基礎數學 MA-1015A

Chapter 1. Logic and Proofs

§1.1 Propositions and Connectives

§1.2 Conditionals and Biconditionals

§1.3 Quantified Statements

§1.4 Basic Proof Methods I

§1.5 Basic Proof Methods II

§1.6 Proofs Involving Quantifiers

§1.7 Strategies for Constructing Proofs

§1.8 Proofs from Number Theory

§1.1 Propositions and Connectives

Definition

A ***proposition*** is a sentence that has exactly one truth value. It is either true, which we denote by T, or false, which we denote by F.

Example

$7^2 > 60$ (F), $\pi > 3$ (T), Earth is the closest planet to the sun (F).

Example

The statement "the north Pacific right whale（露脊鯨）will be extinct species before the year 2525" has one truth value but it takes time to determine the truth value.

Example

That "Euclid was left-handed" is a statement that has one truth value but may never be known.

§1.1 Propositions and Connectives

Definition

A ***negation*** of a proposition P, denoted by $\sim\mathrm{P}$, is the proposition "not P". The proposition $\sim\mathrm{P}$ is $\begin{matrix}\text{true}\\ \text{false}\end{matrix}$ exactly when P is $\begin{matrix}\text{false}\\ \text{true}\end{matrix}$.

Definition

Given propositions P and Q, the $\begin{matrix}\textit{\textbf{conjunction}}\\ \textit{\textbf{disjunction}}\end{matrix}$ of P and Q, denoted by $\begin{matrix}\mathrm{P}\wedge\mathrm{Q}\\ \mathrm{P}\vee\mathrm{Q}\end{matrix}$, is the proposition "$\mathrm{P}$ $\begin{matrix}\text{and}\\ \text{or}\end{matrix}$ Q". $\begin{matrix}\mathrm{P}\wedge\mathrm{Q}\\ \mathrm{P}\vee\mathrm{Q}\end{matrix}$ is true exactly when $\begin{matrix}\text{both } \mathrm{P} \text{ and } \mathrm{Q} \text{ are true}\\ \text{at least one of } \mathrm{P} \text{ or } \mathrm{Q} \text{ is true}\end{matrix}$.

§1.1 Propositions and Connectives

Example

Now we analyze the sentence "either 7 is prime and 9 is even, or else 11 is not less than 3". Let P denote the sentence "7 is a prime", Q denote the sentence "9 is even", and R denote the sentence "11 is less than 3". Then the original sentence can be symbolized by $(\mathrm{P} \wedge \mathrm{Q}) \vee (\sim \mathrm{R})$, and the table of truth value for this sentence is

P	Q	R	$\mathrm{P} \wedge \mathrm{Q}$	$\sim \mathrm{R}$	$(\mathrm{P} \wedge \mathrm{Q}) \vee (\sim \mathrm{R})$
T	T	T	T	F	T
T	T	F	T	T	T
T	F	T	F	F	F
F	T	T	F	F	F
T	F	F	F	T	T
F	T	F	F	T	T
F	F	T	F	F	F
F	F	F	F	T	T

Since P is true and Q, R are false, the sentence $(\mathrm{P} \wedge \mathrm{Q}) \vee (\sim \mathrm{R})$ is true.

§1.1 Propositions and Connectives

Definition

A $\begin{array}{c}\textbf{\textit{tautology}}\\ \textbf{\textit{contradiction}}\end{array}$ is a propositional form that is $\begin{array}{c}\text{true}\\ \text{false}\end{array}$ for every assignment of truth values to its component.

Example

The logic symbol $(\mathrm{P} \vee \mathrm{Q}) \vee (\sim\mathrm{P} \wedge \sim\mathrm{Q})$ is a tautology.

Example

The logic symbol $\sim(\mathrm{P} \vee \sim\mathrm{P}) \vee (\mathrm{Q} \wedge \sim\mathrm{Q})$ is a contradiction.

Definition

Two propositional forms are said to be ***equivalent*** if they have the same truth value.

§1.1 Propositions and Connectives

Theorem

For propositions P, Q, R, *we have the following:*

(a) $\mathrm{P} \Leftrightarrow \sim(\sim \mathrm{P})$. (**Double Negation Law**)

$$\left.\begin{array}{l}\text{(b) } \mathrm{P} \vee \mathrm{Q} \Leftrightarrow \mathrm{Q} \vee \mathrm{P} \\ \text{(c) } \mathrm{P} \wedge \mathrm{Q} \Leftrightarrow \mathrm{Q} \wedge \mathrm{P}\end{array}\right\} \quad \textbf{(Commutative Laws)}$$

$$\left.\begin{array}{l}\text{(d) } \mathrm{P} \vee (\mathrm{Q} \vee \mathrm{R}) \Leftrightarrow (\mathrm{P} \vee \mathrm{Q}) \vee \mathrm{R} \\ \text{(e) } \mathrm{P} \wedge (\mathrm{Q} \wedge \mathrm{R}) \Leftrightarrow (\mathrm{P} \wedge \mathrm{Q}) \wedge \mathrm{R}\end{array}\right\} \quad \textbf{(Associative Laws)}$$

$$\left.\begin{array}{l}\text{(f) } \mathrm{P} \wedge (\mathrm{Q} \vee \mathrm{R}) \Leftrightarrow (\mathrm{P} \wedge \mathrm{Q}) \vee (\mathrm{P} \wedge \mathrm{R}) \\ \text{(g) } \mathrm{P} \vee (\mathrm{Q} \wedge \mathrm{R}) \Leftrightarrow (\mathrm{P} \vee \mathrm{Q}) \wedge (\mathrm{P} \vee \mathrm{R})\end{array}\right\} \quad \textbf{(Distributive Laws)}$$

$$\left.\begin{array}{l}\text{(h) } \sim(\mathrm{P} \wedge \mathrm{Q}) \Leftrightarrow (\sim \mathrm{P}) \vee (\sim \mathrm{Q}) \\ \text{(i) } \sim(\mathrm{P} \vee \mathrm{Q}) \Leftrightarrow (\sim \mathrm{P}) \wedge (\sim \mathrm{Q})\end{array}\right\} \quad \textbf{(De Morgan's Laws)}$$

§1.1 Propositions and Connectives

Proof.

We prove (g) for example, and the other cases can be shown in a similar fashion. Using the truth table,

P	Q	R	$\mathrm{Q}\wedge\mathrm{R}$	$\mathrm{P}\vee(\mathrm{Q}\wedge\mathrm{R})$	$\mathrm{P}\vee\mathrm{Q}$	$\mathrm{P}\vee\mathrm{R}$	$(\mathrm{P}\vee\mathrm{Q})\wedge(\mathrm{P}\vee\mathrm{R})$
T	T	T	T	T	T	T	T
T	T	F	F	T	T	T	T
T	F	T	F	T	T	T	T
F	T	T	T	T	T	T	T
T	F	F	F	T	T	T	T
F	T	F	F	F	T	F	F
F	F	T	F	F	F	T	F
F	F	F	F	F	F	F	F

we find that "$\mathrm{P}\vee(\mathrm{Q}\wedge\mathrm{R})$" is equivalent to "$(\mathrm{P}\vee\mathrm{Q})\wedge(\mathrm{P}\vee\mathrm{R})$". □

§1.1 Propositions and Connectives

Definition

A ***denial*** of a proposition is any proposition equivalent to $\sim \mathrm{P}$.

- **Rules for $\sim$, $\wedge$ and $\vee$:**

1. $\sim$ is always applied to the smallest proposition following it.
2. $\wedge$ connects the smallest propositions surrounding it.
3. $\vee$ connects the smallest propositions surrounding it.

Example

Under the convention above, we have

1. $\sim \mathrm{P} \vee \sim \mathrm{Q} \Leftrightarrow (\sim \mathrm{P}) \vee (\sim \mathrm{Q})$.
2. $\mathrm{P} \vee \mathrm{Q} \vee \mathrm{R} \Leftrightarrow (\mathrm{P} \vee \mathrm{Q}) \vee \mathrm{R} \Leftrightarrow \mathrm{P} \vee (\mathrm{Q} \vee \mathrm{R})$.
3. $\mathrm{P} \wedge \sim \mathrm{Q} \vee \sim \mathrm{R} \Leftrightarrow \big[\mathrm{P} \wedge (\sim \mathrm{Q})\big] \vee (\sim \mathrm{R})$.
4. $\mathrm{R} \wedge \mathrm{P} \wedge \mathrm{S} \wedge \mathrm{Q} \Leftrightarrow \big[(\mathrm{R} \wedge \mathrm{P}) \wedge \mathrm{S}\big] \wedge \mathrm{Q}$.

§1.2 Conditionals and Biconditionals

Definition

For propositions P and Q, the ***conditional sentence*** $P \Rightarrow Q$ is the proposition "if P, then Q". Proposition P is called the ***antecedent*** and Q is the ***consequence***. The sentence $P \Rightarrow Q$ is true if and only if P is false or Q is true.

Remark:

In a conditional sentence, P and Q might not have connections. The truth value of the sentence "$P \Rightarrow Q$" only depends on the truth value of P and Q.

§1.2 Conditionals and Biconditionals

Example

We would like to determine the truth value of the sentence "if $x > 8$, then $x > 5$". Let P denote the sentence "$x > 8$" and Q the sentence "$x > 5$".

1. If P, Q are both true statements, then $x > 8$ which is (exactly the same as P thus) true.
2. If P is false while Q is true, then $5 < x \leqslant 8$ which is (exactly the same as $\sim\mathrm{P} \wedge \mathrm{Q}$ thus) true.
3. If P, Q are both false statements, then $x \leqslant 5$ which is (exactly the same as $\sim\mathrm{Q}$ thus) true.
4. It is not possible to have P true but Q false.

§1.2 Conditionals and Biconditionals

- **How to read $\mathrm{P} \Rightarrow \mathrm{Q}$ in English?**

  1. If P, then Q. 2. P is sufficient for Q. 3. P only if Q.

  4. Q whenever P. 5. Q is necessary for P. 6. Q, if/when P.

Definition

Let P and Q be propositions.

1. The ***converse*** of $\mathrm{P} \Rightarrow \mathrm{Q}$ is $\mathrm{Q} \Rightarrow \mathrm{P}$.
2. The ***contrapositive*** of $\mathrm{P} \Rightarrow \mathrm{Q}$ is $\sim\mathrm{Q} \Rightarrow \sim\mathrm{P}$.

§1.2 Conditionals and Biconditionals

Example

We would like to determine the truth value, as well as the converse and the contrapositive, of the sentence "if π is an integer, then 14 is even".

1. Since that π is an integer is false, the implication "if π is an integer, then 14 is even" is true.
2. The converse of the sentence is "if 14 is even, then π is an integer" which is a false statement.
3. The contrapositive of the sentence is "if 14 is not even, then π is not an integer" which is a true statement since the antecedent "14 is not even" is false.

By this example, we know that a sentence and its converse cannot be equivalent.

§1.2 Conditionals and Biconditionals

Theorem

For propositions P *and* Q*, the sentence* $\mathrm{P} \Rightarrow \mathrm{Q}$ *is equivalent to its contrapositive* $\sim\mathrm{Q} \Rightarrow \sim\mathrm{P}$.

Proof.

Using the truth table

P	Q	$\mathrm{P} \Rightarrow \mathrm{Q}$	$\sim\mathrm{Q}$	$\sim\mathrm{P}$	$\sim\mathrm{Q} \Rightarrow \sim\mathrm{P}$
T	T	T	F	F	T
T	F	F	T	F	F
F	T	T	F	T	T
F	F	T	T	T	T

we conclude that the truth value of $\mathrm{P} \Rightarrow \mathrm{Q}$ and $\sim\mathrm{Q} \Rightarrow \sim\mathrm{P}$ are the same; thus they are equivalent sentences. □

§1.2 Conditionals and Biconditionals

Definition

For propositions P and Q, the ***bi-conditional sentence*** $\mathrm{P} \Leftrightarrow \mathrm{Q}$ is the proposition "P if and only if Q". The sentence $\mathrm{P} \Leftrightarrow \mathrm{Q}$ is true exactly when P and Q have the same truth values. In other words, $\mathrm{P} \Leftrightarrow \mathrm{Q}$ is true if and only if P is equivalent to Q.

Remark: The notation $\Leftrightarrow$ is a combination of $\Rightarrow$ and its converse $\Leftarrow$, so the notation seems to suggest that $(\mathrm{P} \Leftrightarrow \mathrm{Q})$ is equivalent to $(\mathrm{P} \Rightarrow \mathrm{Q}) \wedge (\mathrm{Q} \Rightarrow \mathrm{P})$. This is in fact true since

P	Q	$\mathrm{P} \Leftrightarrow \mathrm{Q}$	$\mathrm{P} \Rightarrow \mathrm{Q}$	$\mathrm{Q} \Rightarrow \mathrm{P}$	$(\mathrm{P} \Rightarrow \mathrm{Q}) \wedge (\mathrm{P} \Rightarrow \mathrm{Q})$
T	T	T	T	T	T
T	F	F	F	T	F
F	T	F	T	F	F
F	F	T	T	T	T

§1.2 Conditionals and Biconditionals

Example

1. The proposition “$2^3 = 8$ if and only if 49 is a perfect square” is true because both components are true.
2. The proposition “$\pi = \dfrac{22}{7}$ if and only if $\sqrt{2}$ is a rational number” is also true (since both components are false).
3. The proposition “$6 + 1 = 7$ if and only if Argentina is north of the equator” is false because the truth values of the components differ.

§1.2 Conditionals and Biconditionals

Remark:

Definitions may be stated with the "if and only if" wording, but it is also common practice to state a formal definition using the word "if". For example, we could say that "a function *f* is continuous at a number *c* if $\cdots$" leaving the "only if" part understood.

Example

A teacher says "If you score 74% or higher on the next test, you will pass the exam". Even though this is a conditional sentence, everyone will interpret the meaning as a biconditional (since the teacher tries to "define" how you can pass the exam).

§1.2 Conditionals and Biconditionals

Theorem

For propositions P, Q *and* R, *we have the following:*

(a) $(\mathrm{P} \Rightarrow \mathrm{Q}) \;\Leftrightarrow\; (\sim\mathrm{P} \vee \mathrm{Q})$.

(b) $(\mathrm{P} \Leftrightarrow \mathrm{Q}) \;\Leftrightarrow\; (\mathrm{P} \Rightarrow \mathrm{Q}) \wedge (\mathrm{Q} \Rightarrow \mathrm{P})$.

(c) $\sim(\mathrm{P} \Rightarrow \mathrm{Q}) \;\Leftrightarrow\; (\mathrm{P} \wedge \sim\mathrm{Q})$.

(d) $\sim(\mathrm{P} \wedge \mathrm{Q}) \;\Leftrightarrow\; (\mathrm{P} \Rightarrow \sim\mathrm{Q})$.

(e) $\sim(\mathrm{P} \wedge \mathrm{Q}) \;\Leftrightarrow\; (\mathrm{Q} \Rightarrow \sim\mathrm{P})$.

(f) $\mathrm{P} \Rightarrow (\mathrm{Q} \Rightarrow \mathrm{R}) \;\Leftrightarrow\; (\mathrm{P} \wedge \mathrm{Q}) \Rightarrow \mathrm{R}$.

(g) $\mathrm{P} \Rightarrow (\mathrm{Q} \wedge \mathrm{R}) \;\Leftrightarrow\; (\mathrm{P} \Rightarrow \mathrm{Q}) \wedge (\mathrm{P} \Rightarrow \mathrm{R})$.

(h) $(\mathrm{P} \vee \mathrm{Q}) \Rightarrow \mathrm{R} \;\Leftrightarrow\; (\mathrm{P} \Rightarrow \mathrm{R}) \wedge (\mathrm{Q} \Rightarrow \mathrm{R})$.

§1.2 Conditionals and Biconditionals

- **How to read** $\mathrm{P} \Leftrightarrow \mathrm{Q}$ **in English**?

  1. P if and only if Q.
  2. P if, but only if, Q.
  3. P implies Q, and conversely.
  4. P is equivalent to Q.
  5. P is necessary and sufficient for Q.

- **Rules for** $\sim$, $\wedge$, $\vee$, $\Rightarrow$ **and** $\Leftrightarrow$: These connectives are always applied in the order listed.

