21127 Concept of Mathematics Notes

Yutian Chen

April 17, 2022

Contents

Chapter 1

Preface

1.1 Introduction to 21-127

1.1.1 Course Info

Garrett Ervin

Textbook: Sullivan.pdf

Rubric:

- HW - 30%
- Quizzes - 10%
- 2 Midterms - 15%
- Final - 30%

There will have Quizzes on Wednesday. Using LaTeX to finish homework will receive 1 extra credit.

1.1.2 Overview and Foundation

- This Class is an intro to writing proofs
- Set Algebra, Logic, Induction, Relation/Function, ...

What is 'doing math' ? $\rightarrow$ It's about investigating mathematical objects (e.g. integers, line, continuous functions, ...) by proving or deproving mathematical statements.

Mathematical objects are described by precise definitions.

Definition (Mathematical Statement). Mathematical statements (a.k.a. propositions) are declarative sentences about mathematical objects that are either true or false.

Definition (Proof). (roughly) A proof is a sequence of logical deductions from axioms or previously proved statements whose conclusion is the proposition in question.

Theorem 1.1: Infinite Prime

There are infinitly many primes.

Proof. sps toward a contradiction that proposition 1.1 is false, i.e. that there are finitely many primes. Then we can list all the primes

$$p_1, p_2, \cdots, p_n$$

Consider the integer

$$N = p_1 p_2 \cdots p_n + 1$$

Since N is not divisible by any of $p_1, p_2, \cdots, p_n$, N is either a new prime number not in our previous enumeration, or there is some prime number $p_i < N$ not in the list of primes.

On both case, there is a prime out of our list of primes, which contradict with our assumption.

Therefore, there are infinitely many primes.

□

Chapter 2

Set Theorem

2.1 Introduction to Set

Definition (Set). (roughly) A set is a collection of objects. (sometimes described by a common property)

Objects in a set are called elements.

Definition (Law of Extensionality). Sets are determined by their elements. Order and repetition of elemetns don't matter.

Sets can be elements of sets!

2.1.1 In, Intersection and Union

- $a \in A$ means 'a is an element of set A'
- $b \notin A$ means 'b is *not* and element of set A'

Suppose we have two sets A and B, then we have

Definition (Intersection). $A \cap B$ is the set where every element in it is both in A and in B.

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

Definition (Union). $A \cup B$ is teh set where every element in it is either in A and in B.

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

2.1.2 Some Fundamental Sets

Notation	Meaning
$\mathbb{N}$	Natural Numbers = $\{1, 2, \cdots\}$
$\mathbb{Z}$	Integers = $\{-2, -1, 0, 1, \cdots\}$
$\mathbb{R}$	Real Numbers
$\mathbb{Q}$	Rational Numbers = $\left\{ \frac{p}{q} \middle\| p, q \in \mathbb{N}, q \neq 0 \right\}$
$\mathbb{C}$	Complex Numbers = $\{a + bi \mid a, b \in \mathbb{R}\}$
$\emptyset$ or $\{\}$	Set that contains no element

*In the context of this course, $0 \notin \mathbb{N}$.

2.1.3 Roster Notation & Set-builder Notation

Definition (Roster Notation). Finite sets can be defined by writing all of their elements in brackets. This is called **roster notation**

Definition (Set builder Notation). (axiom of restricted comprehension)

Given a set X and a property P, we can define a set Y consisting of elements of X with property P. We can denote Y as

$$Y = \{x \in X \mid x \text{ has } P\}$$

> **Example.** *Define the set of all even natural numbers E using set builder notation.*

Solution.

$$E = \{n \in \mathbb{N} \mid \exists k \in \mathbb{N} \; s.t \; n = 2k\}$$

$\rightarrow$ *End of Solution*

2.1.4 Special Notations for This Course

$[n]$ denotes a set $\{i \in \mathbb{N} \mid i \leq n\}$ in this course. This is NOT a common notation and is only used in the context of this course.

2.1.5 Subset

Definition (Subset Equal). A set y is a subset of a set X if for every $y \in Y$ we have $y \in X$. Denoted as

$$Y \subseteq X$$

Definition (Proper (strict) Subset). We say Y is a proper subset of X if $Y \subseteq X$ and $Y \neq X$. It will be denoted as

$$Y \subset X \text{ or } Y \subsetneq X$$

Theorem 1.1: Transitivity of Subset

For any sets A, B and C:

If $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

Proof. Suppose $x \in A$ is a fixed, arbitrary element of A.

Since $A \subseteq B$, we have $x \in B$, by definition of subset.

Since $B \subseteq C$, we have $x \in C$, again by definition of subset.

Since $x \in A$ was arbitrary, the same argument applies to any element of A.

Therefore, every element of A is an element of C. i.e. $A \subseteq C$ $\square$

2.2 More Concepts of Sets

2.2.1 Difference and Complement of Sets

Definition (Difference of Sets). $A - B$ denotes the difference of A and B.

$$x \in A - B \quad \text{iff } x \in A \wedge x \notin B$$

Notes. Difference is not a commutative operation.

Definition (Complement). Given a set A and a universal set u and $A \subseteq u$, the complement of A, denoted $\bar{A}$, is the set of elements in u but not in A.

$$\bar{A} = \{x \in u \mid x \notin A\}$$

2.2.2 Indexing Sets

Definition (Indexed Union and Intersection). Suppose that I is a set (the index set) s.t. for every index $i \in I$, we've defined a set A_i.

We defined

$$\bigcup_{i \in I} A_i$$

as the set of elements contained in at least one of the A_i. i.e. $x \in \bigcup_{i \in I} A_i$ iff $\exists i \in I$ s.t. $x \in A_i$.

We also define

$$\bigcap_{i \in I} A_i$$

as the set of elements contained in every A_i. i.e. $x \in \bigcap_{i \in I} A_i$ iff $\forall i \in I$ we have $x \in A_i$.

Definition (Collection of Index Sets). If for every $i \in I$ we've defined A_i. We will write

$$\{A_i : i \in I\}$$

for the set where elements are sets A_i.

2.2.3 Powersets

Definition (Powerset). Given a set X, the powerset of X is denoted as $\mathcal{P}(A)$. It's the set of all subsets of x, i.e.

$$y \in \mathcal{P}(X) \text{ iff } y \subseteq X$$

Theorem 2.1

For any set A, B. If $A \subseteq B$, then $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.

Proof. For some arbitrary, fix $X \in \mathcal{P}(A)$

Then $X \subseteq A$, by the definition of powerset.

Since $A \subseteq B$, we have $X \subseteq B$ by *transitivity of subset*

Hence $X \in \mathcal{P}(B)$.

Since $X \in \mathcal{P}$ is arbitrary, we've proved every element in $\mathcal{P}(A)$ is an element of $\mathcal{P}(B)$. Therefore, $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.

□

2.2.4 Cartesian Products

Definition (Cartesian Product). The cartesian product of two sets A, B is denoted by $A \times B$. It's the set S of all ordered pairs (a, b) with $a \in A$, $b \in B$.

Here's an informal set builder notation of $A \times B$

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

> *Notes.* The cartesian product $A \times B \times C$ is NOT the same as $(A \times B) \times C$.
>
> $$A \times B \times C = (a, b, c) \text{ while } (A \times B) \times C = ((a, b), c)$$

2.3 Proofs with Sets

2.3.1 Subset Relationship

Proving $A \subseteq B$

1. Fix an arbitrary $a \in A$
2. Prove $a \in B$
3. Since a is arbitrary, that every element of A belongs to B, i.e. $A \subseteq B$.

Proof. Suppose A, B, X are sets. If $X \subseteq A$ and $X \subseteq B$, then $X \subseteq A \cap B$.

- Fix $x \in X$
- Since $X \subseteq A$, we have $x \in A$ by definition of subset.
- Since $X \subseteq B$, we have $x \in B$ for similar reason.
- hence $x \in A \cap B$
- Since $x \in X$ was arbitrary, we've proved $X \subseteq A \cap B$.

□

Proof. Suppose A, B are sets, then $\mathcal{P}(A) \cap \mathcal{P}(B) \subseteq \mathcal{P}(A \cap B)$

- Fix $X \in \mathcal{P}(A) \cap \mathcal{P}(B)$
- then $X \in \mathcal{P}(A)$ and $X \in \mathcal{P}(B)$
- hence $X \subseteq A$ and $X \subseteq B$
- by previous proposition, we have $X \subseteq A \cap B$
- hence $X \in \mathcal{P}(A \cap B)$
- since $X \in \mathcal{P}(A) \cap \mathcal{P}(B)$ is an arbitrary element, same argument applies to every element of $\mathcal{P}(A) \cap \mathcal{P}(B)$.
- hence $\mathcal{P}(A) \cap \mathcal{P}(B) \subseteq \mathcal{P}(A \cap B)$.

□

2.3.2 Set Equality

A set is determined by its elements: two sets are equal exactly when they contain the same elements.

