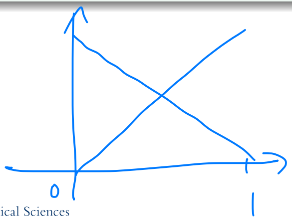
Can you think of a chain that is a subset of $(C([0,1],\mathbb{R})$?

example.

1) constant function

2) $f_n(x) = f(x) + n$

$\{f_n(x)\}$ is a chain




$f(x) = x$

$g(x) = 1 - x$

no order

## Definition

A non-empty partially ordered set $(X, \leq)$ is *well-ordered* if every non-empty subset $A \subseteq X$ has a mimimum element.

Example:

$(\mathbb{N}, \leq)$ is... well-ordered

$(\mathbb{R}, \leq)$ is... not well-ordered

$\mathbb{R}$ itself, $(a, b)$ don't have minimum

## Definition

Let $(X, \leq)$ be a partially ordered set and $S \subseteq X$.

Then $x \in X$ is an *upper bound* for $S$ if for all $s \in S$ we have $s \leq x$. Similarly, $y \in X$ is a *lower bound* for $S$ if for all $s \in S$, $y \leq s$.

If there exists an upper bound for $S$, we call $S$ *bounded above* and if there exists a lower bound for $S$, we call $S$ *bounded below*. If $S$ is bounded above and bounded below, we say $S$ is *bounded*.

We can also ask if there exists a least upper bound or a greatest lower bound.

## Definition

Let $(X, \leq)$ be a partially ordered set and $S \subseteq X$.

We call $x \in X$ *least upper bound* or *supremum*, denoted $x = \sup S$, if $x$ is an upper bound and for any other upper bound $y \in X$ of $S$ we have $x \leq y$.

$x$ is smaller than any other upper bound

Likewise, $x \in X$ is the *greatest lower bound* or *infimum* for $S$, denoted $x = \inf S$, if it is a lower bound and for any other lower bound $y \in X$, $y \leq x$.

Note that the supremum and infimum of a bounded set do not necessarily need to exist. However, if they do exists they are unique, which justifies the article *the* (exercise). Nevertheless, the reals have a remarkable property, which we will take as an axiom.

## Completeness Axiom

Let $S \subseteq \mathbb{R}$ be bounded above. Then there exists $r \in \mathbb{R}$ such that $r = \sup S$, i.e. $S$ has a least upper bound.

By setting $S' = -S := \{-s : s \in S\}$ and noting $\inf S = -\sup S'$, we obtain a similar statement for infima if $S$ is bounded below. As mentioned above, this property is fairly special, for example it fails for the rationals.

## Example

Let $S = \{q \in \mathbb{Q} : x^2 < 7\}$. Then $S$ is bounded above in $\mathbb{Q}$, but there exists no least upper bound in $\mathbb{Q}$.

if you consider sup and inf in $\mathbb{R}$, they do exist.

There is a nice alternative characterization for suprema in the real numbers.

**Proposition**

*Let $S \subseteq \mathbb{R}$ be bounded above. Then $r = \sup S$ if and only if $r$ is an upper bound and for all $\epsilon > 0$ there exists an $s \in S$ such that $r - \epsilon < s$.*

*Proof.* ($\Rightarrow$) if part

Suppose $r$ is an upper bound of $S$ and $\forall\, \varepsilon > 0, \exists\, s \in S$ s.t. $r - \varepsilon < s$. (*)

Suppose $r \neq \sup S$. Since $r$ is an upper bound, $r > \sup S$.

Let $\varepsilon = r - \sup S > 0$. By (*), $\exists\, s \in S$ s.t. $r - \varepsilon < s$

Then $s > r - \varepsilon = r - (r - \sup S) = \sup S$.

This contradicts $s \in S$.

*Proof.* $(\Leftarrow)$ Only if

Suppose $r = \sup S$.

Suppose that $\exists \varepsilon > 0$, $\forall s \in S$, $r - \varepsilon \geq s$

$r - \varepsilon$ is an upper bound of $S$.

However, $r - \varepsilon < \sup S$. This is a contradiction. //

Using the same trick, we may obtain a similar result for infima.

## Example

Consider $S = \{1/n : n \in \mathbb{N}\}$. Then $\sup S = 1$ and $\inf S = 0$.

Also the maximum

# Functions

## Definition

A function $f$ from a set $X$ to a set $Y$ is a subset of $X \times Y$ with the properties:

1. For every $x \in X$, there exists a $y \in Y$ such that $(x, y) \in f$ $\subset X \times Y$
2. If $(x, y) \in f$ and $(x, z) \in f$, then $y = z$. $\longrightarrow$ For each $x$, a unique $y$ is associated.

$X$ is called the *domain* of $f$.

How does this connect to other descriptions of functions you may have seen?

## Example

For a set $X$, the identity function is:

$$1_X : X \to X, \quad x \mapsto x$$

## Definition (Image and pre-image)

Let $f : X \to Y$ and $A \subseteq X$ and $B \subseteq Y$.

- The *image* of $f$ is the set $f(A) := \{f(x) : x \in A\}$.
- The *pre-image* of $f$ is the set $f^{-1}(B) := \{x : f(x) \in B\}$.

Helpful way to think about it for proofs:

**Image:** If $y \in f(A)$, then $y \in Y$, and there exists an $x \in A$ such that $y = f(x)$.

**Pre-image:** If $x \in f^{-1}(B)$, then $x \in X$ and $f(x) \in B$.

## Definition (Surjective, injective and bijective)

Let $f : X \to Y$, where $X$ and $Y$ are sets. Then

- $f$ is *injective* if $x_1 \neq x_2$ implies $f(x_1) \neq f(x_2)$ $\quad Y = f(x)$
- $f$ is *surjective* if for every $y \in Y$, there exists an $x \in X$ such that $y = f(x)$
- $f$ is *bijective* if it is both injective and surjective

## Example

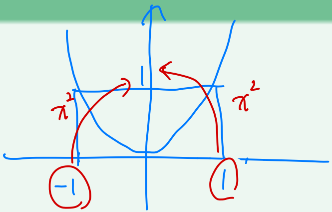
Let $f : X \to Y$, $x \mapsto x^2$.

$f$ is surjective if $\quad X = \mathbb{R}, \quad Y = \mathbb{R}_{\geq 0}$

$f$ is injective if $\quad X = \mathbb{R}_{\geq 0}$

$f$ is bijective if $\quad X = \mathbb{R}_{\geq 0}, \quad Y = \mathbb{R}_{\geq 0}$

$f$ is neither surjective nor injective if




$X = Y = \mathbb{R}$

# References

Marcoux, Laurent W. (2019). *PMATH 351 Notes*. url: https://www.math.uwaterloo.ca/ lwmarcou/notes/pmath351.pdf

Runde ,Volker (2005). *A Taste of Topology*. Universitext. url: https://link.springer.com/book/10.1007/0-387-28387-0

Zwiernik, Piotr (2022). *Lecture notes in Mathematics for Economics and Statistics*. url: http://84.89.132.1/ piotr/docs/RealAnalysisNotes.pdf