Example

1. $\mathrm{P} \Rightarrow \sim \mathrm{Q} \vee \mathrm{R} \Leftrightarrow \mathrm{S}$ is an abbr. for $\big(\mathrm{P} \Rightarrow \big[(\sim \mathrm{Q}) \vee \mathrm{R}\big]\big) \Leftrightarrow \mathrm{S}$.
2. $\mathrm{P} \vee \sim \mathrm{Q} \Leftrightarrow \mathrm{R} \Rightarrow \mathrm{S}$ is an abbr. for $\big[\mathrm{P} \vee (\sim \mathrm{Q})\big] \Leftrightarrow (\mathrm{R} \Rightarrow \mathrm{S})$.
3. $\mathrm{P} \Rightarrow \mathrm{Q} \Rightarrow \mathrm{R}$ is an abbr. for $(\mathrm{P} \Rightarrow \mathrm{Q}) \Rightarrow \mathrm{R}$.

§1.3 Quantified Statements

Definition

An ***open sentence*** is a sentence that contains variables. When P is an open sentence with a variable x (or variables $x_1, \cdots, x_n$), the sentence is symbolized by $\mathrm{P}(x)$ (or $\mathrm{P}(x_1, \cdots, x_n)$).
The ***truth set*** of an open sentence is the collection of variables (from a certain universe) that may be substituted to make the open sentence a true proposition. (使得 $\mathrm{P}(x)$ 為真的所有 x 形成 the truth set of $\mathrm{P}(x)$)

Remark:

In general, **an open sentence is not a proposition**. It can be true or false depending on the value of variables.

§1.3 Quantified Statements

Example

Let $\mathrm{P}(x)$ be the open sentence "x is a prime number between 5060 and 5090". In this open sentence, the universe is usually chosen to be $\mathbb{N}$, the natural number system, and the truth set of $\mathrm{P}(x)$ is $\{5077, 5081, 5087\}$.

Remark:

The truth set of an open sentence $\mathrm{P}(x)$ depends on the universe where x belongs to. For example, suppose that $\mathrm{P}(x)$ is the open sentence "$x^2 + 1 = 0$". If the universe is $\mathbb{R}$, then $\mathrm{P}(x)$ is false for all x (in the universe). On the other hand, if the universe is $\mathbb{C}$, the complex plane, then $\mathrm{P}(x)$ is true when $x = \pm i$ (which also implies that the truth set of $\mathrm{P}(x)$ is $\{i, -i\}$).

§1.3 Quantified Statements

Definition

With a universe X specified, two open sentences $\mathrm{P}(x)$ and $\mathrm{Q}(x)$ are equivalent if they have the same truth set of all $x \in X$.

Example

The two sentences "$3x + 2 = 20$" and "$2x - 7 = 5$" are equivalent open sentences in any of the number system, such as $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$.

Example

The two sentences "$x^2 - 1 > 0$" and "$(x < -1) \vee (x > 1)$" are equivalent open sentences in $\mathbb{R}$.

§1.3 Quantified Statements

Given an open sentence $\mathrm{P}(x)$, the first question that we should ask ourself is "whether the truth set of $\mathrm{P}(x)$ is empty or not".

Definition

The symbol $\exists$ is called the ***existential quantifier***. For an open sentence $\mathrm{P}(x)$, the sentence $(\exists x)\mathrm{P}(x)$ is read "there exists x such that $\mathrm{P}(x)$" or "for some x, $\mathrm{P}(x)$". The sentence $(\exists x)\mathrm{P}(x)$ is true if the truth set of $\mathrm{P}(x)$ is non-empty.

Remark:

An open sentence $\mathrm{P}(x)$ does **not** have a truth value, but the quantified sentence $(\exists x)\mathrm{P}(x)$ does.

§1.3 Quantified Statements

Example

The quantified sentence $(\exists\, x)(x^7 - 12x^3 + 16x - 3 = 0)$ is true in the universe of real numbers.

Example (Fermat number)

The quantified sentence $(\exists\, n)(2^{2^n} + 1$ is a prime number$)$ is true in the universe of natural numbers.

Example (Fermat's last theorem)

The quantified sentence

$$(\exists\, x, y, z, n)(x^n + y^n = z^n \wedge n \geqslant 3)$$

is true in the universe of integers, but is false in the universe of natural numbers.

§1.3 Quantified Statements

Definition

The symbol $\forall$ is called the ***universal quantifier***. For an open sentence $\mathrm{P}(x)$, the sentence $(\forall\, x)\mathrm{P}(x)$ is read “for all x, $\mathrm{P}(x)$”, ”for every x, $\mathrm{P}(x)$” or “for every given x (in the universe), $\mathrm{P}(x)$”. The sentence $(\forall\, x)\mathrm{P}(x)$ is true if the truth set of $\mathrm{P}(x)$ is the entire universe.

Example

The quantified sentence $(\forall\, n)(2^{2^n}+1$ is a prime number) is false in the universe of natural numbers since

$$2^{2^6}+1 = 641 \times 6700417\,.$$

§1.3 Quantified Statements

In general, statements of the form “every element of the set A has the property P” and “some element of the set A has property P” may be symbolized as $(\forall\, x \in A)\mathrm{P}(x)$ and $(\exists\, x \in A)\mathrm{P}(x)$, respective. Moreover,

1. “All $\mathrm{P}(x)$ are $\mathrm{Q}(x)$”（所有滿足 P 的 x 都滿足 Q or 只要滿足 P 的 x 就滿足 Q）should be symbolized as
$$“(\forall\, x)\big(\mathrm{P}(x) \Rightarrow \mathrm{Q}(x)\big)”.$$
(See the next slide for the explanation!)

2. “Some $\mathrm{P}(x)$ are $\mathrm{Q}(x)$”（有些滿足 P 的 x 也滿足 Q or 有些 x 同時滿足 P 和 Q）should be symbolized as
$$“(\exists\, x)\big(\mathrm{P}(x) \wedge \mathrm{Q}(x)\big)”.$$

§1.3 Quantified Statements

- **Explanation of 1**: Suppose that the truth set of $\mathrm{P}(x)$ is A and the truth set of $\mathrm{Q}(x)$ is B. Then "All $\mathrm{P}(x)$ are $\mathrm{Q}(x)$" implies that $A \subseteq B$; that is, if x in A, then x in B. Therefore, by reading the truth table

$x \in A$	$x \in B$	$\mathrm{P}(x)$	$\mathrm{Q}(x)$	$\mathrm{P}(x) \Rightarrow \mathrm{Q}(x)$
T	T	T	T	T
T	F	T	F	F
F	T	F	T	T
F	F	F	F	T

we find that the truth set of the open sentence $\mathrm{P}(x) \Rightarrow \mathrm{Q}(x)$ is the whole universe since the second case $(x \in A) \wedge \sim (x \in B)$ cannot happen.

§1.3 Quantified Statements

Example

1. The sentence “for every odd prime x less than 10, $x^2 + 4$ is prime” can be symbolized as

$$(\forall\, x)\big[(x \text{ is odd}) \wedge (x \text{ is prime}) \wedge (x < 10) \Rightarrow (x^2 + 4 \text{ is prime})\big].$$

2. The sentence “for every rational number there is a larger integer” can be symbolized as

$$(\forall\, x \in \mathbb{Q})\big[(\exists\, z \in \mathbb{Z})(z > x)\big]\,.$$

§1.3 Quantified Statements

Example

1. The sentence "some functions defined at 0 are not continuous at 0" can be symbolized as
$$(\exists f)\big[(f \text{ is defined at } 0) \wedge (f \text{ is not continuous at } 0)\big].$$
2. The sentence "some integers are even and some integers are odd" can be symbolized as
$$(\exists x)(x \text{ is even}) \wedge (\exists y)(y \text{ is odd}).$$
3. The sentence "some real numbers have a multiplicative inverse" (有些實數有乘法反元素) can be symbolized as
$$(\exists x \in \mathbb{R})\big[(\exists y \in \mathbb{R})(xy = 1)\big].$$

§1.3 Quantified Statements

To symbolized the sentence "any real numbers have an additive inverse" (任何實數都有加法反元素), it is required that we combine the use of the universal quantifier and the existential quantifier:

$$(\forall\, x \in \mathbb{R})\big[(\exists\, y \in \mathbb{R})(x + y = 0)\big]\,.$$

This is in fact quite common in mathematical statement. Another example is the sentence "some real number does not have a multiplicative inverse" (有些實數沒有乘法反元素) which can be symbolized by

$$(\exists\, x \in \mathbb{R}) \sim \big[(\exists\, y \in \mathbb{R})(xy = 1)\big]$$

or simply

$$(\exists\, x \in \mathbb{R})\big[(\forall\, y \in \mathbb{R})(xy \neq 1)\big]\,.$$

§1.3 Quantified Statements

- **Continuity of functions**: By the definition of continuity and using the logic symbol, f is continuous at a number c if

$$\underbrace{(\forall\,\varepsilon)\,(\exists\delta)\,\underbrace{(\forall\,x)\Big[(|x-c|<\delta)\Rightarrow(|f(x)-f(c)|<\varepsilon)\Big]}_{\mathrm{Q}(\varepsilon,\delta)}}_{\mathrm{P}(\varepsilon)\equiv(\exists\,\delta)\mathrm{Q}(\varepsilon,\delta)}\,.$$

1. The universe for the variables ε and δ is the collection of positive real numbers. Therefore, sometimes we write

$$(\forall\,\varepsilon>0)(\exists\,\delta>0)(\forall\,x)\Big[(|x-c|<\delta)\Rightarrow(|f(x)-f(c)|<\varepsilon)\Big]\,.$$

2. The sentence $\mathrm{P}(\varepsilon)$ is always true for any $\varepsilon>0$.

§1.3 Quantified Statements

- **Continuity of functions**: By the definition of continuity and using the logic symbol, f is continuous at a number c if

$$\underbrace{(\forall\,\varepsilon)\,(\exists\delta)\,\underbrace{(\forall\,x)\Big[(|x-c|<\delta)\Rightarrow(|f(x)-f(c)|<\varepsilon)\Big]}_{\mathrm{Q}(\varepsilon,\delta)}}_{\mathrm{P}(\varepsilon)\equiv(\exists\,\delta)\mathrm{Q}(\varepsilon,\delta)}\,.$$

1. The universe for the variables ε and δ is the collection of positive real numbers. Therefore, sometimes we write
$$(\forall\,\varepsilon>0)(\exists\,\delta>0)(\forall\,x)\Big[(|x-c|<\delta)\Rightarrow(|f(x)-f(c)|<\varepsilon)\Big]\,.$$
2. The sentence $(\exists\,\delta)\mathrm{Q}(\varepsilon,\delta)$ is always true for any $\varepsilon>0$.

§1.3 Quantified Statements

- **Continuity of functions**: By the definition of continuity and using the logic symbol, f is continuous at a number c if

$$(\forall\,\varepsilon)\,\underbrace{(\exists\delta)\,\underbrace{(\forall\,x)\Big[(|x-c|<\delta)\Rightarrow(|f(x)-f(c)|<\varepsilon)\Big]}_{\mathrm{Q}(\varepsilon,\delta)}}_{\mathrm{P}(\varepsilon)\equiv(\exists\,\delta)\mathrm{Q}(\varepsilon,\delta)}\,.$$

2. The sentence $(\exists\,\delta)\mathrm{Q}(\varepsilon,\delta)$ is always true for any $\varepsilon>0$.

3. Suppose ε is a given positive number. Then the truth set of $\mathrm{Q}(\varepsilon,\delta)$ is non-empty which implies that "there is at least one positive number δ making the sentence $\mathrm{Q}(\varepsilon,\delta)$ true".

§1.3 Quantified Statements

Definition

Two quantified statement are equivalent in a given universe if they have the same truth value in that universe. Two quantified sentences are equivalent if they are equivalent in every universe.

Example

Consider quantified sentences "$(\forall\, x)(x > 3)$" and "$(\forall\, x)(x \geqslant 4)$".

1. They are equivalent in the universe of integers because both are false.
2. They are equivalent in the universe of natural numbers greater than 10 because both are true.
3. They are not equivalent in the universe $X = [3.7, \infty)$ of the real line.

§1.3 Quantified Statements

Theorem

If $\mathrm{P}(x)$ *is an open sentence with variable* x*, then*

1. $\sim(\forall\, x)\mathrm{P}(x)$ *is equivalent to* $(\exists\, x) \sim \mathrm{P}(x)$.
2. $\sim(\exists\, x)\mathrm{P}(x)$ *is equivalent to* $(\forall\, x) \sim \mathrm{P}(x)$.

Proof.

Let X be the universe, and A be the truth set of $\mathrm{P}(x)$.

1. The sentence $(\forall\, x)\mathrm{P}(x)$ is true if and only if $A = X$; hence $\sim(\forall\, x)\mathrm{P}(x)$ is true if and only if $A \neq X$. The sentence $(\exists\, x) \sim \mathrm{P}(x)$ is true if and only if the truth set of $\sim \mathrm{P}(x)$ is non-empty; thus $(\exists\, x) \sim \mathrm{P}(x)$ is true if and only if $A \neq X$.
2. Using (a) and the double negation law,

$$\sim(\exists\, x)\mathrm{P}(x) \Leftrightarrow \sim\Big[\sim\big((\forall\, x) \sim \mathrm{P}(x)\big)\Big] \Leftrightarrow (\forall\, x) \sim \mathrm{P}(x)\,.$$

□

§1.3 Quantified Statements

Corollary

1. *If* $\mathrm{P}(x, y, z)$ *and* $\mathrm{Q}(x, y, z)$ *are open sentences with variables* x, y, z, *then* $\sim\big[(\forall\, x)(\exists\, y)(\forall\, z)\big(\mathrm{P}(x, y, z) \Rightarrow \mathrm{Q}(x, y, z)\big)\big]$ *is equivalent to* $(\exists\, x)(\forall\, y)(\exists\, z)\big(\mathrm{P}(x, y, z) \wedge \sim\mathrm{Q}(x, y, z)\big)$.
2. *If* $\mathrm{P}(x_1, \cdots, x_4)$ *and* $\mathrm{Q}(x_1, \cdots, x_4)$ *are open sentences with variables* x_1, x_2, x_3, x_4, *then* $\sim\big[(\exists\, x_1)(\forall\, x_2)(\exists\, x_3)(\forall\, x_4)\big(\mathrm{P}(x_1, \cdots, x_4) \Rightarrow \mathrm{Q}(x_1, \cdots, x_4)\big)\big]$ *is equivalent to* $(\forall\, x_1)(\exists\, x_2)(\forall\, x_3)(\exists\, x_4)\big(\mathrm{P}(x_1, \cdots, x_4) \wedge \sim\mathrm{Q}(x_1, \cdots, x_4)\big)$.

Proof.

The corollary can be proved using the theorem in the previous page and the fact that $\sim(\mathrm{P} \Rightarrow \mathrm{Q}) \Leftrightarrow (\mathrm{P} \wedge \sim \mathrm{Q})$. □

§1.3 Quantified Statements

- **Discontinuity of functions**:

A function f is continuous at c if and only if

$$(\forall\,\varepsilon>0)(\exists\,\delta>0)(\forall\,x)\Big[\big(|x-c|<\delta\big)\Rightarrow\Big(\big|f(x)-f(c)\big|<\varepsilon\Big)\Big]\,.$$

Therefore, f is not continuous at c if and only if

$$(\exists\,\varepsilon>0)(\forall\,\delta>0)(\exists\,x)\Big[\big(|x-c|<\delta\big)\wedge\Big(\big|f(x)-f(c)\big|\geqslant\varepsilon\Big)\Big]\,.$$

解讀：f 在 c 不連續，則存在一個正數 ε 使得任意正數 δ 所定義的開區間 $(c-\delta,c+\delta)$ 中有 x 會滿足 $\big|f(x)-f(c)\big|\geqslant\varepsilon$。

§1.3 Quantified Statements

- **Non-existence of limits**:

A function f defined on an interval containing c, except possibly at c, is said to have a limit at c $\big($or $\lim\limits_{x\to c} f(x)$ exists$\big)$ if and only if

$$(\exists\, L \in \mathbb{R})(\forall\, \varepsilon > 0)(\exists\, \delta > 0)(\forall\, x)\big((0 < |x - c| < \delta) \Rightarrow (|f(x) - L| < \varepsilon)\big)\,.$$

Therefore, f does not have a limit at c if

$$(\forall\, L \in \mathbb{R})(\exists\, \varepsilon > 0)(\forall\, \delta > 0)(\exists\, x)\big((0 < |x - c| < \delta) \wedge (|f(x) - L| \geqslant \varepsilon)\big)\,.$$

解讀：若 f 在 c 極限不存在，則不管對哪個（可能的極限）實數 L 都可以找到一個正數 ε，使得任意正數 δ 所定義的去中心區域 $(c-\delta, c) \cup (c, c+\delta)$ 中都有 x 會滿足 $|f(x) - L| \geqslant \varepsilon$。

§1.3 Quantified Statements

Theorem

Let $\mathrm{P}(x, y)$ *be an open sentence with two variables* x *and* y*. Then*

$$(\forall\, x, y)\mathrm{P}(x, y) \Leftrightarrow (\forall\, x)\big[(\forall\, y)\mathrm{P}(x, y)\big]\,.$$

Proof.