Definition (Set equality). For sets A, B, we define

$$A = B \text{ iff } A \subseteq B \wedge B \subseteq A \qquad \text{(Double Containment Proof)}$$

> **Example.** *For any sets A, B, C, we have $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$*

Proof. First, we want to show that

$$A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$$

- Fix $x \in A \cap (B \cup C)$
- Then $x \in A$ and $x \in B \cup C$
- Since $x \in B \cup C$, we have either
- Case 1: $x \in B$
  - Since $x \in A$, we have $x \in A \cap B$
  - Hence $x \in (A \cap B) \cup (A \cap C)$
- Case 2: $x \in C$
  - Since $x \in A$, we have $x \in A \cap C$
  - Hence $x \in (A \cap B) \cup (A \cap C)$
- Since x is an arbitrary element of $A \cap (B \cup C)$, same argument applies to every element of $A \cap (B \cup C)$.
- Therefore, $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$

Then, we want to show that

$$(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$$

- Fix $x \in (A \cap B) \cup (A \cap C)$
- Case 1: $x \in A \cap B$
  - Hence $x \in A$ and $x \in B$
  - Hence $x \in A$ and $x \in B \cup C$
  - Therefore $x \in A \cap (B \cup C)$
- Case 2: $x \in A \cap C$
  - Hence $x \in A$ and $x \in C$
  - Hence $x \in A$ and $x \in B \cup C$
  - Therefore $x \in A \cap (B \cup C)$
- Hence in all cases $x \in A \cap (B \cup C)$
- Since $x \in (A \cap B) \cup (A \cap C)$ was arbitrary, we've proved $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$
- Hence $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

□

2.3.3 Proof by Contradiction

To proof that a statement S is true, you can:

1. Suppose toward contradiction that S is false
2. Prove that assumption contradicts your hypothesis or a previously proved statement.
3. Conclude S is true

> **Example.** *Proposition: For every $n \in \mathbb{N}$, define*
>
> $$A_n = \left\{ x \in \mathbb{R} \,\middle|\, 0 \leq x < \frac{1}{n} \right\}$$
>
> *Then we know:*
>
> $$\bigcap_{n \in \mathbb{N}} A_n = \{0\}$$

Proof. ($\subseteq$) Proving $\{0\} \subseteq \bigcap_{n\in\mathbb{N}} A_n$ os equivalent to proving $\{0\} \in \bigcap_{n\in\mathbb{N}} A_n$, i.e. for every $n \in \mathbb{N}$ we have $0 \in A_n$

- Fix $n \in \mathbb{N}$
- Since $A_n = \left\{ x \in \mathbb{R} \,\middle|\, 0 \leq x < \frac{1}{n} \right\}$
- Clearly $0 \in A_n$ since $0 \leq 0 < \frac{1}{n}$
- Since $n \in \mathbb{N}$ is arbitrary, we've proved for every $n \in \mathbb{N}$, $0 \in A_n$
- i.e. $0 \in \bigcap_{n\in\mathbb{N}} A_n$
- $\{0\} \subseteq \bigcap_{n\in\mathbb{N}} A_n$

($\supseteq$) We want to show $\bigcap_{n\in\mathbb{N}} A_n \subseteq \{0\}$

- Fix $x \in \bigcap_{n\in\mathbb{N}} A_n$, we want to show $x \in \{0\}$
- Suppose toward a contradiction, that $x \neq 0$
- Since $x \in \bigcap_{n\in\mathbb{N}} A_n$ in particular we have $x \in A_1$, i.e. $0 \leq x < 1$
- But since $x \neq 0$, it must be $x \geq 0$
- Pick on an $N \in \mathbb{N}$ large enough so that $\frac{1}{N} < x$.
- But then $x \notin A_N$ since $A_N = [0, \frac{1}{N})$
- There is a contradiction since $x \in A_n$ for any $n \in \mathbb{N}$
- Hense it must be $x = 0$.
- Hence $x \in \{0\}$
- Since $x \in \bigcap_{n\in\mathbb{N}} A_n$ was arbitrary, we've proved $\bigcap_{n\in\mathbb{N}} A_n \subseteq \{0\}$

Hence $\bigcap_{n\in\mathbb{N}} A_n = \{0\}$. □

Chapter 3

Mathematical Logic

3.1 Intro to Mathematical Logic

Goals

- Learn how to write statements more formally (more symbols)
- See how the form of a statement suffests the form of its own proof

3.1.1 Mathematical Statement

Definition (Mathematical Statement). A Mathematical statement (or proposition) is a grammatically correct declarative statement that is either true or false.

Definition (Variable Proposition). A meaningful, correct sentence that becomes a statement once the variables are specified.

If P represents such a sentence, then $P(x)$ represent the proposition with specified variable x.

> **Example (Statements).** *There are two types of statements - universal and existential statement.*
>
> 1. *Every integer is a real number. (Universal Statement)*
> 2. *There exists some $x \in \mathbb{R}$ s.t. $x \notin \mathbb{Z}$ (Existential Statement)*
> 3. *$x^2 + 1 = 2$ (Variable Proposition)*

> **Example (How to write Proposition).** *Let $P(x)$ denote the variable proposition $x^2 + 1 = 2$.*
>
> *Then $P(1) = P(-1) = True$, while $P(x) = False$ $\forall x \in \mathbb{R} \backslash \{1, -1\}$*

3.2 Logical Quantifiers

3.2.1 $\forall$ And $\exists$ Quantifiers

The other way to write a variable proposition into a statement is to **quantify** the variables.

Definition (Existential Quantifier). The '$\exists$' is called the "existential quantifier" - we read it as "there exists".

Definition (Universal Quantifier). The '$\forall$' is called the "universal quantifier" - we read it as "for all".

Given a ariable proposition $P(x)$ and a set S, we can convert the variable proposition into a mathmetical statement

- There exists $x \in S$ s.t. $P(x) \implies \exists x \in S \; s.t. \; P(x)$ (Also written as $\exists x \in S.P(x)$)
- For all $x \in S$ s.t. $P(x) \implies \forall x \in S \; s.t. \; P(x)$ (Also written as $\forall x \in S.P(x)$)

3.2.2 Multiple Quantifiers

We can also use multiple quantifiers together:

> **Example.** *Consider $x + y \geq 2$, we can say*
>
> $$(\forall x \in \mathbb{N}) \; (\forall y \in \mathbb{N}) \; x + y \geq 2$$

When multiple quantifiers in a row are the same (all $\forall$ or all $\exists$), then order is irrelevant

However, when there the quantifiers are different, the order do matter.

> *Notes.* We insist all quantified variablesrange over a specified set S. The 'background set' **must** be explicitly defined.

3.2.3 Special Case: Quantifier on Sets ...

But ... what if we want to quantify over variables referring to sets?

If we specify the variable into a 'set that contains all sets', then **Contor's Paradox** will occur. Therefore, when we want to say '$\forall S$', we have to say

'For all sets S' or 'there exists set S' instead of using notation form.

3.3 Connectives

3.3.1 And $\wedge$, Or $\vee$ and Negation $\neg$

Definition (Connectives). Connectives are symbols use to combine multiple statement into one. All of the connectives will be binary operation, except for negation (which is unary).

Definition (Conjunction). Conjunction is 'logical and', denoted as $\wedge$. The truth table of $P \wedge Q$ is:

P	Q	$P \wedge Q$
T	T	T
T	F	F
F	T	F
F	F	F

Definition (Disjunction). Disjunction is 'logical or', denoted as $\vee$. The truth table of $P \vee Q$ is:

P	Q	$P \vee Q$
T	T	T
T	F	T
F	T	T
F	F	F

Definition (Negation). Negation is 'logical not', denoted as $\neg A$ (or sometimes $\overline{A}$)

P	$\neg P$
T	F
F	T

- $P \vee \neg P$ is always True
- $P \wedge \neg P$ is always False

Truth tables tell us how truth value of connected statements depend on the truth values of their constituent statement.

3.3.2 Logic Operation and Set Operation

We can represent set operation using the logic operations

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

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

$$\overline{A} = \{x \in U \mid \neg(x \in A)\}$$

3.3.3 Logical Implication

Definition (Implication). Given two mathematical statement P and Q, the statement $P \implies Q$ is read 'P implies Q' or 'If P then Q'

P	Q	$P \implies Q$
T	T	T
T	F	F
F	T	T
F	F	T

Notes. $P \implies Q$ is always true when P is true.

When P is false, $P \implies Q$ is called 'vacuous truth'

When calculating the negation of $P \implies Q$, we have

$$\neg(P \implies Q) = P \wedge (\neg Q)$$

Proof.

$$\begin{aligned} \neg(P \implies Q) &\implies \neg(\neg(P) \vee Q) \\ &\implies P \wedge (\neg Q) \end{aligned}$$

□

Example.

$$(\forall x \in \mathbb{R})(x \geq 2) \implies (x^2 \geq 4)$$

is a true statement.

Proof. For any $x \in \mathbb{R}$, Either $x \geq 2$, where $x^2 \geq 4$ is also true, and $T \implies T$ is a true statement.

Or $x < 2$, where the statement is true vacuosly. □

3.3.4 Logical Equivalence

Definition (Equivalence). Given statement P, Q, the statement $P \iff Q$ is read 'P if and only if Q'.

The statements P, Q are called logically equivalent if they have the same truth value.

The truth table of equivalence is:

P	Q	$P \iff Q$
T	T	T
T	F	F
F	T	F
F	F	T

The following logical equivalence hold for any mathematical statement P and Q:

1. $(P \implies Q) \iff (\neg P \vee Q)$
2. $(P \implies Q) \iff (\neg Q \implies \neg P)$ (Contrapositive)
3. $(P \iff Q) \iff ((P \implies Q) \wedge (Q \implies P))$

3.4 Negating Logical Operations

3.4.1 Negating Quantified Statements

Theorem 4.1

Suppose $P(x)$ is a variable proposition and S is a set. Then we have

- $\neg(\forall x \in S)P(x) \iff (\exists x \in S)\neg P(x)$
- $\neg(\exists x \in S)P(x) \iff (\forall x \in S)\neg P(x)$

When there are multiple quantifiers, iterate the process (apply negation on each quantifier)

$$\neg(\forall x \in \mathbb{R})(\exists y \in \mathbb{R})(xy = 1) \iff (\exists x \in \mathbb{R})(\forall y \in \mathbb{R})(xy \neq 1)$$

3.4.2 Negating Connected Statements

Theorem 4.2

For any P, Q that following logical equivalences hold (i.e. The statemetns below are always true)

- $\neg\neg P \iff P$
- $\neg(P \wedge Q) \iff (\neg P) \vee (\neg Q)$
- $\neg(P \vee Q) \iff (\neg P) \wedge (\neg Q)$

To prove the statements above are always true, we need to use the truth table:

P	$\neg P$	$\neg\neg P$	$\neg\neg P \iff P$
T	F	T	T
F	T	F	T

Since for every row of the truth table, we have $\neg\neg P \iff P$ is true, the statement is always true.