Suppose that the universe of x and y are X and Y, respectively. We note that

$$\begin{aligned}(\forall\, x, y)\mathrm{P}(x, y) \text{ is true} &\Leftrightarrow \text{the truth set of } \mathrm{P}(x, y) \text{ is } X \times Y\\ &\Leftrightarrow \text{For every given } x \in X\text{, the truth set of}\\ &\qquad \mathrm{P}(x, y) \text{ is } Y\\ &\Leftrightarrow (\forall\, x)\big[(\forall\, y)\mathrm{P}(x, y)\big]\end{aligned}$$

□

§1.3 Quantified Statements

Definition

The symbol $\exists!$ is called the ***unique existential quantifier***. For an open sentence $\mathrm{P}(x)$, then sentence $(\exists! x)\mathrm{P}(x)$ is read "there is a unique x such that $\mathrm{P}(x)$". The sentence $(\exists! x)\mathrm{P}(x)$ is true if the truth set of $\mathrm{P}(x)$ has exactly one element.

Theorem

If $\mathrm{P}(x)$ is an open sentence with variable x, then

1. $(\exists! x)\mathrm{P}(x) \Rightarrow (\exists x)\mathrm{P}(x)$.
2. $(\exists! x)\mathrm{P}(x) \Leftrightarrow \Big[\big((\exists x)\mathrm{P}(x)\big) \wedge \big((\forall\, y)(\forall\, z)(\mathrm{P}(y) \wedge \mathrm{P}(z) \Rightarrow y = z)\big)\Big]$.

§1.4 Basic Proof Methods I (Direct Proof)

Mathematical Theorem: A statement that describes a pattern or relationship among quantities or structures, usually of the form $\mathrm{P} \Rightarrow \mathrm{Q}$.

Proofs of a Theorem: Justifications of the truth of the theorem that follows the principle of logic.

Lemma: A result that serves as a preliminary step to prove the main theorem.

Axiom (公設): Some facts that are used to develop certain theory and **cannot** be proved.

Undefined terms: Not everything can/have to be defined, and we have to treat them as known.

§1.4 Basic Proof Methods I (Direct Proof)

Remark:

1. To validate a conditional sentence $\mathrm{P} \Rightarrow \mathrm{Q}$, by definition you only need to show that there is **no** chance that P is true but at the same time Q is false. Therefore, you often show that if P is true then Q is true, if Q is false then P is false or that P is true and Q is false leads to a contradiction (always false).

2. Sometimes it is difficult to identify the antecedent of a mathematical theorem. Usually it is because the antecedent is too trivial to be stated. For example, "$\sqrt{2}$ is an irrational number" is a mathematical theorem and it can be understood as "**if you know what an irrational number is**, then $\sqrt{2}$ is an irrational number".

§1.4 Basic Proof Methods I (Direct Proof)

- **General format of proving $\mathrm{P} \Rightarrow \mathrm{Q}$ directly**:

Direct proof of $\mathrm{P} \Rightarrow \mathrm{Q}$

Proof.

Assume P. (可用很多方式取代，主要是看 P 的內容)

$\vdots$

Therefore, Q.

Thus, $\mathrm{P} \Rightarrow \mathrm{Q}$. □

§1.4 Basic Proof Methods I (Direct Proof)

Basic Rules: In any proof at any time you may

1. state an axiom (by the axiom of $\cdots\cdots$), an assumption (assume that $\cdots\cdots$), or a previously proved result (by the fact that $\cdots\cdots$).
2. state a sentence whose symbolic translation is a tautology (such as classification 分類).
3. state a sentence (or use a definition) equivalent to any statement earlier in the proof.
4. use the *modus ponens rule*: after statements P and $\mathrm{P} \Rightarrow \mathrm{Q}$ appear in a proof, state Q.

§1.4 Basic Proof Methods I (Direct Proof)

Example

Prove that if x is odd, then $x+1$ is even.

Proof.

Assume that x is an odd number.

Then $x = 2k+1$ for some integer k;

thus $x+1 = 2k+1+1 = 2(k+1)$ which shows that $x+1$ is a multiple of 2.

Therefore, $x+1$ is even. □

§1.4 Basic Proof Methods I (Direct Proof)

Example

Let a, b, c be integers. If a divides b and b divides c, then a divides c.

Proof.

Let a, b, c be integers.

Assume that a divides b and b divides c.

Then $b = am$ for some integer m, and $c = bn$ for some integer n;

thus $c = (am)n = a(mn)$ which shows that c is an multiple of a.

Therefore, a divides c. □

§1.4 Basic Proof Methods I (Direct Proof)

Example

Let a, b, c be integers. If a divides b and b divides c, then a divides c.

Proof.

Let a, b, c be integers.

Assume that a divides b. Then $b = am$ for some integer m.

Assume that b divides c. Then $c = bn$ for some integer n.

Thus, $c = (am)n = a(mn)$ which shows that c is an multiple of a.

Therefore, a divides c. □

§1.4 Basic Proof Methods I (Direct Proof)

Example

Show that $(\forall\, x \in \mathbb{R})(x^2 + 1 > 0)$.

翻譯成 P ⇒ Q 的句型：**Show that if $x \in \mathbb{R}$, then $x^2 + 1 > 0$.**

Proof.

Assume that x is a real number.

Then either $x > 0$, $x = 0$ or $x < 0$.

1. If $x > 0$, then $x^2 = x \cdot x > 0$.
2. If $x = 0$, then $x^2 = 0$.
3. If $x < 0$, then $(-x) > 0$; thus $x^2 = (-x) \cdot (-x) > 0$.

In either cases, $x^2 \geqslant 0$; thus $x^2 + 1 > 0$.

Therefore, $x^2 + 1 > 0$. □

§1.4 Basic Proof Methods I (Direct Proof)

Example

Show that $(\forall\, \varepsilon > 0)\left(\#\left\{n \in \mathbb{N} \,\middle|\, \frac{1}{n} > \varepsilon\right\} < \infty\right)$.

翻譯成 P $\Rightarrow$ Q 的句型：**Show that if $\varepsilon > 0$, then the collection $\left\{n \in \mathbb{N} \,\middle|\, \frac{1}{n} > \varepsilon\right\}$ has only finitely many elements.**

Proof.

Assume that $\varepsilon > 0$. Then $\frac{1}{\varepsilon} < \infty$.

Note that $\left\{n \in \mathbb{N} \,\middle|\, \frac{1}{n} > \varepsilon\right\} = \left\{n \in \mathbb{N} \,\middle|\, n < \frac{1}{\varepsilon}\right\}$ which is the collection of natural numbers less than $\frac{1}{\varepsilon}$. Therefore,

$$\#\left\{n \in \mathbb{N} \,\middle|\, \frac{1}{n} > \varepsilon\right\} \leqslant \frac{1}{\varepsilon} < \infty\,.$$

□

§1.4 Basic Proof Methods I (Direct Proof)

Example

Show that $(\forall\, x \in \mathbb{R})(\exists\, y \in \mathbb{R})(x + y = 0)$.

翻譯成 $\mathrm{P} \Rightarrow \mathrm{Q}$ 的句型：**Show that "if $x \in \mathbb{R}$, then the truth set of the open sentence $\mathrm{P}(y) \equiv (x + y = 0)$ is non-empty" or "if $x \in \mathbb{R}$, then there exists $y \in \mathbb{R}$ such that $x + y = 0$".**

Proof.

Assume that x is a real number.

Then $y = -x$ is a real number and $x + y = 0$.

Thus, there exists $y \in \mathbb{R}$ such that $x + y = 0$.

Therefore, for each $x \in \mathbb{R}$, there exists $y \in \mathbb{R}$ such that $x + y = 0$. □

§1.4 Basic Proof Methods I (Direct Proof)

Example

Show that $(\forall x \in \mathbb{R})(\exists y \in \mathbb{R})(x + y = 0)$.

翻譯成 $\mathrm{P} \Rightarrow \mathrm{Q}$ 的句型：**Show that "if $x \in \mathbb{R}$, then the truth set of the open sentence $\mathrm{P}(y) \equiv (x + y = 0)$ is non-empty" or "if $x \in \mathbb{R}$, then there exists $y \in \mathbb{R}$ such that $x + y = 0$".**

Proof.

Let x be a real number.

Then $y = -x$ is a real number and $x + y = 0$.

Thus, there exists $y \in \mathbb{R}$ such that $x + y = 0$.

Therefore, for each $x \in \mathbb{R}$, there exists $y \in \mathbb{R}$ such that $x + y = 0$. □

§1.4 Basic Proof Methods I (Direct Proof)

Example

Show that $(\forall\, x \in \mathbb{R})(\exists\, y \in \mathbb{R})(x + y = 0)$.

翻譯成 $\mathrm{P} \Rightarrow \mathrm{Q}$ 的句型：**Show that "if $x \in \mathbb{R}$, then the truth set of the open sentence $\mathrm{P}(y) \equiv (x + y = 0)$ is non-empty" or "if $x \in \mathbb{R}$, then there exists $y \in \mathbb{R}$ such that $x + y = 0$".**

Proof.

Let $x \in \mathbb{R}$ be given.

Then $y = -x$ is a real number and $x + y = 0$.

Thus, there exists $y \in \mathbb{R}$ such that $x + y = 0$.

Therefore, for each $x \in \mathbb{R}$, there exists $y \in \mathbb{R}$ such that $x + y = 0$. □

§1.5 Basic Proof Methods II (Indirect Proof)

Recall that a conditional sentence is equivalent to its contrapositive; that is, $(P \Rightarrow Q) \Leftrightarrow (\sim Q \Rightarrow \sim P)$.

- **General format of proving $P \Rightarrow Q$ by contraposition**:

Proof of $P \Rightarrow Q$ by Contraposition

Proof.

Assume $\sim Q$. (可用很多方式取代，主要是看 $\sim Q$ 的內容)

$\vdots$

Therefore, $\sim P$.

Thus, $\sim Q \Rightarrow \sim P$.

Therefore, $P \Rightarrow Q$. □

§1.5 Basic Proof Methods II (Indirect Proof)

Example

Let m be an integer. Show that if m^2 is even, then m is even.

Proof.

Assume (the contrary) that m is odd.

Then $m = 2k + 1$ for some integer k.

Therefore, $m^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$ which is an odd number.

Thus, if m is odd, then m^2 is odd.

Therefore, if m^2 is even, then m is even. □

§1.5 Basic Proof Methods II (Indirect Proof)

Example

Let x and y be real numbers such that $x < 2y$. Show that if $7xy \leqslant 3x^2 + 2y^2$, then $3x \leqslant y$.

Proof.

Let x and y be real numbers such that $x < 2y$.

Assume the contrary that $3x > y$.

Then $2y - x > 0$ and $3x - y > 0$.

Therefore, $(2y - x)(3x - y) > 0$.

Expanding the expression, we find that $7xy - 3x^2 - 2y^2 > 0$.

Therefore, $7xy > 3x^2 + 2y^2$.

Thus, if $3x > y$, then $7xy > 3x^2 + 2y^2$.

Therefore, if $7xy \leqslant 3x^2 + 2y^2$, then $3x \leqslant y$. □

§1.5 Basic Proof Methods II (Indirect Proof)

- **General format of proving $\mathrm{P} \Rightarrow \mathrm{Q}$ by contradiction**:

Proof of $\mathrm{P} \Rightarrow \mathrm{Q}$ by Contradiction

Proof.

Assume P and $\sim\mathrm{Q}$. (可用很多方式取代，主要是看 P 與 $\sim\mathrm{Q}$ 的內容)

$\vdots$

Therefore, $\sim\mathrm{P}$.

Thus, $\mathrm{P} \wedge \sim\mathrm{P}$, a contradiction.

Therefore, $\mathrm{P} \Rightarrow \mathrm{Q}$. □

§1.5 Basic Proof Methods II (Indirect Proof)

- **General format of proving $\mathrm{P} \Rightarrow \mathrm{Q}$ by contradiction:**

Proof of $\mathrm{P} \Rightarrow \mathrm{Q}$ by Contradiction

Proof.

Assume P and $\sim\mathrm{Q}$. (可用很多方式取代，主要是看 P 與 $\sim\mathrm{Q}$ 的內容)

$\vdots$

Therefore, $\sim\mathrm{P}$, a contradiction.

~~Thus, $\mathrm{P} \wedge \sim\mathrm{P}$, a contradiction.~~

Therefore, $\mathrm{P} \Rightarrow \mathrm{Q}$. □

§1.5 Basic Proof Methods II (Indirect Proof)

As mentioned before, there are cases that the antecedent of a theorem is unclear. This kind of theorems are of the form Q.

- **General format of proving Q by contradiction**:

Proof of Q by Contradiction

Proof.

Assume $\sim\mathrm{Q}$. (可用很多方式取代，主要是看 $\sim\mathrm{Q}$ 的內容)

$\vdots$ (通常是敘述公設或是定義的過程)

Therefore, P.

$\vdots$ (由 $\mathrm{P}\wedge\sim\mathrm{Q}$ 進行邏輯推演)

Therefore, $\sim\mathrm{P}$.

Thus, $\mathrm{P}\wedge\sim\mathrm{P}$, a contradiction.

Therefore, $\mathrm{P}\Rightarrow\mathrm{Q}$. □

§1.5 Basic Proof Methods II (Indirect Proof)

Example

Show that $\sqrt{2}$ is an irrational number.

Proof.

Assume the contrary that $\sqrt{2}$ is a rational number.

Then $\sqrt{2} = \frac{q}{p}$ for some positive integers p, q satisfying $(p, q) = 1$.

Thus, q^2 is an even number since $q^2 = 2p^2$.

By previous example, q is even; thus $q = 2k$ for some integer k.

Then p^2 is an even number since $p^2 = \frac{q^2}{2} = 2k^2$.

The previous example again implies that p is an even number.

Therefore, $(p, q) \neq 1$, a contradiction.

Therefore, $\sqrt{2}$ is an irrational number. □

§1.5 Basic Proof Methods II (Indirect Proof)

Example

Show that the collection of primes is infinite.

Proof.

Assume the contrary that there are only finitely many primes.

Suppose that $p_1 < p_2 < \cdots < p_k$ are all the prime numbers.

Let $n = p_1 p_2 \cdots p_k + 1$. Then $n > p_k$ and n is not a prime.

Therefore, n has a prime divisor（質因數）q; that is, q is a prime and $q|n$.

Since q is a prime, $q = p_j$ for some $1 \leqslant j \leqslant k$.

However, $q = p_j$ does not divide n, a contradiction.

Therefore, the collection of primes is infinite. □

§1.5 Basic Proof Methods II (Indirect Proof)

Example

There are n people ($n \geqslant 2$) at a party, some of whom are friends. Prove that there exists someone at the party who is friends with the same number of party-goers as another person.

中文解釋：證明在一個宴會中，至少有兩個人在宴會中的朋友數一樣多。

Proof.

Assume the contrary that no two party-goers have the same number of friends. Note that the number of friends should range from 0 to $n-1$; thus by the assumption that no two party-goers have the same number of friends, there must be one party-goer who has no friend, while there must be one party-goer who has $n-1$ friends. This is impossible because the one who has $n-1$ friends is a friend of the one who has no friend. □

§1.5 Basic Proof Methods II (Indirect Proof)

Some mathematical theorems are of the form $\mathrm{P} \Leftrightarrow \mathrm{Q}$. As explained before, this means $\mathrm{P} \Rightarrow \mathrm{Q}$ and $\mathrm{Q} \Rightarrow \mathrm{P}$; thus one should establish these two implication separately.

- **General format of proving** $\mathrm{P} \Leftrightarrow \mathrm{Q}$:

Proof of $\mathrm{P} \Leftrightarrow \mathrm{Q}$

Proof.

(i) Show that $\mathrm{P} \Rightarrow \mathrm{Q}$ using the methods mentioned above.

(ii) Show that $\mathrm{Q} \Rightarrow \mathrm{P}$ using the methods mentioned above.

Therefore, $\mathrm{P} \Leftrightarrow \mathrm{Q}$. □

§1.5 Basic Proof Methods II (Indirect Proof)

Example

Let m, n be integers. Show that m and n have the same parity (同奇同偶) if and only if $m^2 + n^2$ is even.

Proof.

$(\Rightarrow)$ If m and n are both even, then $m = 2k$ and $n = 2\ell$ for some integers k and ℓ. Therefore, $m^2 + n^2 = 2(2k^2 + 2\ell^2)$ which is even. If m and n are both odd, then $m = 2k + 1$ and $n = 2\ell + 1$ for some integers k and ℓ. Therefore, $m^2 + n^2 = 2(2k^2 + 2\ell^2 + 2k + 2\ell + 1)$ which is even. Therefore, if m and n have the same parity, $m^2 + n^2$ is even. □

§1.5 Basic Proof Methods II (Indirect Proof)

Example

Let m, n be integers. Show that m and n have the same parity (同奇同偶) if and only if $m^2 + n^2$ is even.

Proof.

($\Leftarrow$) Assume the contrary that there are m and n having opposite parity. W.L.O.G. we can assume that m is even and n is odd. Then $m = 2k$ and $n = 2\ell + 1$ for some integers k and ℓ. Therefore, $m^2 + n^2 = 2(2k^2 + 2\ell^2 + 2\ell) + 1$ which is odd. Thus, if m and n have opposite parity, then $m^2 + n^2$ is odd. Therefore, if $m^2 + n^2$ is even, then m and n have the same parity. □

§1.5 Basic Proof Methods II (Indirect Proof)

Remark:

1. Sometimes it requires intermediate equivalent propositions to show $\mathrm{P} \Leftrightarrow \mathrm{Q}$; that is, one might establish
$$(\mathrm{P} \Leftrightarrow \mathrm{R}_1) \wedge (\mathrm{R}_1 \Leftrightarrow \mathrm{R}_2) \wedge \cdots \wedge (\mathrm{R}_{n-1} \Leftrightarrow \mathrm{R}_n) \wedge (\mathrm{R}_n \Leftrightarrow \mathrm{Q})$$
to prove $\mathrm{P} \Leftrightarrow \mathrm{Q}$.

2. Often times it is more efficient to show a theorem of the form "$\mathrm{P}_1, \mathrm{P}_2, \cdots, \mathrm{P}_n$ are equivalent" (which means $\mathrm{P}_1, \mathrm{P}_2, \cdots, \mathrm{P}_n$ have the same truth value) by showing that $\mathrm{P}_1 \Rightarrow \mathrm{P}_2$, $\mathrm{P}_2 \Rightarrow \mathrm{P}_3$, $\cdots$, and $\mathrm{P}_n \Rightarrow \mathrm{P}_1$. In other words, one uses the following relation
$$\begin{aligned}&\big[(\mathrm{P}_1 \Leftrightarrow \mathrm{P}_2) \wedge (\mathrm{P}_2 \Leftrightarrow \mathrm{P}_3) \wedge \cdots \wedge (\mathrm{P}_{n-1} \Leftrightarrow \mathrm{P}_n)\big]\\ \Leftrightarrow\ &\big[(\mathrm{P}_1 \Rightarrow \mathrm{P}_2) \wedge (\mathrm{P}_2 \Rightarrow \mathrm{P}_3) \wedge \cdots \wedge (\mathrm{P}_n \Rightarrow \mathrm{P}_1)\big]\end{aligned}$$
to prove this kind of theorems.

§1.5 Basic Proof Methods II (Indirect Proof)

Example

Let x, y be non-negative real numbers such that $x - 4y < y - 3x$. Prove that if $3x > 2y$, then $12x^2 + 10y^2 < 24xy$.

Proof.

(Direct Proof): Let x, y be non-negative real numbers such that $x - 4y < y - 3x$. Suppose that $3x > 2y$. Then $4x - 5y < 0$ and $3x - 2y > 0$. Therefore,

$$0 > (4x - 5y)(3x - 2y) = 12x^2 + 10y^2 - 23xy$$

or equivalently, $12x^2 + 10y^2 < 23xy$. Since x, y are non-negative real numbers, $23xy \leqslant 24xy$; thus $12x^2 + 10y^2 < 24xy$. □

§1.5 Basic Proof Methods II (Indirect Proof)

Example

Let x, y be non-negative real numbers such that $x - 4y < y - 3x$. Prove that if $3x > 2y$, then $12x^2 + 10y^2 < 24xy$.

Proof.

(Proof by Contraposition): Let x, y be non-negative real numbers such that $x - 4y < y - 3x$. Assume the contrary that $12x^2 + 10y^2 \geqslant 24xy$. Since x, y are non-negative real numbers,

$$12x^2 + 10y^2 \geqslant 24xy \geqslant 23xy;$$

thus $(4x - 5y)(3x - 2y) = 12x^2 + 10y^2 - 23xy \geqslant 0$. Since $x - 4y < y - 3x$, we find that $4x - 5y < 0$; thus $3x - 2y \leqslant 0$. □

§1.5 Basic Proof Methods II (Indirect Proof)

Example

Let x, y be non-negative real numbers such that $x - 4y < y - 3x$. Prove that if $3x > 2y$, then $12x^2 + 10y^2 < 24xy$.

Proof.

(Proof by Contradiction): Let x, y be non-negative real numbers such that $x - 4y < y - 3x$. Assume that $3x > 2y$ and $12x^2 + 10y^2 \geqslant 24xy$. Then $4x - 5y < 0$ and $3x - 2y > 0$; thus

$$0 > (4x-5y)(3x-2y) = 12x^2+8y^2-23xy \geqslant 24xy-23xy = xy \geqslant 0\,,$$

where the last inequality follows from the fact that x, y are non-negative real numbers. Thus, we reach a contradiction $0 > 0$. □

§1.6 Proofs Involving Quantifiers

- **General format of proving** $(\forall\, x)\mathrm{P}(x)$ **directly**:

Note that to establish $(\forall\, x)\mathrm{P}(x)$ is the same as proving that

"if x is in the universe, then $\mathrm{P}(x)$ is true".

Direct Proof of $(\forall\, x)\mathrm{P}(x)$

Proof.

Let x be given in the universe. (可用很多方式取代，主要是看宇集是什麼)

$\vdots$

Hence $\mathrm{P}(x)$ is true.

Therefore, $(\forall\, x)\mathrm{P}(x)$ is true. □

§1.6 Proofs Involving Quantifiers

- **General format of proving** $(\forall x)\mathrm{P}(x)$ **by contradiction**:

To prove "if x is in the universe, then $\mathrm{P}(x)$ is true" by contradiction is to show that "an x in the universe so that $\mathrm{P}(x)$ is false leads to a contradiction".

Proof of $(\forall x)\mathrm{P}(x)$ **by contradiction**

Proof.

Assume (the contrary) that $\sim(\forall x)\mathrm{P}(x)$.

Then $(\exists x) \sim \mathrm{P}(x)$.

Let x be an element in the universe such that $\sim \mathrm{P}(x)$.

$$\vdots$$

Therefore, $\mathrm{Q} \wedge \sim \mathrm{Q}$, a contradiction.

Thus $(\exists x) \sim \mathrm{P}(x)$ is false, so $(\forall x)\mathrm{P}(x)$ is true. □

§1.6 Proofs Involving Quantifiers

- **General format of proving $(\forall x)\mathrm{P}(x)$ by contradiction**:

To prove "if x is in the universe, then $\mathrm{P}(x)$ is true" by contradiction is to show that "an x in the universe so that $\mathrm{P}(x)$ is false leads to a contradiction".

Proof of $(\forall x)\mathrm{P}(x)$ by contradiction

Proof.

Assume (the contrary) that ~~$\sim(\forall x)\mathrm{P}(x)$~~.

~~Then~~ $(\exists x) \sim\mathrm{P}(x)$.

Let x be an element in the universe such that $\sim\mathrm{P}(x)$.

$$\vdots$$

Therefore, $\mathrm{Q} \wedge \sim\mathrm{Q}$, a contradiction.

Thus $(\exists x) \sim\mathrm{P}(x)$ is false, so $(\forall x)\mathrm{P}(x)$ is true. □

§1.6 Proofs Involving Quantifiers

Example

Show that for all $x \in \left(0, \frac{\pi}{2}\right)$, $\sin x + \cos x > 1$.

Proof.

Assume that there exists $x \in (0, \pi/2)$ such that $\sin x + \cos x \leqslant 1$. Then $0 < \sin x + \cos x \leqslant 1$; thus

$$0 < (\sin x + \cos x)^2 \leqslant 1\,.$$

Expanding the square and using the identity $\sin^2 x + \cos^2 x = 1$, we find that

$$0 < 1 + 2 \sin x \cos x \leqslant 1$$

which shows $\sin x \cos x \leqslant 0$. On the other hand, since $x \in (0, \pi/2)$, we have $\sin x > 0$ and $\cos x > 0$ so that $\sin x \cos x > 0$, a contradiction. Therefore, $\sin x + \cos x > 1$ for all $x \in (0, \pi/2)$. □

§1.6 Proofs Involving Quantifiers

- **General format of proving $(\exists x)\mathrm{P}(x)$ directly: Method 1.**

The most straight forward way to show that $(\exists x)\mathrm{P}(x)$ is to give a precise x in the universe and show that $\mathrm{P}(x)$ is true; however, this usually requires that you makeq some effort to find out which x suits this requirement.

Constructive Proof of $(\exists x)\mathrm{P}(x)$

Proof.

Specify one particular element a.

If necessary, verify that a is in the universe.

$\vdots$

Therefore, $\mathrm{P}(a)$ is true.

Thus $(\exists x)\mathrm{P}(x)$ is true. □

§1.6 Proofs Involving Quantifiers

Example

Show that between two different rational numbers there is a rational number.

Proof.

Let a, b be rational numbers and $a < b$. Let $c = \frac{a+b}{2}$. Then $c \in \mathbb{Q}$ and $a < c < b$. □

Example

Show that there exists a natural number whose fourth power is the sum of other three fourth power.

Proof.

20615693 is one such number because it is a natural number and

$$20615673^4 = 2682440^4 + 1536539^4 + 18796760^4\,.$$

□

§1.6 Proofs Involving Quantifiers

- **General format of proving $(\exists\, x)\mathrm{P}(x)$ directly: Method 2.**

To show $(\exists\, x)\mathrm{P}(x)$, often times it is almost impossible to provide a precise x so that $\mathrm{P}(x)$ is true. Proving $(\exists\, x)\mathrm{P}(x)$ directly (not proving by contradiction) then usually requires a lot of abstract steps.

Non-Constructive Proof of $(\exists\, x)\mathrm{P}(x)$

Proof.

$$\vdots$$

Therefore, $\mathrm{P}(a)$ is true.

Thus $(\exists\, x)\mathrm{P}(x)$ is true. □

§1.6 Proofs Involving Quantifiers

Example

Let $f\colon [0,1] \to [0,1]$ be continuous. Show that

$$(\exists\, x \in [0,1])\big(x = f(x)\big)\,.$$

Proof.

1. If $f(0) = 0$ or $f(1) = 1$, then $(\exists\, x \in [0,1])\big(x = f(x)\big)$.
2. If $f(0) \neq 0$ and $f(1) \neq 1$, then $0 < f(0), f(1) < 1$.

   Define $g : [0,1] \to \mathbb{R}$ by $g(x) = x - f(x)$. Then g is continuous on $[0,1]$. Moreover, $g(0) < 0$ and $g(1) > 0$. Thus, the **Intermediate Value Theorem** implies that there exists x such that $0 < x < 1$ and $g(x) = 0$ (which is the same as $x = f(x)$).

In either cases, there exists $x \in [0,1]$ such that $x = f(x)$. □

§1.6 Proofs Involving Quantifiers

- **General format of proving $(\exists\, x)\mathrm{P}(x)$ by contradiction**:

Proof of $(\exists\, x)\mathrm{P}(x)$ by contradiction

Proof.

Suppose the contrary that $\sim(\exists\, x)\mathrm{P}(x)$.

Then $(\forall\, x) \sim \mathrm{P}(x)$.

$$\vdots$$

Therefore, $\mathrm{Q} \wedge \sim \mathrm{Q}$, a contradiction.

Thus $(\exists\, x)\mathrm{P}(x)$ is true. □

§1.6 Proofs Involving Quantifiers

Example

Let S be a set of 6 positive integers, each less than or equal to 10. Prove that there exists a pair of integers in S whose sum is 11.

Proof.

Suppose the contrary that every pair of integers in S has a sum different from 11. Then S contains at most one element from each of the sets $\{1,10\}$, $\{2,9\}$, $\{3,8\}$, $\{4,7\}$ and $\{5,6\}$. Thus, S contains at most 5 elements, a contradiction. We conclude that S contains a pair of numbers whose sum in 11. □

§1.6 Proofs Involving Quantifiers

- **General format of proving** $(\exists\,!x)\mathrm{P}(x)$:

Proof of $(\exists\,!x)\mathrm{P}(x)$

Proof.

(i) Prove that $(\exists\,x)\mathrm{P}(x)$ is true using the methods mentioned above.

(ii) Prove that $(\forall\,y)(\forall\,z)\Big[\big(P(y) \wedge P(z)\big) \Rightarrow (y = z)\Big]$:

Assume that y and z are elements in the universe such that $\mathrm{P}(y)$ and $\mathrm{P}(z)$ are true.

$\vdots$

Therefore, $y = z$.

From (i) and (ii) we conclude that $(\exists\,!x)\mathrm{P}(x)$ is true. □

§1.6 Proofs Involving Quantifiers

Example

Prove that every non-zero real number has a unique multiplicative inverse.

Proof.

Let x be a non-zero real number.

1. Let $y = \frac{1}{x}$. Since $x \neq 0$, y is a real number. Moreover, $xy = 1$; thus $(\exists\, y \in \mathbb{R})(xy = 1)$.
2. Suppose that y and z are real numbers such that $xy = xz = 1$. Then $x(y - z) = xy - xz = 0$. By the fact that $x \neq 0$, we must have $y = z$.

Therefore, $(\forall\, x \neq 0)(\exists\, !y)(xy = 1)$. □

§1.6 Proofs Involving Quantifiers

Some manipulations of quantifiers that permit valid deductions:

$$(\forall\, x)(\forall\, y)\mathrm{P}(x,y) \Leftrightarrow (\forall\, y)(\forall\, x)\mathrm{P}(x,y)\,, \tag{1a}$$

$$(\exists\, x)(\exists\, y)\mathrm{P}(x,y) \Leftrightarrow (\exists\, y)(\exists\, x)\mathrm{P}(x,y)\,, \tag{1b}$$

$$(\forall\, x)\mathrm{P}(x) \vee (\forall\, x)\mathrm{Q}(x) \Rightarrow (\forall\, x)\big[\mathrm{P}(x) \vee \mathrm{Q}(x)\big]\,, \tag{1c}$$

$$(\forall\, x)\big[\mathrm{P}(x) \Rightarrow \mathrm{Q}(x)\big] \Rightarrow \big[(\forall\, x)\mathrm{P}(x) \Rightarrow (\forall\, x)\mathrm{Q}(x)\big]\,, \tag{1d}$$

$$(\forall\, x)\big[\mathrm{P}(x) \wedge \mathrm{Q}(x)\big] \Leftrightarrow \big[(\forall\, x)\mathrm{P}(x) \wedge (\forall\, x)\mathrm{Q}(x)\big]\,, \tag{1e}$$

$$(\exists\, x)(\forall\, y)\mathrm{P}(x,y) \Rightarrow (\forall\, y)(\exists\, x)\mathrm{P}(x,y)\,. \tag{1f}$$

§1.6 Proofs Involving Quantifiers

Counter-examples for the non-equivalence in (1c), (1d), (1f):

1. the "if" direction in (1c): Let the universe be all the integers, $\mathrm{P}(x)$ be the statement "x is an even number" and $\mathrm{Q}(x)$ be the statement "x is an odd number". Then clearly $(\forall\, x)\big[\mathrm{P}(x) \vee \mathrm{Q}(x)\big]$ but we do not have $(\forall\, x)\mathrm{P}(x) \vee (\forall\, x)\mathrm{Q}(x)$.
2. the "if" direction in (1d): Let the universe be all the animals, $\mathrm{P}(x)$ be the statement "x has wings" and $\mathrm{Q}(x)$ be the statement "x is a bird". Then clearly the implication $\big[(\forall\, x)\mathrm{P}(x) \Rightarrow (\forall\, x)\mathrm{Q}(x)\big]$ is true (since the antecedent is false) while the statement $(\forall\, x)\big[\mathrm{P}(x) \Rightarrow \mathrm{Q}(x)\big]$ is false.
3. the "if" direction in (1f): Let the universe be all the non-negative real numbers, and $\mathrm{P}(x, y)$ be the statement "$y = x^2$". Clearly $(\forall\, y)(\exists\, x)\mathrm{P}(x, y)$ but we do not have $(\exists\, x)(\forall\, y)\mathrm{P}(x, y)$.