Proof. We want to show that $\neg(P \wedge Q) \iff \neg P \vee \neg Q$

P	Q	$P \wedge Q$	$\neg(P \wedge Q)$	$\neg P$	$\neg Q$	$\neg P \vee \neg Q$	$\neg(P \wedge Q) \iff \neg P \vee \neg Q$
T	T	T	F	F	F	F	T
T	F	F	T	F	T	T	T
F	T	F	T	T	F	T	T
F	F	F	T	T	T	F	T

Since for all rows in the truth table, we have T for $\neg(P \wedge Q) \iff \neg P \vee \neg Q$, this statement is always true. □

Definition (Positive Form). A statement P is in positive form iff any negation symbol in P occur necxt to substatements with no variables or quantifiers.

(i.e. $\neg$ are as "inside as possible")

It is possible to find the logically equivalent statement P' in positive form for any mathematical statement P.

3.4.3 Negating Implies and Logical Equivalence

Theorem 4.3

The following logical equivalency hold

- $\neg(P \implies Q) \iff (P \wedge \neg Q)$
- $\neg(P \iff Q) \iff ((P \wedge \neg Q) \vee (\neg P \wedge Q))$

Example. *Convert the following mathematical statement into its positive form:*

$$\neg(\forall x \in \mathbb{R})((x \geq 0) \iff (\exists y \in \mathbb{R})(y^2 = x))$$

Solution.

$$\begin{aligned}
&\neg(\forall x \in \mathbb{R})((x \geq 0) \iff (\exists y \in \mathbb{R})(y^2 = x)) \\
&\iff (\exists x \in \mathbb{R})\neg((x \geq 0) \iff (\exists y \in \mathbb{R})(y^2 = x)) \\
&\iff (\exists x \in \mathbb{R})\left((x \geq 0) \wedge \neg(\exists y \in \mathbb{R})(y^2 = x) \vee \neg(x \geq 0) \wedge (\exists y \in \mathbb{R})(y^2 = x)\right) \\
&\iff (\exists x \in \mathbb{R})\left((x \geq 0) \wedge (\forall y \in \mathbb{R})(y^2 \neq x) \vee (x < 0) \wedge (\exists y \in \mathbb{R})(y^2 = x)\right)
\end{aligned}$$

→ *End of Solution*

3.4.4 More Useful Equivalences

- $$P \wedge (Q \wedge R) \iff (P \wedge Q) \wedge R$$
- $$P \vee (Q \vee R) \iff (P \vee Q) \vee R$$
- $$P \wedge (Q \vee R) \iff (P \wedge Q) \vee (P \wedge R)$$
- $$P \vee (Q \wedge R) \iff (P \vee Q) \wedge (P \vee R)$$

3.5 Connection between Set and Logical Operation

There is an analogy between the logical connectives and the set operations.

Logical Operation	Set Operation	Explanation
$P \wedge Q$	$A \cap B$	$x \in A \wedge x \in B$
$P \vee Q$	$A \cup B$	$x \in A \vee x \in B$
$\neg P$	$\overline{A}$	$\neg(x \in A)$

Moreover, the stement analogy can also apply with quantifiers ...

Logical Operation	Set Operation
$(\forall x \in A)(x \in B)$	$A \subseteq B$
$(\forall x \in U)(x \in A \iff x \in B)$	$A = B$

Notes. Though such analogy between logical operation and set operations exists, the set operations $\cap$, $\cup$ and $\overline{A}$ only applies to set. It's meaningless to apply them on mathematical statements. (and vice versa for logical operators)

Theorem 5.1

Suppose A, B are sets and both subsets of U, then we have

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

Proof. 1. We w.t.s. $\overline{\overline{A}} = A$

- Let $x \in U$ be a fixed, arbitrary element of U.
- Then

$$\begin{aligned} x \in \overline{\overline{A}} &\iff x \notin \overline{A} \\ &\iff \neg(x \in \overline{A}) \\ &\iff \neg(\neg x \in A) \\ &\iff x \in A \end{aligned}$$

- We have proved $x \in \overline{\overline{A}} \iff x \in A$.
- Since x is arbitrary element in U, same argument applies to every element of U.
- We have proved that $(\forall x \in U)(x \in \overline{\overline{A}} \iff x \in A)$
- Therefore, we have $\overline{\overline{A}} = A$

2. We w.t.s. $\overline{A \cap B} = \overline{A} \cup \overline{B}$

- Let $x \in U$ be a fixed, arbitrary element of U.
- Then

$$\begin{aligned} x \in \overline{A \cap B} &\iff \neg(x \in A \cap B) \\ &\iff \neg(x \in A \wedge x \in B) \\ &\iff x \in \overline{A} \vee x \in \overline{B} \\ &\iff x \in \overline{A} \cup \overline{B} \end{aligned}$$

- We have proved $x \in \overline{A \cap B} \iff x \in \overline{A} \cup \overline{B}$
- Since x is arbitrary element in U, same argument applies to every element of U.
- We have proved that $(\forall x \in U)(x \in \overline{A \cap B} \iff x \in \overline{A} \cup \overline{B})$
- Therefore, we have $\overline{A \cap B} = \overline{A} \cup \overline{B}$

□

Theorem 5.2

For any sets A, B, C, we have

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

3.6 How to Write Proof

There are always two approaching - to prove P, one can prove directly, or assume $\neg P$ and derive a contradiction.

3.6.1 Existence Statements - $(\exists x \in S)\ P(x)$

Direct Proof: Find a specific $x \in S$ and prove $P(x)$

Indirect proof: (contradiction): Assume $\neg(\exists x \in S)P(x)$, then derive a contradiction.

3.6.2 Universal Statement - $(\forall x \in S)\ P(x)$

Direct Proof: Let x be an arbitrary, fixed element of S, show that $P(x)$ is true.

Indirect Proof: Suppose there exists $x \in S$ such that $P(x)$ is false, derive contradiction from this assumption.

3.6.3 Conditional Statement - $P(x) \implies Q(x)$

Directly: Assume P, prove Q

By Contrapositive: Prove $\neg Q \implies \neg P$

Indirectly: Assume there exists case where $P \wedge \neg(Q)$, derive contradiction

3.6.4 Equivalence Statement - $P(x) \iff Q(x)$

Proof From both Directions: Prove $P \implies Q$ and $Q \implies P$

Proof Directly Showing that $P \iff Q$

Chapter 4

Induction Proof

4.1 Induction Proof (Weak Induction)

4.1.1 Principle of Mathematial Induction, PMI

Theorem 1.1: PMI - Principle of Mathematial Induction

Suppose $P(n)$ is a variable proposition. Suppose further that we have

1. $P(1)$ - the base case is true
2. $(\forall n \in \mathbb{N})(P(n) \implies P(n+1))$ - Inductive Case

Then we can conclude that $(\forall n \in \mathbb{N})P(n)$ is true.

Notes. PMI is best thought of a reasoning principle as opposed to a theorem. In this course, we will take PMI as an **axiom**.

To use PMI to prove $(\forall n \in \mathbb{N})P(n)$, we need

1. Base Case (BC) - Verify $P(1)$
2. Inductive Hypothesis (IH) - Fix $n \in \mathbb{N}$, assume $P(n)$
3. Inductive Step (IS) - Using the assumption, prove $P(n+1)$

Example. *What is the sum of first n odd integers?*

$$\begin{aligned} 1 &= 1 &&= 1^2 \\ 1+3 &= 4 &&= 2^2 \\ 1+3+5 &= 9 &&= 3^2 \\ &\cdots \end{aligned}$$

That is, do the equation below always hold?

$$1 + 3 + \cdots + (2n-1) = n^2$$

Proof.

Base Case Observed the identity is true for $n = 1$ since

$$\sum_{k=1}^{1} (2k-1) = 1^2$$

Inductive Case Fix $n \in \mathbb{N}$. Suppose we know the identity for n, that is, assume

$$\sum_{k=1}^{n} (2k-1) = n^2$$

we want to show that

$$\sum_{k=1}^{n+1} (2k-1) = (n+1)^2$$

That is,

$$n^2 + (2(n+1)-1) = (n+1)^2$$

Because we have

$$\begin{aligned} n^2 + (2(n+1)-1) &= n^2 + 2n + 1 \\ &= (n+1)^2 \end{aligned}$$

Therefore, the equality holds for any $n \in \mathbb{N}$. □

> **Example.** *Prove that*
>
> $$\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$$

Proof.

Base Case: When $n = 1$, we have

$$1 = \frac{1(1+1)}{2} = \frac{2}{2} = 1$$

So the proposition is true for $n = 1$

Inductive Hypothesis For some fixed, arbitrary $n \in \mathbb{N}$, assume

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$$

Inductive Step We wants to show that

$$\sum_{k=1}^{n+1} k = \frac{(n+1)(n+2)}{2}$$

$$\begin{aligned} \sum_{k=1}^{n+1} k &= \sum_{k=1}^{n} k + (n+1) \\ &= \frac{n(n+1)}{2} + (n+1) \\ &= \frac{n(n+1) + 2(n+1)}{2} \\ &= \frac{(n+2)(n+1)}{2} \end{aligned}$$

□

Example. *Prove that for $x \in \mathbb{R}$ where $x \neq 0$, then for every $n \in \mathbb{N}$, we have*

$$1 + x + x^2 + \cdots + x^{n-1} = \frac{x^n - 1}{x - 1}$$

That is,

$$\sum_{k=0}^{n-1} x^k = \frac{x^n - 1}{x - 1} \qquad \text{(Sum of Geometric Series)}$$

Proof.