§1.7 Strategies for Constructing Proofs

Summary of strategies you should try when you begin to write a proof:

1. **Understand the statement to be proved**: make sure you know the **definitions** of all terms that appear in the statement.
2. **Identify the assumption(s) and the conclusion**, and **determine the logical form of the statement**.
3. **Look for the key ideas**: Ask yourself what is needed to reach the conclusion. Find relationships among the terms, the equations, and formulas involved. Recall known facts and previous results about the antecedent and consequence.

§1.7 Strategies for Constructing Proofs

Proof of $(\mathrm{P} \Rightarrow \mathrm{Q}_1 \vee \mathrm{Q}_2)$: Note that

$$(\mathrm{P} \Rightarrow \mathrm{Q}_1 \vee \mathrm{Q}_2) \;\Leftrightarrow\; \big[(\mathrm{P} \wedge \sim\mathrm{Q}_1) \Rightarrow \mathrm{Q}_2\big].$$

Example

If (x, y) is inside the circle $(x-6)^2 + (y-3)^3 = 8$, then $x > 4$ or $y > 1$.

Proof.

Suppose that (x, y) is inside the circle $(x-6)^2 + (y-3)^2 = 8$ and $x \leqslant 4$. Then $(x-6)^2 + (y-3)^2 < 8$ and $6 - x \geqslant 2$. Therefore,

$$(y-3)^2 < 8 - (6-x)^2 \leqslant 8 - 4 = 4$$

which implies that $|y-3| < 2$; thus $-2 < y - 3 < 2$ which further shows $1 < y < 5$. □

§1.8 Proofs from Number Theory

Theorem (The Division Algorithm)

For all integers a and b, with $a \neq 0$, there exist unique integer q and r such that $b = aq + r$ and $0 \leqslant r < |a|$.

1. The integer a is the **divisor** (除數), b is the **divident** (被除數), q is the **quotient** (商), and r is the **remainder** (餘數).
2. a is said to divide b if $b = aq$ for some integer q.
3. A **common divisor** (公因數) of nonzero integers a and b is an integer that divides both a and b.

§1.8 Proofs from Number Theory

Definition

Let a and b be non-zero integers. We say the integer d is the **greatest common divisor (gcd)** of a and b, and write $d = \gcd(a, b)$, if

1. d is a common divisor of a and b.
2. every common divisor c of a and b is not greater than d.

Theorem

Let a and b be non-zero integers. The gcd of a and b is the smallest positive linear combination of a and b; that is,

$$\gcd(a, b) = \min\{am + bn \,\big|\, am + bn > 0\,, \quad m, n \in \mathbb{Z}\}\,.$$

Proof.

Let $d = am + bn$ be the smallest positive linear combination of a and b. We show that d satisfies (1) and (2) in the definition of the greatest common divisor. □

§1.8 Proofs from Number Theory

Proof (Cont'd).

1. **First we show that d divides a.** By the Division Algorithm, there exist integers q and r such that $a = dq + r$, where $0 \leqslant r < d$. Then
$$r = a - dq = a - (am + bn)q = a(1 - m) + b(-nq)\,;$$
thus r is a linear combination of a and b. Since $0 \leqslant r < d$ and d is the smallest positive linear combination, we must have $r = 0$. Therefore, $a = dq$; thus d divides a. Similarly, d divides b (replacing a by b in the argument above); thus d is a common divisor of a and b.
2. **Next we show that all common divisors of a and b is not greater than d.** Let c be a common divisor of a and b. Then c divides d since $d = am + bn$. Therefore, $c \leqslant d$.

By (1) and (2), we find that $d = \gcd(a, b)$. □

§1.8 Proofs from Number Theory

Theorem (Euclid's Algorithm)

Let a and b be positive integers with $a \leqslant b$. Then there are two lists of positive integers $q_1, q_2, \cdots, q_{k-1}, q_k, q_{k+1}$ and $r_1, r_2, \cdots, r_{k-1}, r_k, r_{k+1}$ such that

1. $a > r_1 > r_2 > \cdots > r_{k-1} > r_k > r_{k+1} = 0.$
2. $b = aq_1 + r_1, \quad a = r_1q_2 + r_2, \quad r_1 = r_2q_3 + r_3, \quad \cdots\cdots,$
   $r_{k-3} = r_{k-2}q_{k-1} + r_{k-1}, \quad r_{k-2} = r_{k-1}q_k + r_k,$
   $r_{k-1} = r_kq_{k+1}$ (*that is,* $r_{k+1} = 0$).

Furthermore, $\gcd(a, b) = r_k$, *the last non-zero remainder in the list.*

§1.8 Proofs from Number Theory

Theorem (輾轉相除法)

Let a and b be positive integers with $a \leqslant b$. Then there are two lists of positive integers $q_1, q_2, \cdots, q_{k-1}, q_k, q_{k+1}$ and $r_1, r_2, \cdots, r_{k-1}, r_k, r_{k+1}$ such that

1. $a > r_1 > r_2 > \cdots > r_{k-1} > r_k > r_{k+1} = 0.$
2. $b = aq_1 + r_1, \quad a = r_1q_2 + r_2, \quad r_1 = r_2q_3 + r_3, \quad \cdots\cdots,$
   $r_{k-3} = r_{k-2}q_{k-1} + r_{k-1}, \quad r_{k-2} = r_{k-1}q_k + r_k,$
   $r_{k-1} = r_kq_{k+1}$ *(that is,* $r_{k+1} = 0$*).*

Furthermore, $\gcd(a, b) = r_k$*, the last non-zero remainder in the list.*

§1.8 Proofs from Number Theory

Proof of Euclid's Algorithm.

Let a and b be positive integers with $a \leqslant b$. By the Division Algorithm, there exists positive integer q_1 and non-negative integer r_1 such that $b = aq_1 + r_1$ and $0 \leqslant r_1 < a$. If $r_1 = 0$, the lists terminate; otherwise, for $0 < r_1 < a$, there exists positive integer q_2 and non-negative integer r_2 such that $a = r_1 q_2 + r_2$ and $0 \leqslant r_2 < r_1$. If $r_2 = 0$, the lists terminate; otherwise, for $0 < r_2 < r_1$, there exists positive integer q_3 and non-negative integer r_3 such that $r_1 = r_2 q_3 + r_3$ and $0 \leqslant r_3 < r_2$. □

§1.8 Proofs from Number Theory

Proof of Euclid's Algorithm (Cont'd).

Continuing in this fashion, we obtain a strictly decreasing sequence of non-negative integers $r_1, r_2, r_3, \cdots$. This lists must end, so there is an integer k such that $r_{k+1} = 0$. Thus we have

$$\begin{aligned} & r_0 \equiv a > r_1 > r_2 > \cdots > r_k > r_{k+1} = 0\,, \\ & r_{j-1} = r_j q_{j+1} + r_{j+1} \quad \text{for all } 1 \leqslant j \leqslant k\,, \\ & b = r_0 q_1 + r_1\,. \end{aligned}$$

We now show that $r_k = d \equiv \gcd(a, b)$.

1. The remainder r_k divides r_{k-1} since $r_{k-1} = r_k q_{k+1}$. Also, r_k divides r_{k-2} since
$$r_{k-2} = r_{k-1} q_k + r_k = r_k q_{k+1} q_k + r_k = r_k (q_k q_{k+1} + 1)\,.$$
Therefore, by the fact that $r_{j-1} = r_j q_{j+1} + r_{j+1}$ for all $1 \leqslant j \leqslant k$, we find that r_k divides r_j for all $0 \leqslant j \leqslant k-1$. □

§1.8 Proofs from Number Theory

Proof of Euclid's Algorithm (Cont'd).

Continuing in this fashion, we obtain a strictly decreasing sequence of non-negative integers $r_1, r_2, r_3, \cdots$. This lists must end, so there is an integer k such that $r_{k+1} = 0$. Thus we have

$$\begin{aligned} & r_0 \equiv a > r_1 > r_2 > \cdots > r_k > r_{k+1} = 0\,, \\ & r_{j-1} = r_j q_{j+1} + r_{j+1} \quad \text{for all } 1 \leqslant j \leqslant k\,, \\ & b = r_0 q_1 + r_1\,. \end{aligned}$$

We now show that $r_k = d \equiv \gcd(a, b)$.

1. The remainder r_k divides r_{k-1} since $r_{k-1} = r_k q_{k+1}$. Also, r_k divides r_{k-2} since
$$r_{k-2} = r_{k-1} q_k + r_k = r_k q_{k+1} q_k + r_k = r_k (q_k q_{k+1} + 1)\,.$$
Therefore, r_k divides linear combinations of r_j; thus r_k divides a (which is r_0) and b (which is $r_0 q_1 + r_1$). □

§1.8 Proofs from Number Theory

Proof of Euclid's Algorithm (Cont'd).

Continuing in this fashion, we obtain a strictly decreasing sequence of non-negative integers $r_1, r_2, r_3, \cdots$. This lists must end, so there is an integer k such that $r_{k+1} = 0$. Thus we have

$$\begin{aligned} & r_0 \equiv a > r_1 > r_2 > \cdots > r_k > r_{k+1} = 0\,, \\ & r_{j-1} = r_j q_{j+1} + r_{j+1} \quad \text{for all } 1 \leqslant j \leqslant k\,, \\ & b = r_0 q_1 + r_1\,. \end{aligned}$$

We now show that $r_k = d \equiv \gcd(a, b)$.

2. On the other hand, d divides r_1 since $r_1 = b - aq_1$. Also, d also divides r_2 since

$$r_2 = r_1 - aq_2 = b - aq_1 - aq_2 = b - a(q_1 + q_2)\,.$$

Therefore, by the fact that $r_{j+1} = r_{j-1} - r_j q_{j+1}$ for all $1 \leqslant j \leqslant k$, we find that d divides r_k for all $0 \leqslant j \leqslant k$. □

§1.8 Proofs from Number Theory

Proof of Euclid's Algorithm (Cont'd).

By (1), r_k is a common divisor of a and b. By (2), the greatest common divisor of a and b must divide r_k; thus we conclude that $r_k = \gcd(a, b)$. □

Example

Using Euclid's algorithm to compute the greatest common divisor of 12 and 32:

$$\begin{aligned} 32 &= 12 \times 2 + 8\,, \\ 12 &= 8 \times 1 + 4\,, \\ 8 &= 4 \times 2 + 0\,. \end{aligned}$$

Therefore, $4 = \gcd(12, 32)$. Moreover, by working backward,

$$4 = 12 - 8 \times 1 = 12 - (32 - 12 \times 2) \times 1 = 12 \times 3 + 32 \times (-1)\,.$$

§1.8 Proofs from Number Theory

Definition

We say that non-zero integers a and b are **relatively prime** (互質) or **coprime** if $\gcd(a, b) = 1$.

Lemma (Euclid's Lemma)

Let a, b and p be integers. If p is a prime and p divides ab, then p divides a or p divides b.

Proof.

Let a, b be integers, and p be a prime. Suppose that p divides ab, and p does not divides a. Then $\gcd(p, a) = 1$; thus there exist integers m and n such that $1 = am + pn$. Therefore, $b = abm + apn$. Since p divides ab, we conclude that p divides b (since b is a linear combination of ab and p). □

§1.8 Proofs from Number Theory

Remark: The same argument of showing Euclid's Lemma can be applied to shown a more general case:

Let a, b, p be integers such that p divides ab.

If $\gcd(a, p) = 1$, then p divides b.

Chapter 2. Sets and Induction

§2.1 Basic Concepts of Set Theory

Definition

A ***set*** is a collection of objects called ***elements*** or ***members*** of the set. To denote a set, we make a complete list $\{x_1, x_2, \cdots, x_N\}$ or use the notation

$$\{x : \mathrm{P}(x)\} \quad \text{or} \quad \{x \,|\, \mathrm{P}(x)\},$$

where the sentence $\mathrm{P}(x)$ describes the property that defines the set (the set $\{x \,|\, \mathrm{P}(x)\}$ is in fact the truth set of the open sentence $\mathrm{P}(x)$). A set A is said to be a ***subset*** of S if every member of A is also a member of S. We write $x \in A$ (or A contains x) if x is a member of A, write $x \notin A$ if x is not a member of A, and write $A \subseteq S$ (or S includes A) if A is a subset of S. The empty set, denoted $\varnothing$, is the set with no member.

§2.1 Basic Concepts of Set Theory

Example

The set $A = \{1, 3, 5, 7, 9, 11, 13\}$ may also be written as $\{x \,|\, x \in \mathbb{N}, x \text{ is odd, and } x < 14\}$ or $\{x \in \mathbb{N} \,|\, x \text{ is odd, and } x < 14\}$.

Remark:

1. Beware of the distinction between "is an element of" and "is a subset of". For example, let $A = \{1, \{2, 4\}, \{5\}, 8\}$. Then $4 \notin A$, $\{5\} \in A$, $\{1, \{5\}\} \subseteq A$ and $\{\{5\}\} \subseteq A$, but $\{5\} \nsubseteq A$.
2. Not all open sentences $\mathrm{P}(x)$ can be used to defined sets. For example, $\mathrm{P}(x) \equiv$ "x is a set" is not a valid open sentence to define sets for otherwise it will lead to the construction of a set which violates the axiom of regularity.

§2.1 Basic Concepts of Set Theory

- **Direct proof of** $A \subseteq B$: $(\forall\, x)\big[(x \in A) \Rightarrow (x \in B)\big]$.

Direct proof of $A \subseteq B$

Proof.

Let x be an element in A.

$\vdots$

Thus, $x \in B$.

Therefore, $A \subseteq B$. □

§2.1 Basic Concepts of Set Theory

- **Proof of $A \subseteq B$ by contraposition**: $\sim(x \in B) \Rightarrow \sim(x \in A)$.

Proof of $A \subseteq B$ by contraposiction

Proof.

Let x be an element.

Suppose that $x \notin B$; that is, x is not an element of B.

$\vdots$

Thus, $x \notin A$.

Therefore, $A \subseteq B$. □

§2.1 Basic Concepts of Set Theory

- **Proof of $A \subseteq B$ by contraposition**: $\sim(x \in B) \Rightarrow \sim(x \in A)$.

Proof of $A \subseteq B$ by contraposiction

Proof.

Let x be an element which does not belong to B.

~~Suppose that $x \notin B$; that is, x is not an element of B.~~

$\vdots$

Thus, $x \notin A$.

Therefore, $A \subseteq B$. □

§2.1 Basic Concepts of Set Theory

- **Proof of $A \subseteq B$ by contradiction**: $\sim(\exists\, x)\big[(x \in A) \wedge \sim(x \in B)\big]$.

Proof of $A \subseteq B$ by contradiction

Proof.

Assume that there exists $x \in A$ but $x \notin B$.

$$\vdots$$

Thus, $\mathrm{P} \wedge \sim \mathrm{P}$, a contradiction.

Therefore, $A \subseteq B$. □

§2.1 Basic Concepts of Set Theory

Theorem

1. *For every set A, $\varnothing \subseteq A$.*
2. *For every set A, $A \subseteq A$.*
3. *For all sets A, B and C, if $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.*

Proof.

1. Note that since there is no element in $\varnothing$, the open sentence $\mathrm{P}(x) \equiv \big[(x \in \varnothing) \Rightarrow (x \in A)\big]$ is always true (since the antecedent $(x \in \varnothing)$ is always false) for all x.
2. This follows from that the conditional sentence $\mathrm{P} \Rightarrow \mathrm{P}$ is a tautology (always true).
3. This follows from that
$$\big[(\mathrm{P} \Rightarrow \mathrm{Q}) \wedge (\mathrm{Q} \Rightarrow \mathrm{R})\big] \Rightarrow (\mathrm{P} \Rightarrow \mathrm{R}) . \qquad \square$$

§2.1 Basic Concepts of Set Theory

Definition

Two sets A and B are said to be ***equal***, denoted by $A = B$, if $(\forall x)(x \in A \Leftrightarrow x \in B)$; that is $(A \subseteq B) \wedge (B \subseteq A)$. A set B is said to be a ***proper subset*** of a set A, denoted by $B \subsetneq A$, if $B \subseteq A$ but $A \neq B$.

- **Proof of** $A = B$:

Two-part proof of $A = B$

Proof.

(i) Prove that $A \subseteq B$ (by any method.)

(ii) Prove that $B \subseteq A$ (by any method).

Therefore, $A = B$. □

§2.1 Basic Concepts of Set Theory

Theorem

If A and B are sets with no elements, then $A = B$.

Proof.