Base Case if $n = 1$, we have

$$\sum_{k=0}^{0} = x^0 = 1 = \frac{x - 1}{x - 1}$$

Inductive Hypothesis Let $n \in \mathbb{N}$ be a fixed element of $\mathbb{N}$, assume

$$\sum_{k=0}^{n-1} x^k = \frac{x^n - 1}{x - 1}$$

Inductive Case We w.t.s.

$$\sum_{k=0}^{n} x^k = \frac{x^{n+1} - 1}{x - 1}$$

Therefore, we have

$$\begin{aligned}
\sum_{k=0}^{n} x^k &= \sum_{k=0}^{n-1} x^k + x^n \\
&= \frac{x^n - 1}{x - 1} + x^n \\
&= \frac{x^n - 1 + (x-1)x^n}{x - 1} \\
&= \frac{x^n - 1 + x^{n+1} - x^n}{x - 1} \\
&= \frac{x^{n+1} - 1}{x - 1}
\end{aligned}$$

□

4.1.2 Variation of Mathematical Induction

Theorem 1.2

Suppose $P(n)$ is a variable proposition, $n_0 \in \mathbb{Z}$, let $S = \{n_0, n_0 + 1, n_0 + 2, \cdots\}$

If $P(n)$ holds and $(\forall (n \in S))(P(n) \implies P(n+1))$

Then we can say that $(\forall (n \in S))P(n)$ holds.

Example. *For which $n \in \mathbb{N}$ do we have $n! > 2^n$?*

Proof. **Base Case** - If $n = 4$

$$2^4 = 16 < 24 = 4!$$

Induction Hypothesis Fix $n \in \mathbb{N}$ is an element where $n \geq 4$. Assume we have

$$n! > 2^n$$

Inductive Case We w.t.s.

$$(n+1)! > 2^{n+1}$$

$$(n+1)! = n! \cdot (n+1)$$

Since $n \geq 4$, we have $n + 1 > 2$. By assumption, we have $n! > 2^n$. Therefore, we have

$$n! \cdot (n+1) > 2^{n+1} \iff (n+1)! > 2^{n+1}$$

□

4.1.3 Induction with Jumps

Sometimes we want to prove $P(n)$, not for all $n \in \mathbb{N}$, but for even n / odd n / etc.

Theorem 1.3: Induction with Jumps

Let $P(n)$ be the variable proposition. Fix $n_0 \in \mathbb{Z}$ as a starting point, step size $k \in \mathbb{N}$. Define S as

$$S = \{n_0, n_0 + k, n_0 + 2k, \cdots\}$$

1. If $P(n_0)$ is true
2. And we have $(\forall n \in \S)(P(n) \implies P(n+k))$

Then we have $(\forall n \in S)(P(n))$ is true.

> **Example.** *Consider the alternating sum of the first n squares*
>
> $$1^2 - 2^2 + 3^2 - 4^2 + \cdots + (-1)^{n+1} n^2$$
>
> *Prove that*
>
> - *for all odd n, we have*
>
> $$\sum_{k=1}^{n} (-1)^{k-1} k^2 = \sum_{k=1}^{n} k$$
>
> - *for all even n, we have*
>
> $$\sum_{k=1}^{n} (-1)^{k-1} k^2 = -\sum_{k=1}^{n} k$$

Proof.

- For odd n

  Here $n_0 = 1$, $jump = 2$, so that $S = \{1, 3, 5, 7, \cdots\}$

$P(n)$ is

$$\sum_{k=1}^{n}(-1)^{k-1}k^2 = \sum_{k=1}^{n}k$$

BC If $n = 1$, then we have

$$1^2 = 1$$

So $P(1)$ is true.

IH Fix $n \in S$, assume that we have identity

$$\sum_{k=1}^{n}(-1)^{k-1}k^2 = \sum_{k=1}^{n}k$$

IS We want to show that the same identity ($P(n+2)$) holds.

$$\begin{aligned}
\sum_{k=1}^{n+1}(-1)^{k-1}k^2 &= \sum_{k=1}^{n}(-1)^{k-1}k^2 - (n+1)^2 + (n+2)^2 \\
&= \sum_{k=1}^{n}k - ((n+1)+(n+2))((n+1)-(n+2)) \\
&= \sum_{k=1}^{n}k - (-1)((n+1)+(n+2)) \\
&= \sum_{k=1}^{n}k + (n+1) + (n+2) \\
&= \sum_{k=1}^{n+2}k
\end{aligned}$$

- For even n

  Here $n_0 = 2$, $jump = 2$, so that $S = \{2, 4, 6, 8 \cdots\}$

  $P(n)$ here is

  $$\sum_{k=1}^{n}(-1)^{k-1}k^2 = -\sum_{k=1}^{n}k$$

  detailed proof here are omitted ...

□

4.2 Induction Proof (Strong)

In certain proofs, we may need to assume more than $P(n)$ to prove $P(n+1)$.

We may need to assume $P(n), P(n-1), \cdots, P(1)$ to prove $P(n+1)$.

Theorem 2.1: Principle of Strong Mathematical Induction (PSMI)

Suppose $P(n)$ is a variable proposition.

If

1. $P(1)$ holds
2. $(\forall n \in \mathbb{N})\left((\forall n \in [n])P(n) \implies P(n+1)\right)$

Then $(\forall n \in \mathbb{N})P(n)$ holds.

Template for PSMI proof

Proof.

Base Case Prove $P(1)$

Strong Induction Hypothesis Fix $n \in \mathbb{N}$. Assume $(\forall k \in [n])(P(k))$ is true.

Inductie Step Based on this assumption, prove $P(n+1)$ □

Example. *Let S_n ba the sequence defined by*

$$\begin{cases} S_0 = 1 \\ S_n = 1 + \sum_{k=0}^{n-1} S_n \end{cases}$$

Proposition. $(\forall n \in \mathbb{N} \cup \{0\})$, we have $S_n = 2^n$

Proof.

Base Case If $n = 0$, we have $S_0 = 1 = 2^0$

Strong Induction Hypothesis Fix $n \in \mathbb{N}$, assume $(\forall k \in [n])(S_k = 2^k)$

Inductive Step Based on the assumption made in Strong IH, we have

$$\begin{aligned} S_{n+1} &= 1 + \sum_{k=0}^{n} S_k \\ &= 1 + \sum_{k=0}^{n} 2^k \\ &= 1 + (2^{n+1} - 1) \\ &= 2^{n+1} \end{aligned}$$

□

Definition (Prime Factorization). A prime factorization of a given $n \in \mathbb{N}\backslash\{1\}$ is a way of writing n as a product of primes.

Proposition. $\forall n \in \mathbb{N}\backslash\{1\}$, n has a prime factorization.

Proof.

Base Case When $n = 2$, we have $n = 2$ itself as a prime factorization.

Strong Inductive Hypothesis Fix $n \in \mathbb{N}\backslash\{1\}$, assume $(\forall k \in [n]\backslash\{1\})$, k has a prime factorization.

Induction Step

Case 1 If $n+1$ is prime, then $n+1 = n+1$ itself is the prime factorization

Case 2 Otherwise, $n+1 = a \cdot b$ where $a, b < n+1$. By assumption of Induction Hypothesis, we can know that a, b have prime factorization.

Suppose without lose of generality, $a = p_1 p_2 \cdots p_n$ and $b = q_1 q_2 \cdots q_n$ are the prime factorization of a and b.

Then $n+1 = p_1 p_2 \cdots p_n \cdot q_1 q_2 \cdots q_n$ is the prime factorization of $n+1$.

□

Notes. In some situation, we need to have Multiple Base Cases

Example. *Define a sequence X_n by*

$$\begin{cases} X_1 = 2 \\ X_2 = 3 \\ X_n = 3X_{n-1} - 2X_{n-2} \quad \textit{for } n \geq 3 \end{cases}$$

Proposition. For all $n \in \mathbb{N}$, we have $X_n = 2^{n-1} + 1$

Proof.

Base Case

- If $n = 1$, we have $X_1 = 2 = 2^{1-1} + 1$
- If $n = 2$, we have $X_2 = 3 = 2^{2-1} + 1$

Inductive Hypothesis Fix $n \geq 2$, assume $\forall k \in [n]$, we have $X_k = 2^{k-1} + 1$

Inductive Step

$$\begin{aligned} X_{n+1} &= 3X_n - 2X_{n-2} \\ &= 3 \cdot (2^{n-1} + 1) - 2 \cdot (2^{n-2} + 1) \\ &= (2^{n-1} + 1) + 2^n + 2 - 2^{n-1} - 2 \\ &= 2^n + 1 \end{aligned}$$

□

Chapter 5

Binary Relationship

5.1 Binary Relationship

Definition (Binary Relation). Suppose A, B are sets. A binary relationship on A and B is simply a subset of the Cartesian product $A \times B$.

$$R \subseteq A \times B$$

Definition (Related). If $(a, b) \in R$, we say that "a is related to b". Sometimes, we write $a \ R \ b$.

We say A is the **domain** of R, B is the **codomain** of R.

If we have $R \subseteq A \times A$, then we say R is a relation on A.