Let A, B be set. If A has no element, then $A = \varnothing$; thus by the fact that empty set is a subset of any set, $A \subseteq B$. Similarly, if B has no element, then $B \subseteq A$. □

Theorem

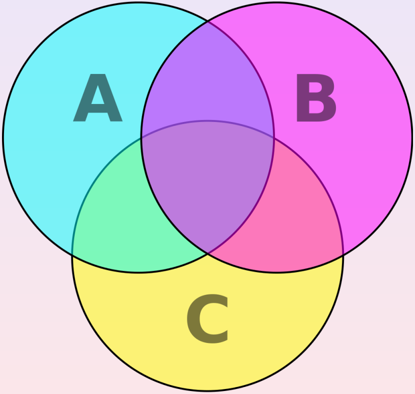
For any sets A and B, if $A \subseteq B$ and $A \neq \varnothing$, then $B \neq \varnothing$.

Proof.

Let A, B be sets, $A \subseteq B$, and $A \neq \varnothing$. Then there is an element x such that $x \in A$. By the assumption that $A \subseteq B$, we must have $x \in B$. Therefore, $B \neq \varnothing$. □

§2.1 Basic Concepts of Set Theory

- **Venn diagrams**:



§2.1 Basic Concepts of Set Theory

Definition

Let A be a set. The ***power set*** of A, denoted by $\mathcal{P}(A)$ or 2^A, is the colloection of all subsets of A. In other words, $\mathcal{P}(A) \equiv \big\{B \,\big|\, B \subseteq A\big\}$.

Example

If $A = \{a, b, c, d\}$, then

$$\mathcal{P}(A) = \Big\{\varnothing, \{a\}, \{b\}, \{c\}, \{d\}, \{a, b\}, \{a, c\}, \{a, d\}, \{b, c\}, \{b, d\}, \\ \{c, d\}, \{a, b, c\}, \{a, b, d\}, \{a, c, d\}, \{b, c, d\}, \{a, b, c, d\}\Big\}.$$

We note that $\#(A) = 4$ and $\#(\mathcal{P}(A)) = 16 = 2^{\#(A)}$.

§2.1 Basic Concepts of Set Theory

Theorem

If A is a set with n elements, then $\mathcal{P}(A)$ is a set with 2^n elements.

Proof.

Suppose that A is a set with n elements.

1. If $n = 0$, then $A = \varnothing$; thus $\mathcal{P}(A) = \{\varnothing\}$ which shows that $\mathcal{P}(A)$ has $2^0 = 1$ element.
2. If $n \geqslant 1$, we write A as $\{x_1, x_2, \cdots, x_n\}$. To describe a subset B of A, we need to know for each $1 \leqslant i \leqslant n$ whether x_i is in B. For each x_i, there are two possibilities (either $x_i \in B$ or $x_i \notin B$). Thus, there are exactly 2^n different ways of making a subset of A. Therefore, $\mathcal{P}(A)$ has 2^n elements. □

§2.1 Basic Concepts of Set Theory

Theorem

Let A, B be sets. Then $A \subseteq B$ if and only if $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.

Proof.

Let A, B be sets.

($\Rightarrow$) Suppose that $A \subseteq B$ and $C \in \mathcal{P}(A)$. Then C is a subset of A; thus the fact that $A \subseteq B$ implies that $C \subseteq B$. Therefore, $C \in \mathcal{P}(B)$.

($\Leftarrow$) Suppose that $A \nsubseteq B$. Then there exists $x \in A$ but $x \notin B$. Then $\{x\} \subseteq A$ but $\{x\} \nsubseteq B$ which shows that $\mathcal{P}(A) \nsubseteq \mathcal{P}(B)$. □

§2.2 Set Operations

Definition

Let A and B be sets.

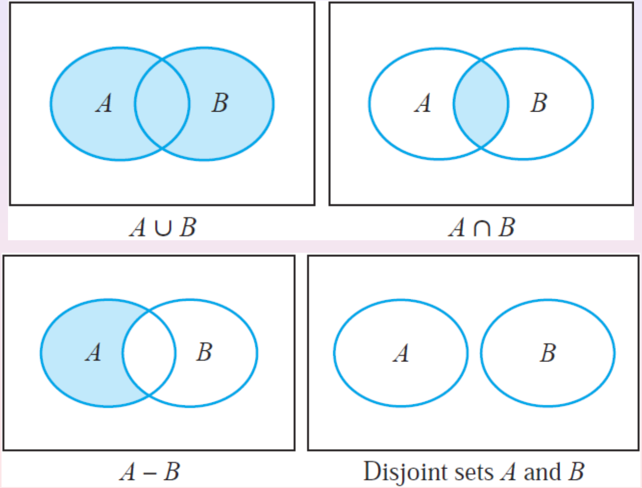
1. The **union of** A **and** B, denoted by $A \cup B$, is the set
$$\left\{x \,\middle|\, (x \in A) \vee (x \in B)\right\}.$$
2. The **intersection of** A **and** B, denoted by $A \cap B$, is the set
$$\left\{x \,\middle|\, (x \in A) \wedge (x \in B)\right\}.$$
3. The **difference of** A **and** B, denoted by $A - B$, is the set
$$\left\{x \,\middle|\, (x \in A) \wedge (x \notin B)\right\}.$$

Definition

Two sets A and B are said to be ***disjoint*** if $A \cap B = \varnothing$.

§2.2 Set Operations

- Venn diagrams:



$A \cup B$

$A \cap B$

$A - B$

Disjoint sets A and B

§2.2 Set Operations

Theorem

Let A, B and C be sets. Then

(a) $A \subseteq A \cup B$; (b) $A \cap B \subseteq A$; (c) $A \cap \varnothing = \varnothing$; (d) $A \cup \varnothing = A$;

(e) $A \cap A = A$; (f) $A \cup A = A$; (g) $A \backslash \varnothing = A$; (h) $\varnothing \backslash A = \varnothing$;

$$\left.\begin{array}{l} \text{(i) } A \cup B = B \cup A; \\ \text{(j) } A \cap B = B \cap A; \end{array}\right\} \quad \textbf{(commutative laws)}$$

$$\left.\begin{array}{l} \text{(k) } A \cup (B \cup C) = (A \cup B) \cup C; \\ (\ell) \ A \cap (B \cap C) = (A \cap B) \cap C; \end{array}\right\} \quad \textbf{(associative laws)}$$

$$\left.\begin{array}{l} \text{(m) } A \cap (B \cup C) = (A \cap B) \cup (A \cap C); \\ \text{(n) } A \cup (B \cap C) = (A \cup B) \cap (A \cup C); \end{array}\right\} \quad \textbf{(distributive laws)}$$

(o) $A \subseteq B \Leftrightarrow A \cup B = B$; (p) $A \subseteq B \Leftrightarrow A \cap B = A$;

(q) $A \subseteq B \Rightarrow A \cup C \subseteq B \cup C$; (r) $A \subseteq B \Rightarrow A \cap C \subseteq B \cap C$.

Note: $(A \cup B) \cap C \neq A \cup (B \cap C)$ in general!

§2.2 Set Operations

Proof of (m) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

Let x be an element in the universe, and P, Q and R denote the propositions $x \in A$, $x \in B$ and $x \in C$, respectively. Note that from the truth table, we conclude that

$$\mathrm{P} \wedge (\mathrm{Q} \vee \mathrm{R}) \Leftrightarrow \big[(\mathrm{P} \wedge \mathrm{Q}) \vee (\mathrm{P} \wedge \mathrm{R})\big],$$

1. Let $x \in A \cap (B \cup C)$. Then $x \in A$ and $x \in B \cup C$; thus the proposition $\mathrm{P} \wedge (\mathrm{Q} \vee \mathrm{R})$ is true. Therefore, the proposition $\big[(\mathrm{P} \wedge \mathrm{Q}) \vee (\mathrm{P} \wedge \mathrm{R})\big]$ is also true which implies that $x \in A \cap B$ or $x \in A \cap C$; thus
$$A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C).$$
2. Working conversely, we find that if $x \in A \cap B$ or $x \in A \cap C$, then $x \in A \cap (B \cup C)$. Therefore,
$$(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C).$$

□

§2.2 Set Operations

Proof of (m) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

Let $x \in A \cap (B \cup C)$. Then $x \in A$ and $x \in B \cup C$. Thus,

1. if $x \in B$, then $x \in A \cap B$.
2. if $x \in C$, then $x \in A \cap C$.

Therefore, $x \in A \cap B$ or $x \in A \cap C$ which shows $x \in (A \cap B) \cup (A \cap C)$; thus we establish that

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

On the other hand, suppose that $x \in (A \cap B) \cup (A \cap C)$.

1. if $x \in A \cap B$, then $x \in A$ and $x \in B$.
2. if $x \in A \cap C$, then $x \in A$ and $x \in C$.

In either cases, $x \in A$; thus if $x \in (A \cap B) \cup (A \cap C)$, then $x \in A$ but at the same time $x \in B$ or $x \in C$. Thus, $x \in A$ and $x \in B \cup C$ which shows that $x \in A \cap (B \cup C)$. Therefore,

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

□

§2.2 Set Operations

Proof of (p) $A \subseteq B \Leftrightarrow A \cap B = A$.

($\Rightarrow$) Suppose that $A \subseteq B$. Let x be an element in A. Then $x \in B$ since $A \subseteq B$; thus $x \in A \cap B$ which implies that $A \subseteq A \cap B$. On the other hand, it is clear that $A \cap B \subseteq A$, so we conclude that $A \cap B = A$.

($\Leftarrow$) Suppose that $A \cap B = A$. Let x be an element in A. Then $x \in A \cap B$ which shows that $x \in B$. Therefore, $A \subseteq B$. □

§2.2 Set Operations

Definition

Let U be the universe and $A \subseteq U$. The ***complement*** (補集) of A, denoted by $A^{\complement}$, is the set $U - A$.

Theorem

Let U be the universe, and $A, B \subseteq U$. Then

(a) $(A^{\complement})^{\complement} = A$. (b) $A \cup A^{\complement} = U$.

(c) $A \cap A^{\complement} = \varnothing$. (d) $A - B = A \cap B^{\complement}$.

(e) $A \subseteq B$ *if and only if* $B^{\complement} \subseteq A^{\complement}$.

(f) $A \cap B = \varnothing$ *if and only if* $A \subseteq B^{\complement}$

$$\left.\begin{array}{l} \text{(g) } (A \cup B)^{\complement} = A^{\complement} \cap B^{\complement}. \\ \text{(h) } (A \cap B)^{\complement} = A^{\complement} \cup B^{\complement}. \end{array}\right\} \quad \textbf{(De Morgan's Law)}$$

§2.2 Set Operations

Proof of (a) $(A^\complement)^\complement = A$.

By the definition of the complement, $x \in (A^\complement)^\complement$ if and only if $x \notin A^\complement$ if and only if $x \in A$. □

Proof of (e) $A \subseteq B \Leftrightarrow B^\complement \subseteq A^\complement$.

By the equivalence of $\mathrm{P} \Rightarrow \mathrm{Q}$ and $\sim\mathrm{Q} \Rightarrow \sim\mathrm{P}$, we conclude that

$$(\forall\, x)\big[(x \in A) \Rightarrow (x \in B)\big] \quad \Leftrightarrow \quad (\forall\, x)\big[(x \notin B) \Rightarrow (x \notin A)\big]$$

and the bi-directional statement is identical to that

$$A \subseteq B \Leftrightarrow B^\complement \subseteq A^\complement\,.$$

□

Alternative proof of (e) $A \subseteq B \Leftrightarrow B^\complement \subseteq A^\complement$.

Using (a), it suffices to show that $A \subseteq B \Rightarrow B^\complement \subseteq A^\complement$. Suppose that $A \subseteq B$, but $B^\complement \nsubseteq A^\complement$. Then there exists $x \in B^\complement$ and $x \in A$; however, by the fact that $A \subseteq B$, x has to belong to B, a contradiction. □

§2.2 Set Operations

Proof of (g) $(A \cup B)^{\complement} = A^{\complement} \cap B^{\complement}$.

By the equivalence of $\sim(\mathrm{P} \vee \mathrm{Q})$ and $(\sim\mathrm{P}) \wedge (\sim\mathrm{Q})$, we find that

$$(\forall\, x) \sim \big[(x \in A) \vee (x \in B)\big] \quad \Leftrightarrow \quad (\forall\, x)\big[(x \notin A) \wedge (x \notin B)\big]$$

and the bi-directional statement is identical to that

$$(A \cup B)^{\complement} = A^{\complement} \cap B^{\complement}\,. \qquad \square$$

Alternative proof of (g) $(A \cup B)^{\complement} = A^{\complement} \cap B^{\complement}$.

Let x be an element in the universe.

$$\begin{aligned} x \in (A \cup B)^{\complement} &\text{ if and only if } x \notin A \cup B \\ &\text{ if and only if it is not the case that } x \in A \text{ or } x \in B \\ &\text{ if and only if } x \notin A \text{ and } x \notin B \\ &\text{ if and only if } x \in A^{\complement} \text{ and } x \in B^{\complement} \\ &\text{ if and only if } x \in A^{\complement} \cap B^{\complement}\,. \end{aligned} \qquad \square$$

§2.2 Set Operations

Definition

An ***ordered pair*** (a, b) is an object formed from two objects a and b, where a is called the ***first coordinate*** and b the ***second coordinate***. Two ordered pairs are equal whenever their corresponding coordinates are the same.

An ***ordered n-tuples*** $(a_1, a_2, \cdots, a_n)$ is an object formed from n objects a_1, a_2, $\cdots$, a_n, where a_j is called the j-th coordinate. Two n-tuples $(a_1, a_2, \cdots, a_n)$, $(c_1, c_2, \cdots, c_n)$ are equal if $a_i = c_i$ for $i \in \{1, 2, \cdots, n\}$.

Definition

Let A and B be sets. The product of A and B, denoted by $A \times B$, is

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

The product of three or more sets are defined similarly.

§2.2 Set Operations

Example

Let $A = \{1, 3, 5\}$ and $B = \{\star, \diamond\}$. Then

$$A \times B = \{(1, \star), (3, \star), (5, \star), (1, \diamond), (3, \diamond), (5, \diamond)\}.$$

Theorem

If A, B, C and D are sets, then

(a) $A \times (B \cup C) = (A \times B) \cup (A \times C)$.

(b) $A \times (B \cap C) = (A \times B) \cap (A \times C)$.

(c) $A \times \varnothing = \varnothing$.

(d) $(A \times B) \cap (C \times D) = (A \cap C) \times (B \cap D)$.

(e) $(A \times B) \cup (C \times D) \subseteq (A \cup C) \times (B \cup D)$.

(f) $(A \times B) \cap (B \times A) = (A \cap B) \times (A \cap B)$.

§2.3 Indexed Family of Sets

Definition

Let $\mathcal{F}$ be a family of sets.

1. The ***union*** of the family $\mathcal{F}$ or the ***union*** over $\mathcal{F}$, denoted by $\bigcup\limits_{A\in\mathcal{F}} A$, is the set $\left\{x \,\middle|\, x \in A \text{ for some } A \in \mathcal{F}\right\}$. Therefore,
$$x \in \bigcup_{A\in\mathcal{F}} A \quad \text{if and only if} \quad (\exists\, A \in \mathcal{F})(x \in A).$$
2. The ***intersection*** of the family $\mathcal{F}$ or the ***intersection*** over $\mathcal{F}$, denoted by $\bigcap\limits_{A\in\mathcal{F}} A$, is the set $\left\{x \,\middle|\, x \in A \text{ for all } A \in \mathcal{F}\right\}$. Therefore,
$$x \in \bigcap_{A\in\mathcal{F}} A \quad \text{if and only if} \quad (\forall\, A \in \mathcal{F})(x \in A).$$

§2.3 Indexed Family of Sets

Example

Let $\mathcal{F}$ be the collection of sets given by

$$\mathcal{F} = \left\{ \left[\frac{1}{n}, 2 - \frac{1}{n}\right] \,\middle|\, n \in \mathbb{N} \right\}.$$

Then $\bigcup\limits_{A \in \mathcal{F}} A = (0,2)$ and $\bigcap\limits_{A \in \mathcal{F}} A = \{1\}$. We also write $\bigcup\limits_{A \in \mathcal{F}} A$ and $\bigcap\limits_{A \in \mathcal{F}} A$ as $\bigcup\limits_{n=1}^{\infty} \left[\frac{1}{n}, 2 - \frac{1}{n}\right]$ and $\bigcap\limits_{n=1}^{\infty} \left[\frac{1}{n}, 2 - \frac{1}{n}\right]$, respectively.