> **Example.** *Let A represent the set of Shakespeare's characters. B represents the set of his play.*
>
> *If we define $R \subseteq A \times B$ by $(a, b) \in R$ iff a appears in b.*
>
> *Then $(Romeo, `RomeoandJuliet') \in R$*

> **Example ($<$ and $\leq$ as Relation).** *Consider $\leq$ and $<$ as relations on $\mathbb{N}$, then we have*
>
> $$\leq = \{(a, b) \in \mathbb{N} \times \mathbb{N} \mid a \text{ is less than or equal to } b\}$$
>
> $$< = \{(a, b) \in \mathbb{N} \times \mathbb{N} \mid a \text{ is strictly less than } b\}$$

> *Notes.* Relations are arbitrary sets of pairs, and need not be defined by some intelligible properties.

5.1.1 Four Basic Properties of Relations

Suppose A is a set and $R \subseteq A \times A$ is a relation on A.

Definition (Reflexive). R is reflexive if and only if

$$(\forall x \in A)(x, x) \in R$$

Definition (Symmetric). R is symmetric if and only if

$$(\forall x, y \in A)((x, y) \in R \implies (y, x) \in R)$$

Definition (Transitive). R is transitive if and only if

$$(\forall x, y, z \in A)\,((x, y) \in R \wedge (y, z) \in R) \implies (x, z) \in R$$

Definition (Antisymmetric). R is Antisymmetric if and only if

$$(\forall x, y \in A)((x, y) \in R \wedge (y, x) \in R) \implies x = y$$

Example. *On any set A, the equality relation is **reflexive, symmetric, transitive**. If a relation has these three properties, then it is called the **equivalence relation**.*

Operator	$=$	$\leq$	$<$
Reflexive	✓	✓	
Symmetric	✓		
Transitive	✓	✓	✓
Antisymmetric	✓	✓	✓

Example. *Consider the divisibility relation $\mid$ on $\mathbb{N}$*

$$n \mid m \quad \textit{iff} \quad (\exists k \in \mathbb{N})(m = nk)$$

Then we will have

Operator	$\mid$ on $\mathbb{N}$
Reflexive	✓
Symmetric	
Transitive	✓
Antisymmetric	✓

Proof. Fix $n, m, l \in \mathbb{N}$.

1. Then $n \mid n$ since $n = n \times 1$ - therefore, $\mid$ is reflexive
2. Consider $2 \mid 4$ is true, but $4 \mid 2$ is false - therefore, $\mid$ is not symmetric
3. Consider $n \mid m$ and $m \mid l$, then we have

   $$(\exists k_1 \in \mathbb{N})m = k_1 \cdot n, \quad (\exists k_2 \in \mathbb{N})l = k_2 \cdot m$$

   then we have

   $$l = k_1 \cdot k_2 \cdot n$$

   therefore, $n \mid l$, and we have proved that $\mid$ is transitive.
4. Suppose we have $n \mid m$ and $m \mid n$, we w.t.s. $m = n$

   $$(\exists k_1, k_2 \in \mathbb{N})n = k_1 \cdot m, \quad m = k_2 \cdot n$$

   therefore, we have

   $$m = k_1 \cdot k_2 \cdot m$$

   Since $k_1, k_2 \in \mathbb{N}$, we have $k_1 = k_2 = 1$. Therefore, we have $m = n$ and therefore $\mid$ is antisymmetric.

□

5.2 Equivalence Relation

Definition (Equivalence Relation). Given a relation R on A, we say R is an equivalence relation if R is **reflexive, symmetric, transitive**.

Definition (Equivalence Class). Suppose $R \subseteq A \times A$ s an equivalence relation on A. Given $x \in A$, the equivalence class of x is

$$[x]_R = \{y \in A \mid (x, y) \in R\}$$

> **Example.** *Define a relation R on $\mathbb{R}$ ($R \subseteq \mathbb{R} \times \mathbb{R}$) such that*
>
> $$(x, y) \in R \text{ iff } \lfloor x \rfloor = \lfloor y \rfloor$$
>
> *Prove that R is an equivalence relation*

Solution.

1. **[Reflexive]** Fix $x \in \mathbb{R}$, we have $\lfloor x \rfloor = \lfloor x \rfloor$.

   Hence, $(x, x) \in R$ and we can know that R is reflexive.

2. **[Symmetric]** Fix $x, y \in \mathbb{R}$, such that we have $\lfloor x \rfloor = \lfloor y \rfloor$

   Hence, $(x, y) \in R$.

   Since $(\lfloor x \rfloor = \lfloor y \rfloor) \iff (\lfloor y \rfloor = \lfloor x \rfloor)$, we can know that $(y, x) \in R$.

   Hence, R is Symmetric

3. **[Transitive]** Fix $x, y, z \in \mathbb{R}$, such that $(x, y) \in R$ and $(y, z) \in R$

   Hence, we have $\lfloor x \rfloor = \lfloor y \rfloor$ and $\lfloor y \rfloor = \lfloor z \rfloor$

   Due to the transitivity of equal relation, we have $\lfloor x \rfloor = \lfloor z \rfloor$

   Therefore, $(x, z) \in R$ and R is Transitive.

$\rightarrow$ *End of Solution*

> *Notes.* In this course, we use $[n]$ to denote the first n natural number (without zero). This has noting to do with equivalence class.

> **Example.** *Equivalence class of floor operation: Prove that*
>
> $$\lfloor x \rfloor = n \implies [x]_{\lfloor\rfloor} = [n, n + 1)$$

Solution.

$$\begin{aligned}
[x]_{\lfloor\rfloor} &= \{y \in \mathbb{R} \mid (x, y) \in R\} \\
&= \{y \in \mathbb{R} \mid \lfloor x \rfloor = \lfloor y \rfloor\} \\
&= \{y \in \mathbb{R} \mid \lfloor y \rfloor = n\} \\
&= \{y \in \mathbb{R} \mid y \in [n, n + 1)\} \\
&= [n, n + 1)
\end{aligned}$$

$\rightarrow$ *End of Solution*

Notes. For some arbitrary equivalence relation R defined on A, the equivalence classes of R will **always partition the set** A.

That is, every element of A will be in one and only one equivalence class.

If R represents an equivalence relation defined on A. If $x, y \in A$ and $(x, y) \in R$, then we can know that

$$[x]_R = [y]_R$$

Notes (**Special Notation**).

$$n \equiv m \bmod k \iff n \equiv_k m$$
$$[n]_{\equiv_k} \iff [n]_k$$

Definition (Partition). Suppose A is a set, a partition P of A is a set of subsets of A such that

1. $\forall x \in P, x \neq \emptyset$ - Every piece of partition is not empty
2. $(\forall x, y \in P)(x \neq y) \implies (x \cap y = \emptyset)$ - Pieces of the partition are pairwise disjoint
3. $\bigcup_{x \in P} x = A$ - The union of all pieces of partition forms the entire set A

Example. *Let* $A = \{1, 2, 3, 4\} = [4]$. *Then*

$$P = \{\{1\}, \{2, 3, 4\}\}$$

is a valid partition of A.

Definition (Set of Equivalence Classes). Suppose R is an equivalence relation on A. We denote the set of equivalence classes by A/R.

$$A/R = \{[x]_R \mid x \in A\}$$

And we call this set of equivalence classes $A \mod R$

Example. *Consider the binary equivalence relation* $\equiv_3$ *on* $\mathbb{Z}$.

$$\mathbb{Z}/\equiv_3 = \{[n]_3 \mid n \in \mathbb{Z}\} = \{[0]_3, [1]_3, [2]_3\}$$

Notes (**More Special Notation ...**). To simplify the symbol, we use

$$\mathbb{Z}/n\mathbb{Z} \iff \mathbb{Z}/\equiv_n$$

in this course specifically.

Theorem 2.1

If R is an equivalence relation on some set A, then A/R is a partition of A.

- We can gain a partition of the set A through an equivalence relation
- We can also construct an equivalence relation through a part of set A

Theorem 2.2

Suppose P is a partition of A. Define R_p by:

$$(x, y) \in R_P \text{ iff } (\exists X \in P)(x \in X \wedge y \in X)$$

then R_P is an equivalence relationship.

Proof.

1. Show that R_P is reflexive
   - Fix $x \in A$
   - Since P is a partition, we have $\bigcup_{X \in P} X = A$
   - Hence $x \in \bigcup_{X \in P} X$, therefore $\exists X \in P$ s.t. $x \in X$
   - Hence $x \in X$ and $x \in X$
   - Hence by definition of R_P, we have $(x, x) \in R_P$
2. Show that R_P is symmetric
   - Fix $x, y \in A$, suppose $x, y \in R_P$
   - Therefore, $\exists X \in P$ s.t. $x \in X \wedge y \in X$
   - Therefore, $y \in X \wedge x \in X$
   - Hence $(y, x) \in R_P$ and R_P is symmetric
3. Show that R_P is transitive
   - Fix $x, y, z \in A$, suppose $(x, y) \in R_P$ and $(y, z) \in R_P$
   - $(\exists x \in P)(x \in X \wedge y \in X)$ and $(\exists Y \in P)(y \in Y \wedge z \in Y)$
   - Therefore, $X \cap Y \neq \emptyset$. By definition of partition, we can know that $X = Y$
   - Hence $x, z \in X$ and $(x, z) \in R_P$
   - Therefore, R_P is transitive

□

5.3 Order Relation

Unlike equivalence relation, order relations come in several flavers.