Example

Let $\mathcal{F}$ be the collection of sets given by

$$\mathcal{F} = \left\{ \left(-\frac{1}{n}, 2 + \frac{1}{n}\right) \,\middle|\, n \in \mathbb{N} \right\}.$$

Then $\bigcup\limits_{A \in \mathcal{F}} A = (-1,3)$ and $\bigcap\limits_{A \in \mathcal{F}} A = [0,2]$. We also write $\bigcup\limits_{A \in \mathcal{F}} A$ and $\bigcap\limits_{A \in \mathcal{F}} A$ as $\bigcup\limits_{n=1}^{\infty} \left(-\frac{1}{n}, 2 + \frac{1}{n}\right)$ and $\bigcap\limits_{n=1}^{\infty} \left(-\frac{1}{n}, 2 + \frac{1}{n}\right)$, respectively.

§2.3 Indexed Family of Sets

Theorem

Let $\mathcal{F}$ be a family of sets.

(a) *For every set B in the family $\mathcal{F}$,* $\bigcap\limits_{A\in\mathcal{F}} A \subseteq B$.

(b) *For every set B in the family $\mathcal{F}$,* $B \subseteq \bigcup\limits_{A\in\mathcal{F}} A$.

(c) *If the family $\mathcal{F}$ is non-empty, then* $\bigcap\limits_{A\in\mathcal{F}} A \subseteq \bigcup\limits_{A\in\mathcal{F}} A$.

$$\left.\begin{array}{l} \text{(d) } \Big(\bigcap\limits_{A\in\mathcal{F}} A\Big)^{\complement} = \bigcup\limits_{A\in\mathcal{F}} A^{\complement}. \\ \text{(e) } \Big(\bigcup\limits_{A\in\mathcal{F}} A\Big)^{\complement} = \bigcap\limits_{A\in\mathcal{F}} A^{\complement}. \end{array}\right\} \quad \textbf{(De Morgan's Law)}$$

§2.3 Indexed Family of Sets

Proof of (d) $\Big(\bigcap\limits_{A\in\mathcal{F}} A\Big)^{\complement} = \bigcup\limits_{A\in\mathcal{F}} A^{\complement}$.

Let x be an element in the universe. Then

$$\begin{aligned} x \in \Big(\bigcap_{A\in\mathcal{F}} A\Big)^{\complement} &\text{ if and only if } x \notin \bigcap_{A\in\mathcal{F}} A \\ &\text{ if and only if } \sim\Big(x \in \bigcap_{A\in\mathcal{F}} A\Big) \\ &\text{ if and only if } \sim(\forall\, A \in \mathcal{F})(x \in A) \\ &\text{ if and only if } (\exists\, A \in \mathcal{F}) \sim (x \in A) \\ &\text{ if and only if } (\exists\, A \in \mathcal{F})(x \notin A) \\ &\text{ if and only if } (\exists\, A \in \mathcal{F})(x \in A^{\complement}) \\ &\text{ if and only if } x \in \bigcup_{A\in\mathcal{F}} A^{\complement}. \end{aligned}$$

□

§2.3 Indexed Family of Sets

Theorem

Let $\mathscr{F}$ be a non-empty family of sets and B a set.

1. *If $B \subseteq A$ for all $A \in \mathscr{F}$, then $B \subseteq \bigcap_{A \in \mathscr{F}} A$.*
2. *If $A \subseteq B$ for all $A \in \mathscr{F}$, then $\bigcup_{A \in \mathscr{F}} A \subseteq B$.*

Proof.

1. Suppose that $B \subseteq A$ for all $A \in \mathscr{F}$, and $x \in B$. Then $x \in A$ for all $A \in \mathscr{F}$. Therefore, $(\forall A \in \mathscr{F})(x \in A)$ or equivalently, $x \in \bigcap_{A \in \mathscr{F}} A$.
2. Suppose that $A \subseteq B$ for all $A \in \mathscr{F}$, and $x \in \bigcup_{A \in \mathscr{F}} A$.Then $x \in A$ for some $A \in \mathscr{F}$. By the fact that $A \subseteq B$, we find that $x \in B$. □

§2.3 Indexed Family of Sets

Example

Let $\mathcal{F} = \left\{[-r, r^2+1) \,\middle|\, r \in \mathbb{R} \text{ and } r \geqslant 0\right\}$. Then $\bigcup\limits_{A\in\mathcal{F}} A = \mathbb{R}$ and $\bigcap\limits_{A\in\mathcal{F}} = [0,1)$. $\Big($We also write $\bigcup\limits_{A\in\mathcal{F}} A$ and $\bigcap\limits_{A\in\mathcal{F}} A$ as $\bigcup\limits_{r\geqslant 0}[-r, r^2+1)$ and $\bigcap\limits_{r\geqslant 0}[-r, r^2+1)$, respectively.$\Big)$

Proof.

1. If $x \in \mathbb{R}$, then $x \in [-r, r^2+1)$ with $r = |x|$ since$-|x| \leqslant x \leqslant x^2+1$. Therefore, $\mathbb{R} \subseteq \bigcup\limits_{A\in\mathcal{F}} A$.
2. If $x \in [0,1)$, then $x \in [-r, r^2+1)$ for all $r \geqslant 0$; thus $[0,1) \subseteq \bigcap\limits_{A\in\mathcal{F}} A$. If $x \in \bigcap\limits_{A\in\mathcal{F}} A$, then $x \in [-r, r^2+1)$ for all $r \geqslant 0$; thus $x \geqslant -r$ and $x < r^2+1$ for all $r \geqslant 0$. In particular, $x \geqslant 0$ and $x < 1$.

□

§2.3 Indexed Family of Sets

Definition

Let Δ be a non-empty set such that for each $\alpha \in \Delta$ there is a corresponding set A_α. The family $\{A_\alpha \,|\, \alpha \in \Delta\}$ is an ***indexed family*** of sets, and Δ is called the ***indexing set*** of this family and each $\alpha \in \Delta$ is called an ***index***.

Remark:

1. The indexing set of an indexed family of sets may be finite or infinite, the member sets need not have the same number of elements, and different indices need not correspond to different sets in the family.
2. If $\mathcal{F} = \{A_\alpha \,|\, \alpha \in \Delta\}$ is an indexed family of sets, we also write $\bigcup\limits_{A \in \mathcal{F}} A$ as $\bigcup\limits_{\alpha \in \Delta} A_\alpha$ and write $\bigcap\limits_{A \in \mathcal{F}} A$ as $\bigcap\limits_{\alpha \in \Delta} A_\alpha$.

§2.3 Indexed Family of Sets

3. Another way for the union and intersection of indexed family of sets whose indexing set is $\mathbb{N}$ is
$$\bigcup_{n\in\mathbb{N}} A_n = \bigcup_{n=1}^{\infty} A_n \quad \text{and} \quad \bigcap_{n\in\mathbb{N}} A_n = \bigcap_{n=1}^{\infty} A_n\,.$$
Also, the union and intersection of sets $A_4, A_5, A_6, \cdots, A_{100}$ can be written as
$$\bigcup_{4\leqslant n\leqslant 100} A_n = \bigcup_{n=4}^{100} A_n \quad \text{and} \quad \bigcap_{4\leqslant n\leqslant 100} A_n = \bigcap_{n=4}^{100} A_n$$
and etc.

Definition

The indexed family $\mathcal{F} = \{A_\alpha \mid \alpha \in \Delta\}$ of sets is said to be ***pairwise disjoint*** if for all $\alpha, \beta \in \Delta$, either $A_\alpha = A_\beta$ or $A_\alpha \cap A_\beta = \varnothing$.

§2.4 Mathematical Induction

- **Peano's Axiom for natural numbers**:

1. 1 is a natural number.
2. Every natural number has a unique successor which is a natural number ($+1$ is defined on natural numbers).
3. No two natural numbers have the same successor ($n+1 = m+1$ implies $n = m$).
4. 1 is not a successor for any natural number (1 is the "smallest" natural number).
5. If a property is possessed by 1 and is possessed by the successor of every natural number that possesses it, then the property is possessed by all natural numbers. (如果某個被自然數 1 所擁有的性質，也被其它擁有這個性質的自然數的下一個自然數所擁有，那麼所有的自然數都會擁有這個性質)

§2.4 Mathematical Induction

- **Principle of Mathematical Induction (PMI)**:

If $S \subseteq \mathbb{N}$ has the property that

1. $1 \in S$, and
2. $n+1 \in S$ whenever $n \in S$,

then $S = \mathbb{N}$.

Definition

A set S of natural numbers is called ***inductive*** if it has the property that whenever $n \in S$, then $n+1 \in S$.

PMI can be rephrased as "if S is an inductive set and $1 \in S$, then $S = \mathbb{N}$".

§2.4 Mathematical Induction

- **Inductive definition**: Inductive definition is a way to define some "functions" $f(n)$ for all natural numbers n. It is done by describe the first object $f(1)$, and then the $(n+1)$-th object $f(n+1)$ is defined in terms of the n-th object $f(n)$. We remark that in this way of defining f, **PMI** ensures that the collection of all n for which the corresponding object $f(n)$ is defined is $\mathbb{N}$.

Example

The **factorial** $n!$ can be defined by

1. $1! = 1$;
2. For all $n \in \mathbb{N}$, $(n+1)! = n! \times (n+1)$.

Note: one can extend the definition of the factorial function by defining $0! = 1$.

§2.4 Mathematical Induction

Example

The notation $\sum_{k=1}^{n} x_k$ can be defined by

1. $\sum_{k=1}^{1} x_k = x_1$;
2. For all $n \in \mathbb{N}$, $\sum_{k=1}^{n+1} x_k = \sum_{k=1}^{n} x_k + x_{n+1}$.

Example

The notation $\prod_{k=1}^{n} x_k$ can be defined by

1. $\prod_{k=1}^{1} x_k = x_1$;
2. For all $n \in \mathbb{N}$, $\prod_{k=1}^{n+1} x_k = \Big(\prod_{k=1}^{n} x_k \Big) \cdot x_{n+1}$.

§2.4 Mathematical Induction

PMI can provide a powerful method for proving statements that are true for all natural numbers.

Suppose that $\mathrm{P}(n)$ is an open sentence concerning the natural numbers.

Proof of $(\forall\, n \in \mathbb{N})\mathrm{P}(n)$ by mathematical induction

Proof.

Let S denote the truth of P.

(i) **Basis Step**. Show that $1 \in S$.

(ii) **Inductive Step**. Show that S is inductive by showing that if $n \in S$, then $n + 1 \in S$.

Therefore, **PMI** ensures that the truth set of P is $\mathbb{N}$. □

§2.4 Mathematical Induction

PMI can provide a powerful method for proving statements that are true for all natural numbers.

Suppose that $\mathrm{P}(n)$ is an open sentence concerning the natural numbers.

Proof of $(\forall\, n \in \mathbb{N})\mathrm{P}(n)$ by mathematical induction

Proof.

(i) **Basis Step**. Show that $\mathrm{P}(1)$ is true.

(ii) **Inductive Step**. Suppose that $\mathrm{P}(n)$ is true.

$$\vdots$$

Therefore, $\mathrm{P}(n+1)$ is true.

Therefore, **PMI** ensures that $(\forall\, n \in \mathbb{N})\mathrm{P}(n)$ is true. □

§2.4 Mathematical Induction

Example

Prove that for every natural number n,

$$1 + 3 + 5 + \cdots + (2n - 1) = n^2 .$$

Proof.

Let $\mathrm{P}(n)$ be the open sentence $1 + 3 + 5 + \cdots + (2n - 1) = n^2$.

1. $\mathrm{P}(1)$ is true since $1 = 1^2$.
2. Suppose that $\mathrm{P}(n)$ is true. Then

   $$1+3+5+\cdots+(2n-1)+(2n+1) = n^2+(2n+1) = (n+1)^2$$

   which shows that $\mathrm{P}(n+1)$ is true.

Therefore, **PMI** ensures that $(\forall\, n \in \mathbb{N})\mathrm{P}(n)$ is true. □

§2.4 Mathematical Induction

Example (De Moivre's formula)

Let θ be a real number. Prove that for every $n \in \mathbb{N}$,

$$(\cos\theta + i\sin\theta)^n = \cos(n\theta) + i\sin(n\theta)\,.$$

Proof.

Let $\mathrm{P}(n)$ be the open sentence $(\cos\theta+i\sin\theta)^n = \cos(n\theta)+i\sin(n\theta)$.

1. Obviously $\mathrm{P}(1)$ is true.
2. Suppose that $\mathrm{P}(n)$ is true. Then

$$\begin{aligned}(\cos\theta + i\sin\theta)^{n+1} &= \big[\cos(n\theta) + i\sin(n\theta)\big]\cdot(\cos\theta + i\sin\theta)\\ &= \big[\cos(n\theta)\cos\theta - \sin(n\theta)\sin\theta\big]\\ &\quad + i\big[\cos(n\theta)\sin\theta + \sin(n\theta)\cos\theta\big]\\ &= \cos(n+1)\theta + i\sin(n+1)\theta\end{aligned}$$

which shows that $\mathrm{P}(n+1)$ is true.

Therefore, **PMI** ensures that $(\forall\, n \in \mathbb{N})\mathrm{P}(n)$ is true. □

§2.4 Mathematical Induction

Example (Archimedean Principle for $\mathbb{N}$)

For any natural numbers a and b, there exists a natural number s such that $sb > a$.

Proof.

Let b be a fixed natural number, and $\mathrm{P}(a)$ be the open sentence

$$(\exists\, s \in \mathbb{N})(sb > a)\,.$$

1. If $a = 1$, then $2b > 1$; thus $\mathrm{P}(1)$ is true.
2. Suppose that $\mathrm{P}(n)$ is true. Then there exists $t \in \mathbb{N}$ such that $tb > n$. Then $(t+1)b = tb + b > n + 1$; thus $\mathrm{P}(n+1)$ is true.

Therefore, **PMI** ensures that $(\forall\, n \in \mathbb{N})\mathrm{P}(n)$ is true. □

§2.4 Mathematical Induction

- **Generalized Principle of Mathematical Induction (GPMI)**:

If $S \subseteq \mathbb{Z}$ has the property that

1. $k \in S$, and
2. $n+1 \in S$ whenever $n \in S$,

then S contains all integers greater than or equal to k.

Reason: Let $T = \{n \in \mathbb{N} \mid k+n-1 \in S\}$. Then $T \subseteq \mathbb{N}$. Moreover,

1. $1 \in T$ since $k \in S$ if and only if $1 \in T$.
2. If $n \in T$, then $k+n-1 \in S$; thus $k+n \in S$ which implies that $n+1 \in T$.

Therefore, **PMI** ensures that $T = \mathbb{N}$ which shows that

$$S = \{n \in \mathbb{Z} \mid n \geqslant k\}.$$

§2.4 Mathematical Induction

Example

Prove by induction that $n^2 - n - 20 > 0$ for all natural number $n > 5$.

Proof.

Let $S = \left\{ n \in \mathbb{N} \,\middle|\, n^2 - n - 20 > 0 \right\}$.

1. $6 \in S$ since $6^2 - 6 - 20 = 10 > 0$.
2. Suppose that $n \in S$. Then

$$\begin{aligned}(n+1)^2 - (n+1) - 20 &= n^2 + 2n + 1 - n - 1 - 20 \\ &> 2n > 0\,.\end{aligned}$$

Therefore, **GPMI** ensures that $S = \left\{ n \in \mathbb{N} \,\middle|\, n \geqslant 6 \right\}$. □

§2.5 Equivalent Forms of Induction

There are two other versions of mathematical induction.

1. **Well-Ordering Principle (WOP)**:

   Every nonempty subset of $\mathbb{N}$ has a smallest element.

2. **Principle of Complete Induction (PCI)**:

   Suppose S is a subset of $\mathbb{N}$ with the property:

   for all natural number n, if $\{1, 2, \cdots, n-1\} \subseteq S$, then $n \in S$.

   Then $S = \mathbb{N}$.

We remark here that in the statement of **PCI** we treat $\{1, 2, \cdots, 0\}$ as $\varnothing$.

Remark:

Similar to **GPMI**, **PCI** can be extended to a more general case stated as follows:

> Suppose S is a subset of $\mathbb{N}$ with the property:
>
> there exists $k \in \mathbb{Z}$ such that for all natural number n, if $\{k, k+1, \cdots, k+n-2\} \subseteq S$, then $k+n-1 \in S$.
>
> Then $S = \{n \in \mathbb{Z} \mid n \geqslant k\}$.

The same as the case of **PCI**, here we treat $\{k, k+1, \cdots, k-1\}$ as the empty set.

In the following, we prove that **PMI** ⇒ **WOP** ⇒ **PCI** ⇒ **PMI**.

§2.5 Equivalent Forms of Induction

Proof of PMI ⇒ WOP.