	Partial	Total
Non-strict	Non-strict Partial Order	Non-strict Total Order
Strict	Strict Partial Order	Strict Total Order

5.3.1 Nonstrict Partial Order

Definition (Nonstrict Partial Order). A relation R on A is a nonstrict partial order if and only if R is

- Reflexive

- Transitive
- Antisymmetric

Definition (Partially Ordered Set (Poset)). If R is a partial order relation on A, we say (A, R) is a partially ordered set (abbr. as *poset*)

> **Example ($\leq$ on $\mathbb{R}$).** *$\leq$ is a partial order on $\mathbb{R}$, since we have*
>
> - $x \leq x$
> - $x \leq y \land y \leq z \implies x \leq z$
> - $x \leq y \land y \leq x \implies x = y$

> **Example ($\subseteq$ on $\mathcal{P}(A)$).** *For a fixed set A, $\subseteq$ is a partial order on $\mathcal{P}(A)$, since for any $x, y, z \in \mathcal{P}(A)$, we have*
>
> - $x \subseteq x$
> - $x \subseteq y \land y \subseteq z \implies x \subseteq z$
> - $x \subseteq y \land y \subseteq x \implies x = y$

Definition (Irreflexive). A relation R is irreflexive if

$$\forall x \in A, (x, x) \notin R$$

Definition (Asymmetric). A relation R is Asymmetric if

$$(\forall x, y \in A)((x, y) \in R \implies (y, x) \notin R)$$

> *Notes.* Asymmetric is not the same as Antisymmetric

5.3.2 Strict Partial Order

Definition (Strict Partial Order). A relation R on A is a strict partial order if and only if R is

- **Irreflexive**
- Transitive
- Antisymmetric

equivalently, the conditions above can also be simplified to

- Transitive
- Asymmetric

> **Example ($<$ on $\mathbb{R}$).** *$<$ is a strict partial order on $\mathbb{R}$, since we have*
>
> - $x \not< x$
> - $x < y \land y < z \implies x < z$
> - $(x < y \land y < x) \implies x = y$ *(vacuously true)*

Notes. In general, R can't be both strict and non-strict partial order. (unless $R = \emptyset$)

5.3.3 Total Orders

Definition (Totality). A relation R on A is total if and only if

$$(\forall x, y \in A)((x, y) \in R \vee (y, x) \in R \vee (x = y))$$

Definition (Strict Total Order). If R is a non-strict partial order that is also total then R is a total order

If R is a strict partial order that is total, then R is a strict total order.

Example. *$\leq$ is a total order on $\mathbb{R}$ since we know that $\leq$ is a partial order and is total since*

$$(\forall x, y \in R)(x \leq y \vee y \leq x \vee x = y)$$

Chapter 6

Functions

6.1 Function

6.1.1 Definition of Function

We can formalize the definition of function as a special kind of binary relations (a set of ordered pairs).

Definition (Function). A function (with domain A and codomain B) is a relation $f \subseteq A \times B$ such that

$$(\forall a \in A)(\exists b \in B)[(a,b) \in f \wedge (\forall c \in B)((a,c) \in f \implies (c = b))]$$

For every $a \in A$, there exists a unique $b \in B$ such that $(a,b) \in f$.

> *Notes* (Notation). We write $f : A \to B$ to mean that a relation $f \subseteq A \times B$ that is a function.
>
> Also, $f(a) = b$ is an abbreviation to mean that $(a,b) \in f$

However, the definition of function above does **NOT** mean...

- for every $b \in B$ there is an $a \in A$ s.t. $f(a) = b$ - Function with this property is **Surjective**
- for every distinct $a, a' \in A$, there must have distinct result b, b' - Function with this property is **Injective**

> **Example.** *Let $f(x) = x^2$, the function f is in fact a mathematical object defined as*
>
> $$f = \{(x,y) \in \mathbb{R} \times \mathbb{R} \mid y = x^2\}$$

> *Notes.* Rules that depend on how input is represented **does not** always yield well-defined functions.

> **Example (Ill-defined Function).**
>
> $$f : \mathbb{Q} \to \mathbb{Z}, \quad \textit{where } f(\frac{m}{n}) = m + n$$
>
> *Under this definition, we have*
>
> $$f\left(\frac{1}{2}\right) = 1 + 2 = 3 \quad f\left(\frac{2}{4}\right) = 2 + 4 = 6$$
>
> *However, since we have $\frac{1}{2} = \frac{2}{4}$, we have $\frac{1}{2}$ having two different results, which violates the definition of*

> *function.*

6.1.2 Equality of Functions

Definition (Equality of Functions). $f = g$ if and only if f, g are equal as sets (of ordered pairs). That is, $f \subseteq g$ and $g \subseteq f$

In practice, it's often to use the following criterion to prove function equality:

Proposition. $f : A \to B$ and $g : A \to B'$ are equal if and only if

$$(\forall a \in A)(f(a) = g(a))$$

6.1.3 Images of Function

Definition (Image). Suppose $f : A \to B$ is a function and $X \subseteq A$. The image of X under f, denoted as $\mathrm{Im}_f(X)$ is defined as

$$\mathrm{Im}_f(X) = \{y \in B \mid (\exists x \in X)(f(x) = y)\}$$

> *Notes* (Notation). When $X = A$, we say $\mathrm{Im}_f(A)$ is the image of f and write Im_f as an abbreviation

Proposition. Suppose $f : A \to B$ is a function and $S, T \subseteq A$, then

$$\mathrm{Im}_f(S \cap T) \subseteq \mathrm{Im}_f(S) \cap \mathrm{Im}_f(T)$$

Proof.

- Fix $y \in Im_f(S \cap T)$ to be an arbitrary element of $\mathrm{Im}_f(S \cap T)$
- $\exists x \in S \cap T$ such that $f(x) = y$
- $x \in S$ and $x \in T$
- Therefore, $f(x) \in \mathrm{Im}_f(S)$ and $f(x) \in \mathrm{Im}_f(T)$
- Therefore, we have $y \in \mathrm{Im}_f(S) \wedge y \in \mathrm{Im}_f(T)$
- Therefore, we have $y \in \mathrm{Im}_f(S) \cap \mathrm{Im}_f(T)$

□

> *Notes.* However, the converse of this proposition is not always true, that is $\mathrm{Im}_f(S \cap T)$ is not always equal to $\mathrm{Im}_f(S) \cap \mathrm{Im}_f(T)$.
>
> > *Example.* $S = \{-1, 0\}$ *and* $T = \{0, 1, 2\}$ *where* $f : \mathbb{R} \to \mathbb{R}$ *is defined as* $f(x) = x^2$.
> >
> > *In this case,* $\mathrm{Im}_f(S) \cap \mathrm{Im}_f(T) = \{0, 1\}$ *while* $\mathrm{Im}_f(S \cap T) = \{0\}$

6.1.4 Inverse Image (Preimage)

Definition (Preimage). Suppose $f : A \to B$ is a function and $Y \subseteq B$. The preimage of Y under f, denoted as $\mathrm{PreIm}_f(y)$ is defined as

$$\mathrm{PreIm}_f(Y) = \{x \in A \mid f(x) \in Y\}$$

We always have

$$\text{PreIm}_f(B) = A \quad \text{for } f : A \to B$$

Proposition. Given $f : A \to B$. Fix $X \subseteq A$, then $\text{PreIm}_f(\text{Im}_f(X)) \supseteq X$

Proof. Fix $x \in X$

- By definition of f, we have $f(x) \in \text{Im}_f(X)$
- Since $\text{PreIm}_f(\text{Im}_f(X)) = \{z \in A \mid f(z) \in \text{Im}_f(X)\}$
- Hence $x \in \text{PreIm}_f(\text{Im}_f(X))$
- Hence $X \subseteq \text{PreIm}_f(\text{Im}_f(X))$

□

Proposition. Given $f : A \to B$. Fix $Y \subseteq B$, then $\text{Im}_f(\text{PreIm}_f(Y)) \subseteq Y$

Proof. Fix $y \in \text{Im}_f(\text{PreIm}_f(Y))$

- Hence $\exists x \in \text{PreIm}_f(Y)$ such that $f(x) = y$
- Then $f(x) \in Y$
- Therefore, $y \in Y$

□

6.1.5 Injections, Surjections& Bijections

Definition (Surjective). A function $f : X \to Y$ is surjective (or, a surjection) if and only if

$$\text{Im}_f(X) = Y$$

that is,

$$(\forall y \in Y)(\exists x \in X)(f(x) = y)$$

Definition (Injective). A function $f : X \to Y$ is injective (or, an injection) if and only if

$$(\forall x, y \in X)(f(x) = f(y) \implies x = y)$$

An equivalence of this will be

$$(\forall x, y \in X)(x \neq y \implies f(x) \neq f(y))$$

> **Example.** *Let $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ be a function defined by $f((m, n)) = m + n$. Prove that f is surjective*

Proof. Want to show $(\forall x \in \mathbb{Z})(\exists (m, n) \in \mathbb{Z} \times \mathbb{Z})(f(m, n) = x)$

- let x be an arbitrary element of $\mathbb{Z}$
- We always have $f((0, x)) = 0 + x = x$
- Therefore, there $\exists (m, n) \in \mathbb{Z} \times \mathbb{Z}$ s.t. $f(m, n) = x$
- Therefore, f is surjective.

□

Proving Injectivity - The approaches: Fix x, y in domain and than

1. Assume $f(x) = f(y)$, prove $x = y$
2. Assume $x \neq y$, prove $f(x) \neq f(y)$

> **Example.** *Define $f : \mathbb{N} \to \mathbb{N}$, by $f(n) = n^2$. Claim: f is an injective function*

Proof. Fix $n, m \in \mathbb{N}$, suppose $n \neq m$ and either $n < m$ or $m < n$.

If $n < m$, since both n, m are positive, we can square on both sides and having $n^2 < m^2$.

Therefore, we have $f(n) < f(m)$, which indicates that $f(n) \neq f(m)$. □

6.1.6 Compositions

Definition (Composition). Suppose we have two functions $f : A \to B$ and $g : B \to C$. The composition of g and f, written as $g \circ f$ is defined as

$$g \circ f(x) = g(f(x))$$

where $g \circ f : A \to C$

Definition (Identity Function). We denote the identity function defined on A as Id_A.

$$(\forall a \in A)(Id_A(a) = a)$$

Definition (Inverse Function). A function $f : A \to B$ is invertible if and only if there exists some function $g : B \to A$ such that

$$(\forall x \in A) g(f(x)) = x = Id_A(x)$$

$$(\forall y \in B) f(g(y)) = y = Id_B(y)$$

> *Notes.* Not all functions are invertible. (When f is not injective, then f^{-1} is not a well-defined function)

Theorem 1.1: Invertibility of Function

$f : A \to B$ is invertible if and only if f is a bijective function.

Proof.

($\Longrightarrow$) Suppose f is invertible, let $g = f^{-1}$, we want to show that f is a bijective function.

1. We want to show that f is surjective, that is

$$(\forall b \in B)(\exists a \in A) s.t. f(a) = b$$

   - Let b be an arbitrary element of B
   - Since f is invertible, $\exists a \in A$ s.t. $g(b) = a$.
   - Hence we have $f(a) = f(g(b)) = b$ by definition of inverse function.
   - Hence $\exists a \in A$ such that $f(a) = b \, \forall b \in B$
   - Therefore, we can conclude that f is surjective.

2. We want to show that f is injective, that is

$$(\forall a, a' \in A)(f(a) = f(a')) \implies (a = a')$$

   - Let $a, a' \in A$ be two arbitrary elements of A, suppose $f(a) = f(a')$
   - Then $g(f(a)) = g(f(a'))$ by definition of function
   - Hence $a = a'$ by definition of inverse function.
   - Therefore, we can conclude that f is injective

Since f is both injective and surjective, we can conclude that f is bijective.

($\Longleftarrow$) Suppose f is a bijective function, we want to show that f is invertible.

- Let $g = \{(b, a) \in B \times A \mid (a, b) \in f\}$, then g is a binary relation defined on $B \times A$.
- We want to show that g is a function. That is

$$(\forall b \in B)(\exists \text{ unique } a \in A) s.t. (b, a) \in g$$

  - Let $b \in B$ be an arbitrary element of B
  - $\exists a \in A$ such that $f(a) = b$ by the surjectivity of f.
  - Therefore, $(\forall b \in B)(\exists a \in A)$ such that $(b, a) \in g$.
  - Suppose there is some other $a' \in A$ such that $f(a') = b$, by the injectivity of f, we have $f(a) = f(a') = b$ indicates $a = a'$.
  - Therefore, $(b, a) = (b, a')$ and there is only one unique $a \in A$ such that $(b, a) \in g$.
- We want to show that g is the inverse of f.

  First, we have $g \circ f(a) = a$

  - Let $a \in A$ be an arbitrary element of A
  - Then $b = f(a)$, then $(a, b) \in f$.
  - Hence $(b, a) \in g$, that is, $g(b) = a$.
  - Hence $g(f(a)) = g(b) = a$

  Second, we have $f \circ g(a) = a$

  - Let $b \in B$ be an arbitrary element of B
  - Then let $a = g(b)$, so $(b, a) \in g$
  - Hence $(a, b) \in f$, by definition of g
  - Hence $f(g(b)) = f(a) = b$

□

Chapter 7

Cardinality and Infinity

7.1 Set Theory Introduction (Infinity)

7.1.1 Cardinality

> **Example (Bijection and cardinality).**
>
> *When we say there are 3 elements in set $\{\heartsuit, \star, \triangle\}$, we are 'counting' the elements in this set.*
>
> *From a perspective of mathematics, we are in fact building a bijective relationship between the set $\{1, 2, 3\}$ when we are 'counting'.*

Generalizing this, we will say two sets have the same size (cardinality) if and only if there exists a bijection between them.

Definition (Cardinality). Two sets A, B have the same cardinality if and only if there is a bijection $f : A \to B$. We denote the cardinality of A as $|A|$.

In this case, we write $A \sim B$ or $|A| = |B|$

Proposition (Reflexive). For any set A, we have $A \sim A$ since $Id_A : A \to A$ is a trivial bijection.

Proposition (Symmetric). If $A \sim B$, then $\exists f : A \to B$ a bijection. Hence $B \sim A$ since f^{-1} is a bijective function $B \to A$.

Proposition (Transitive). If $A \sim B$ and $B \sim C$, then $A \sim C$.

Therefore, $\sim$ is an equivalence relation.

> **Example.** *Let $\mathbb{N}$ be a set of all natural number and E be a set of all even numbers. Which set is bigger, or, if they have the same size?*

Solution. Since there exists a bijection $f : \mathbb{N} \to E$ where $f(n) = 2n$, by definition of cardinality, we have $\mathbb{N} \sim E$.

$\to$ *End of Solution*

> *Notes.* When dealing with infinite sets, it is possible to have A as a **strict subset** of B, yet $A \sim B$.

Definition ($\lesssim$ and $\gtrsim$).

Let A, B be two arbitrary sets, then we say $A \lesssim B$ if there is an injection $f : A \to B$.

Let A, B be two arbitrary sets, then we say $A \gtrsim B$ if there exists a surjection $f : A \to B$.

Notes. When we are saying $A \lesssim B$, we don't mean $B \gtrsim A$. They have very different meaning (though they are logically equivalent).

Theorem 1.1

For set A, B, we have $(A \lesssim B) \iff (B \gtrsim A)$

That is, there exists an injection $f : A \to B$ if and only if there exists a surjection $g : B \to A$.

Proof.

($\implies$) Suppose there is an injection $f : A \to B$, define $g : B \to A$, we want to show that g is surjective.

- Given $b \in B$ an arbitrary element of B
- If $\exists a \in A$ such that $f(a) = b$, then a is unique since f is injection between A and B.
- Else $\neg(\exists a \in A)(f(a) = b)$, then we define $g(b) = a_0$.
- Then g is a function since for every input of $b \in B$, there is an output $g(b) \in A$ and that output is unique.
- Therefore, g is a surjection since $\forall a \in A$, if $b = f(a)$, then $g(b) = a$.

($\impliedby$) Suppose there exists a surjection $g : B \to A$, define $f : A \to B$, we want to show that f is an injection.

- Given $a \in A$, then $\mathrm{PreIm}_g(\{a\}) \neq \emptyset$ since g is surjective.
- Let b be some arbitrary element of $\mathrm{PreIm}_g(\{a\})$, define $f(a) = b$
- Than f is a function since for every $a \in A$, there exists some unique $b \in \mathrm{PreIm}_g(\{a\})$ such that $f(a) = b$
- f is injective since g is a function.

□

7.1.2 Properties of $\lesssim$ and $\gtrsim$

Given A, B, C, we have

[Reflexive]

$$A \lesssim A \text{ and } A \gtrsim A$$

Since $Id_A : A \to A$ is an injection and a surjection.

[Transitive] If we have $A \lesssim B$ and $B \lesssim C$, then we have $A \lesssim C$.

Theorem 1.2: CBS Theorem

A, B are two sets and there

$$\exists \text{ injection } f : A \to B$$
$$\exists \text{ injection } g : B \to A$$

Then we can conclude that there must exist a bijection between $A \to B$. That is, we have $A \sim B$ (or $|A| = |B|$).

> **Example.** *Prove that* $|(0,1)| = |(0,1]|$ *using the CBS theorem.*

Solution. Let $f : (0,1) \to (0,1]$ be defined as $f(n) = n$, then we have f an injection.

For all $x_1, x_2 \in (0,1)$ such that $x_1 \neq x_2$, we must have $f(x_1) \neq f(x_2)$, so f is injective.

Let $g : (0,1] \to (0,1)$ be defined as $g(n) = \frac{1}{2}n$, then we have g an injection.

For all $x_1, x_2 \in (0,1]$ such that $x_1 \neq x_2$, we must have $\left(g(x_1) = \frac{x_1}{2}\right) \neq \left(\frac{x_2}{2} = g(x_2)\right)$. Hence, g is also injective.

By CBS, there must exist a bijection between $(0,1)$ and $(0,1]$. Therefore, $(0,1) \sim (0,1]$.

$\to$ *End of Solution*

7.2 Countable / Uncountable

Definition (Countable Set). X is countable if $\mathbb{N} \sim X$. (i.e. There exists a bijection $f : \mathbb{N} \to X$)

> **Example.** *Prove* $\mathbb{N} \times \mathbb{N}$ *is countable*

Solution (Informal). Since we can count every tuple $\mathbb{N} \times \mathbb{N}$ through a fixed pattern, we can say that there exists $f : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ a bijection.

Therefore, we can conclude that $\mathbb{N} \times \mathbb{N}$ is countable.

$\to$ *End of Solution*

Solution (Formal). Let $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ be defined as

$$f(m,k) = 2^{m-1}(2k-1) \qquad \text{(Pairing Function)}$$

$\to$ *End of Solution*

Theorem 2.1

If A, B is countable, then $A \times B$ is also countable.

Proof. Suppose A, B are countable, then there exists bijections $f : \mathbb{N} \to A$, $g : \mathbb{N} \to B$.

Therefore, we have $\mathbb{N} \times \mathbb{N} \sim A \times B$ since $F(n,m) = (f(n), g(m))$ is a bijection between $\mathbb{N} \times \mathbb{N}$ and $A \times B$.

Since $\mathbb{N} \sim \mathbb{N} \times \mathbb{N}$, by the transitivity of $\sim$, we can know that $A \times B \sim \mathbb{N}$.

Hence, $A \times B$ is countable. □

> **Example.** *Prove* $\mathbb{Q}$ *is countable*

Solution. We will prove

$$\mathbb{N} \lesssim \mathbb{Q} \lesssim \mathbb{Z} \times \mathbb{N} \lesssim \mathbb{N}$$

By transitivity, we have $\mathbb{N} \lesssim \mathbb{Q}$ and $\mathbb{Q} \lesssim \mathbb{N}$, we have $\mathbb{Q} \sim \mathbb{N}$.

$\mathbb{N} \lesssim \mathbb{Q}$ Since we have $f : \mathbb{N} \to \mathbb{Q}$ defined as $f(n) = n$ an injection, we can have $\mathbb{N} \lesssim \mathbb{Q}$

$\mathbb{Z} \times \mathbb{N} \lesssim \mathbb{N}$ Since there is a bijection between $\mathbb{Z}$ and $\mathbb{N}$, we have $\mathbb{Z} \times \mathbb{N} \sim \mathbb{N} \times \mathbb{N}$. Since $\mathbb{N} \times \mathbb{N} \sim \mathbb{N}$, by the transitivity of $\sim$, we have $\mathbb{Z} \times \mathbb{N} \sim \mathbb{N}$. Hence, we have $\mathbb{Z} \times \mathbb{N} \lesssim \mathbb{N}$.

$\mathbb{Q} \lesssim \mathbb{Z} \times \mathbb{N}$ Let $f(m,n) = \frac{m}{n}$ be a function $\mathbb{Z} \times \mathbb{N} \to \mathbb{Q}$. Given any $q \in \mathbb{Q}$, we always have $(m,n) \in \mathbb{Z} \times \mathbb{N}$ such that $F(m,n) = q$.

Hence, we have $\mathbb{Q} \lesssim \mathbb{Z} \times \mathbb{N}$.

$\to$ *End of Solution*

Theorem 2.2: Cantor

$\mathbb{N} < \mathcal{P}(\mathbb{N})$, that is $\mathbb{N} \lesssim \mathcal{P}(\mathbb{N}) \wedge \mathbb{N} \not\sim \mathcal{P}(\mathbb{N})$.

And its general form:

Let A be some arbitrary set, we always have $A < \mathcal{P}(A)$.

Proof. Let $f(n) = [n]$, we can show that f is an injection between $\mathbb{N}$ and $\mathcal{P}(\mathbb{N})$. Therefore, we have $\mathbb{N} \lesssim \mathcal{P}(\mathbb{N})$.

Now we need to prove $\mathbb{N} \not\sim \mathcal{P}(\mathbb{N})$

Suppose $f : \mathbb{N} \to \mathcal{P}(\mathbb{N})$ is a surjection between $\mathbb{N}$ and $\mathcal{P}(\mathbb{N})$. Let some set T be defined as

$$T = \{n \in \mathbb{N} \mid n \notin f(n)\}$$

We now want to show that $\forall n \in \mathbb{N}$, we have $f(n) \neq T$.

Let n be a fixed element of $\mathbb{N}$, then we have

- If $n \in T$, then $n \notin f(n)$ by definition of T. Hence, $T \neq f(n)$
- If $n \notin T$, then $n \in f(n)$ by definition of T. Hence, $T \neq f(n)$

Since there exists some $T \in \mathcal{P}(\mathbb{N})$ such that $(\forall n \in \mathbb{N})(f(n) \neq T)$, we have proved that such bijection between $\mathbb{N}$ and $\mathcal{P}(\mathbb{N})$ does not exist. □

Proof. (General form)

Suppose there is a function $f : A \to \mathcal{P}(A)$, we can define a set F as

$$F = \{a \in A \mid a \notin f(a)\}$$

Since every element of F is in A, we have $F \in \mathcal{P}(A)$. Then there does not exist any $a \in A$ such that $f(a) = F$, f is not surjective.

Hence, we have $A < \mathcal{P}(A)$. □

Definition (Uncountable). An infinite set X is uncountable if $\mathbb{N} \not\sim X$ (or $\mathbb{N} < X$).

> **Example (Sets of Functions).** *Let* $B = \{f \subseteq \mathbb{N} \times \{0,1\} \mid f : \mathbb{N} \to \{0,1\}\}$
>
> *Proof that set* B *is uncountable.*

Solution. Suppose there exist a function $H : \mathbb{N} \to B$. We w.t.s. that H is not a surjection

Let $g : \mathbb{N} \to \{0,1\}$, defined as

$$g(n) = \begin{cases} 1 & H(n)(n) = 0 \\ 0 & H(n)(n) = 1 \end{cases}$$

Note: Since H is a mapping from natural number to element of B (another function), we can write $H(n)(n)$.

Since $\forall n \in \mathbb{N}$, we always have $g \neq H(n)$, we have proved that there exist some

$$(\exists g \in B)(\forall n \in \mathbb{N})(H(n) \neq g)$$

We have shown that H is not surjective.

Hence, we have $\mathbb{N} < B$, B is an uncountable set.

This technique is also called the '**diagonalization**', it is a convenient way to construct a new element that does not match any element of a countable sequence.

$\rightarrow$ *End of Solution*

Chapter 8

Number Theory

8.1 Number Theory

"The queen of Mathematics" – Gauss

8.1.1 Greatest Common Divisor

Definition (Prime & Composite Number). Fix $n \in \mathbb{N}$, $n > 1$

- n is a prime number if and only if its only positive divisors are n and 1.
- n is a composite number if and only if $\exists a, b \in \mathbb{N}$ and $1 < a, b < n$ where $ab = n$.

By strong induction, we can prove that any $n > 1$ can be written as a product of primes.

Theorem 1.1: Fundamental Theorem of Arithmetic

For any $n \in \mathbb{N}$, there exists and only exists a unique way to write n as the product of a series of primes.

Definition (Divisor). Given $m, n \in \mathbb{Z}$, we say m divides n (denoted as $m \mid n$) or m is a divisor of n if $\exists k \in \mathbb{Z}$ s.t. $n = km$.

By definition, we have $(\forall n \in \mathbb{Z})(n \mid 0)$

Definition (Greatest Common Divisor (gcd)). Given $m, n \in \mathbb{Z}$, if not both m, n are zero, the greatest common divisor of m, n, denoted as $\gcd(m, n)$ is the largest $k \in \mathbb{N}$ dividing both m, n.

Theorem 1.2

If you have two numbers $n, m \in \mathbb{Z}$ (not both 0) and let $d = \gcd(m, n)$, then we have

$$\gcd\left(\frac{m}{d}, \frac{n}{d}\right) = 1$$

Proof. Let $a = \gcd(\frac{m}{d}, \frac{n}{d})$, we w.t.s. $a = 1$.

- Since $\gcd$ by definition is greater than or equal to 1, we must have $a \geq 1$. Then we have $a \mid \frac{m}{d}$ and $a \mid \frac{n}{d}$.

- Then $\exists k, l \in \mathbb{Z}$ s.t. $\frac{m}{d} = ak$ and $\frac{n}{d} = al$.
- Which means that $m = (ad)k$ and $n = (ad)l$.
- Hence, ad is a common divisor of $\gcd(m, n)$. However, by definition, we can have d being the gcd of m and n
- However, since a and d are both greater than 1, we must have $ad \geq d$ while ad being a common divisor of m and n.
- Hence, the only situation that both ad and d is the greatest common divisor is that $a = 1$.

□

We can use the Euclid's Algorithm to calculate the gcd efficiently.

Theorem 1.3: Division Algorithm

Fix $b \in \mathbb{Z}$, and $a \in \mathbb{N}$, then there exists unique integers $q, r \in \mathbb{Z}$ s.t. $0 \leq r \leq a$ such that $b = aq + r$.

Proof. Define $S = \{n \in \{0\} \cup \mathbb{N} \mid (\exists k \in \mathbb{Z})(n = b - ak)\}$.

Observe: $S \neq \emptyset$ since $b - ak \geq 0$ whenever $b \geq ak$. Which is should exists for some $k \in \mathbb{Z}$.

Since $\mathbb{N} \cup \{0\}$ satisfy the WOP (well ordering principle), S has a least element, denoted as r.

Claim: We must have $r < a$

Proof. If $r \geq a$ then there must exists some r_1 s.t. $r = r_1 + a$.

But then we have

$$\begin{aligned} b &= aq + r \\ &= aq + a + r_1 \\ &= a(q + 1) + r_1 \\ \implies r_1 &= b - a(q + 1) \\ \implies r_1 &\in S \wedge r_1 < r \end{aligned}$$

Therefore, $\exists r_1 \in S$ s.t. $r_1 < r$, which contradicts our assumption that r is the least element in S. Therefore, we must have $r < a$.

□

Claim: The $r < a$ we have shown in S is the only element in S that is smaller than a.

Proof. Suppose $\exists q', r' \in \mathbb{Z}$ such that $0 \leq r' \leq a$ and $b = aq' + r'$. We w.t.s. $r = r'$ and $q = q'$

For r, r', there have either $r \geq r'$ or $r' \geq r$. Without lossing generality, suppose $r \geq r'$.

Then $r - r' \geq 0$

But $r - r' = (b - aq) - (b - aq') = aq' - aq$. Hence $a \mid (r - r')$. But we have $r - r' < a$ and $r - r' \geq 0$.

Hence, the only possible situation is $r - r' = 0$, where $r = r'$.

But then $b = aq + r = aq' + r' = aq' + r$. Hence $q = q'$

□

Therefore, we can conclude that there exists and only exists one pair of r, q s.t. $r \in [0, a)$ and $b = aq + r$.

□

Theorem 1.4: Bezart's Theorem

Fix $a, b \in \mathbb{Z}$ (not both 0) and let $d = \gcd(a, b)$.

Then $\exists m, n \in \mathbb{Z}$ s.t. $d = am + bn$ - d is the linear combination of a and b.

Moreover, d is least natural number than can be written as a linear combination of a and b.