Assume the contrary that there exists a **non-empty** set $S \subseteq \mathbb{N}$ such that S does not have the smallest element. Define $T = \mathbb{N} \backslash S$, and $T_0 = \{n \in \mathbb{N} \mid \{1, 2, \cdots, n\} \subseteq T\}$ (T 中從 1 開始數起不需跳號就可以數到的數字). Then we have $T_0 \subseteq T$. Also note that $1 \notin S$ for otherwise 1 is the smallest element in S, so $1 \in T$ (thus $1 \in T_0$).

Assume $k \in T_0$. Since $\{1, 2, \cdots, k\} \subseteq T$, $1, 2, \cdots k \notin S$. If $k+1 \in S$, then $k+1$ is the smallest element in S. Since we assume that S does not have the smallest element, $k+1 \notin S$; thus $k+1 \in T \Rightarrow k+1 \in T_0$.

Therefore, by **PMI** we conclude that $T_0 = \mathbb{N}$; thus $T = \mathbb{N}$ which further implies that $S = \varnothing$, a contradiction. □

§2.5 Equivalent Forms of Induction

Proof of WOP $\Rightarrow$ PCI.

Assume the contrary that for some $S \neq \mathbb{N}$, S has the property

$$\text{for all natural number } n, \text{ if } \{1,2,\cdots,n-1\} \subseteq S, \text{ then } n \in S. \quad (\star)$$

Define $T = \mathbb{N} \backslash S$. Then T is a **non-empty** subset of $\mathbb{N}$; thus **WOP** implies that T has a smallest element k. Then $1,2,\cdots,k-1 \notin T$ which is the same as saying that $\{1,2,\cdots,k-1\} \subseteq S$. By property $(\star)$, $k \in S$ which implies that $k \notin T$, a contradiction. □

§2.5 Equivalent Forms of Induction

Proof of PCI $\Rightarrow$ PMI.

Let $S \subseteq \mathbb{N}$ has the property

(a) $1 \in S$, and (b) $n+1 \in S$ whenever $n \in S$.

We show that $S = \mathbb{N}$ by verifying that

for all natural number n, if $\{1, 2, \cdots, n-1\} \subseteq S$, then $n \in S$.

1. (a) implies $1 \in S$; thus the statement "$\{1, 2, \cdots, k-1\} = \varnothing \subseteq S \Rightarrow 1 \in S$" is true.
2. Suppose that $\{1, 2, \cdots, k-1\} \subseteq S$. Then $k-1 \in S$. Using (b) we find that $k \in S$; thus the statement "$\{1, 2, \cdots, k-1\} \subseteq S \Rightarrow k \in S$" is also true.

Therefore, S has property $(\star)$ and **PCI** implies that $S = \mathbb{N}$. □

§2.5 Equivalent Forms of Induction

Theorem (Fundamental Theorem of Arithmetic)

Every natural number greater than 1 is prime or can be expressed uniquely as a product of primes.

The meaning of the unique way to express a composite number as a product of primes:

Let m be a composite number. Then there is a unique way of writing m in the form

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n} ,$$

where $p_1 < p_2 < \cdots < p_n$ are primes and $\alpha_1, \alpha_2, \cdots, \alpha_n$ are natural numbers.

§2.5 Equivalent Forms of Induction

Proof based on **WOP**.

We first show that every natural number greater than 1 is either a prime or a products of primes, then show that the prime factor decomposition, when it is not prime, is unique.

1. Suppose that there is at least one natural number that is greater than 1, not a prime, and cannot be written as a product of primes. Then the set S of such numbers is non-empty, so **WOP** implies that S has a smallest element m. Since m is not a prime, $m = st$ for some natural numbers s and t that are greater than 1 and less than m. Both s and t are less than the smallest element of S, so they are not in S. Therefore, each of s and t is a prime or is the product of primes, which makes m a product of primes, a contradiction. □

§2.5 Equivalent Forms of Induction

Proof based on WOP (Cont'd).

2. Suppose that there exist natural numbers that can be expressed in two or more different ways as the product of primes, and let n be the smallest such number (the existence of such a number is guaranteed by **WOP**). Then

$$n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_m$$

for some $k, m \in \mathbb{N}$, where each p_i, q_j is prime. Then p_1 divides $q_1 q_2 \cdots q_m$ which, with the help of Euclid's Lemma, implies that $p_1 = q_j$ for some $j \in \{1, \cdots, m\}$. Then $\frac{n}{p_1} = \frac{n}{q_j}$ is a natural number smaller than n that has two different prime factorizations, a contradiction. □

§2.5 Equivalent Forms of Induction

Alternative Proof of Fundamental Theorem of Arithmetic.

Let m be a natural number greater than 1. We note that 2 is a prime, so the statement is true when m is 2. Now assume that k is a prime or is a product of primes for all k such that $1 < k < m$. If m has no factors other than 1 and itself, then m is prime. Otherwise, $m = st$ for some natural numbers s and t that are greater than 1 and less than m. By the complete induction hypothesis, each of s and t either is prime or is a product of primes. Thus, $m = st$ is a product of primes, so the statement is true for m. Therefore, we conclude that every natural number greater than 1 is prime or is a product of primes by **PCI**. □

§2.5 Equivalent Forms of Induction

Theorem

Let a and b be nonzero integers. Then there is a smallest positive linear combination of a and b.

Proof.

Let a and b be nonzero integers, and S be the set of all positive linear combinations of a and b; that is,

$$S = \left\{ am + bn \,\middle|\, m, n \in \mathbb{Z}, am + bn > 0 \right\}.$$

Then $S \neq \varnothing$ since $a \cdot 1 + b \cdot 0 > 0$ or $a \cdot (-1) + b \cdot 0 > 0$. By **WOP**, S has a smallest element, which is the smallest positive linear combination of a and b. □

§2.5 Equivalent Forms of Induction

Theorem (Division Algorithm)

For all integers a and b, where $a \neq 0$, there exist a unique pair of integers (q, r) such that $b = aq + r$ and $0 \leqslant r < |a|$. In notation,

$(\forall\,(a, b) \in (\mathbb{Z}\backslash\{0\}) \times \mathbb{Z})(\exists!(q, r) \in \mathbb{Z} \times \mathbb{Z})\big[(a = bq + r) \wedge (0 \leqslant r < |a|)\big]$.

Proof.

W.L.O.G., we assume that $a > 0$ and a does not divide b. Define

$$S = \left\{b - ak \,\middle|\, k \in \mathbb{Z} \text{ and } b - ak \geqslant 0\right\}.$$

Then $0 \notin S$ (which implies that $b \neq 0$). It is clear that if $b > 0$, then $S \neq \varnothing$. If $b < 0$, then $-b > 0$; thus the Archimedean property implies that there exists $k \in \mathbb{N}$ such that $ak > -b$. Therefore, $b - a(-k) > 0$ which also implies that $S \neq \varnothing$. In either case, S is a non-empty subset of $\mathbb{N}$; thus **WOP** implies that S has a smallest element r. Then $b - aq = r$ for some $q \in \mathbb{Z}$; thus $b = aq + r$ and $r > 0$. □

§2.5 Equivalent Forms of Induction

Proof (Cont'd).

Next, we show that $r < |a| = a$. Assume the contrary that $r \geqslant |a| = a$. Then $b - a(q+1) = b - aq - a = r - a \geqslant 0$. Since we assume that $0 \notin S$, we must have $b - a(q+1) > 0$. Therefore,

$$0 < b - a(q+1) = r - a < r = b - aq$$

which shows that r is not the smallest element of S, a contradiction.

To complete the proof, we need to show that the pair (q, r) is unique. Suppose that there exist (q_1, r_1) and (q_2, r_2), where $0 \leqslant r_1, r_2 < |a|$, such that

$$b = aq_1 + r_1 = aq_2 + r_2 \,.$$

W.L.O.G., we can assume that $r_1 \geqslant r_2$; thus $a(q_2 - q_1) = r_1 - r_2 \geqslant 0$. Therefore, a divides $r_1 - r_2$ which is impossible if $0 < r_1 - r_2 < a$. Therefore, $r_1 = r_2$ and then $q_1 = q_2$. □

Chapter 3. Relations and Partitions

§3.1 Relations

§3.2 Equivalence Relations

§3.3 Partitions

§3.4 Modular Arithmetic

§3.5 Ordering Relations

§3.1 Relations

Definition

Let A and B be sets. R is a ***relation*** from A to B if R is a subset of $A \times B$. A relation from A to A is called a relation on A. If $(a, b) \in R$, we say a is R-related (or simply related) to b and write aRb. If $(a, b) \notin R$, we write $a\not{R}b$.

Example

Let R be the relation "is older than" on the set of all people. If a is 32 yrs old, b is 25 yrs old, and c is 45 yrs old, then aRb, cRb, $a\not{R}c$. Similarly, the "less than" relation on $\mathbb{R}$ is the set $\{(x, y) \,|\, x < y\}$.

§3.1 Relations

Remark:

Let A and B be sets. Every subset of $A \times B$ is a relations from A to B; thus every collection of ordered pairs is a relation. In particular, the empty set $\varnothing$ and the set $A \times B$ are relations from A to B ($R = \varnothing$ is the relation that "nothing" is related, while $R = A \times B$ is the relation that "everything" is related).

§3.1 Relations

Definition

For any set A, the ***identity relation on*** A is the (diagonal) set

$$I_A = \left\{(a,a) \,\middle|\, a \in A\right\}.$$

Definition

Let A and B be sets, and R be a relation from A to B. The ***domain*** of R is the set

$$\mathrm{Dom}(R) = \left\{x \in A \,\middle|\, (\exists\, y \in B)(xRy)\right\},$$

and the ***range*** of R is the set

$$\mathrm{Rng}(R) = \left\{y \in B \,\middle|\, (\exists\, x \in A)(xRy)\right\}.$$

In other words, the domain of a relation R from A to B is the collection of all first coordinate of ordered pairs in R, and the range of R is the collection of all second coordinates.

§3.1 Relations

Definition

Let A and B be sets, and R be a relation from A to B. The ***inverse*** of R, denoted by R^{-1}, is the relation

$$R^{-1} = \big\{(y,x) \in B \times A \,\big|\, (x,y) \in R \text{ (or equivalently, } xRy)\big\}\,.$$

In other words, xRy if and only if $yR^{-1}x$ or equivalently, $(x,y) \in R$ if and only if $(y,x) \in R^{-1}$.

Example

Let $T = \big\{(x,y) \in \mathbb{R} \times \mathbb{R} \,\big|\, y < 4x^2 - 7\big\}$. To find the inverse of T, we note that

$$\begin{aligned}(x,y) \in T^{-1} &\Leftrightarrow (y,x) \in T \Leftrightarrow x < 4y^2 - 7 \Leftrightarrow x + 7 < 4y^2 \\ &\Leftrightarrow (x,y) \in \big\{(x,y) \in \mathbb{R} \times \mathbb{R} \,\big|\, x + 7 < 0\big\} \cup \\ &\qquad \big\{(x,y) \in \mathbb{R} \times \mathbb{R} \,\big|\, 0 \leqslant \frac{x+7}{4} < y^2\big\}\,.\end{aligned}$$

§3.1 Relations

Theorem

Let A and B be sets, and R be a relation from A to B.

1. $\mathrm{Dom}(R^{-1}) = \mathrm{Rng}(R)$.
2. $\mathrm{Rng}(R^{-1}) = \mathrm{Dom}(R)$.

Proof.

The theorem is concluded by

$$\begin{aligned} b \in \mathrm{Dom}(R^{-1}) &\Leftrightarrow (\exists\, a \in A)\big[(b,a) \in R^{-1}\big] \Leftrightarrow (\exists\, a \in A)\big[(a,b) \in R\big] \\ &\Leftrightarrow b \in \mathrm{Rng}(R)\,, \end{aligned}$$

and

$$\begin{aligned} a \in \mathrm{Rng}(R^{-1}) &\Leftrightarrow (\exists\, b \in B)\big[(b,a) \in R^{-1}\big] \Leftrightarrow (\exists\, b \in B)\big[(a,b) \in R\big] \\ &\Leftrightarrow a \in \mathrm{Dom}(R)\,. \end{aligned}$$

□

§3.1 Relations

Definition

Let A, B, C be sets, and R be a relation from A to B, S be a relation from B to C. The ***composite*** of R and S is a relation from A to C, denoted by $S \circ R$, given by

$$S \circ R = \Big\{(a, c) \in A \times C \,\Big|\, (\exists\, b \in B)\big[(aRb) \wedge (bSc)\big]\Big\}.$$

We note that $\mathrm{Dom}(S \circ R) \subseteq \mathrm{Dom}(R)$ and it may happen that $\mathrm{Dom}(S \circ R) \subsetneq \mathrm{Dom}(R)$.

§3.1 Relations

Example

Let $A = \{1,2,3,4,5\}$, $B = \{p,q,r,s,t\}$ and $C = \{x,y,z,w\}$. Let R be the relation from A to B:

$$R = \big\{(1,p),(1,q),(2,q),(3,r),(4,s)\big\}$$

and S be the relation from B to C:

$$S = \big\{(p,x),(q,x),(q,y),(s,z),(t,z)\big\}\,.$$

Then $S \circ R = \big\{(1,x),(1,y),(2,x),(2,y),(4,z)\big\}$.

Example

Let $R = \big\{(x,y) \in \mathbb{R} \times \mathbb{R} \,\big|\, y = x+1\big\}$ and $S = \big\{(x,y) \in \mathbb{R} \times \mathbb{R} \,\big|\, y = x^2\big\}$. Then

$$\begin{aligned} R \circ S &= \big\{(x,y) \in \mathbb{R} \times \mathbb{R} \,\big|\, y = x^2 + 1\big\}\,, \\ S \circ R &= \big\{(x,y) \in \mathbb{R} \times \mathbb{R} \,\big|\, y = (x+1)^2\big\}\,. \end{aligned}$$

Therefore, $S \circ R \neq R \circ S$.

§3.1 Relations

Theorem

Suppose that A, B, C, D are sets, R be a relation from A to B, S be a relation from B to C, and T be a relation from C to D.

(a) $(R^{-1})^{-1} = R$.

(b) $T \circ (S \circ R) = (T \circ S) \circ R$ (*so composition is associative*).

(c) $I_B \circ R = R$ *and* $R \circ I_A = R$.

(d) $(S \circ R)^{-1} = R^{-1} \circ S^{-1}$.

Proof of (a).

(a) holds since

$$(a, b) \in (R^{-1})^{-1} \Leftrightarrow (b, a) \in R^{-1} \Leftrightarrow (a, b) \in R\,. \qquad \square$$

§3.1 Relations

Proof of (b) $T \circ (S \circ R) = (T \circ S) \circ R$.

Since $S \circ R$ is a relation from A to C, $T \circ (S \circ R)$ is a relation from $A \to D$. Similarly, $(T \circ S) \circ R$ is also a relation from A to D. Let $(a, d) \in A \times D$. Then

$$\begin{aligned}
&(a, d) \in T \circ (S \circ R) \\
&\qquad \Leftrightarrow (\exists\, c \in C)\big[(a, c) \in S \circ R \wedge (c, d) \in T\big] \\
&\qquad \Leftrightarrow (\exists\, c \in C)(\exists\, b \in B)\big[(a, b) \in R \wedge (b, c) \in S \wedge (c, d) \in T\big] \\
&\qquad \Leftrightarrow (\exists\, (b, c) \in B \times C)\big[(a, b) \in R \wedge (b, c) \in S \wedge (c, d) \in T\big] \\
&\qquad \Leftrightarrow (\exists\, b \in B)(\exists\, c \in C)\big[(a, b) \in R \wedge (b, c) \in S \wedge (c, d) \in T\big] \\
&\qquad \Leftrightarrow (\exists\, b \in B)\big[(a, b) \in R \wedge (b, d) \in T \circ S\big] \\
&\qquad \Leftrightarrow (a, d) \in (T \circ S) \circ R\,.
\end{aligned}$$

Therefore, $T \circ (S \circ R) = (T \circ S) \circ R$. □

§3.1 Relations

Proof of (c) $I_B \circ R = R = R \circ I_A$.

Let $(a,b) \in A \times B$ be given. Then

$$(a,b) \in I_B \circ R \Leftrightarrow (\exists\, c \in B)\big[(a,c) \in R \wedge (c,b) \in I_B\big]\,.$$

Note that $(c,b) \in I_B$ if and only if $c = b$; thus

$$(\exists\, c \in B)\big[(a,c) \in R \wedge (c,b) \in I_B\big] \Leftrightarrow (a,b) \in R\,.$$

Therefore, $(a,b) \in I_B \circ R \Leftrightarrow (a,b) \in R$. Similarly, $(a,b) \in R \circ I_A \Leftrightarrow (a,b) \in R$. □

Proof of (d) $(S \circ R)^{-1} = R^{-1} \circ S^{-1}$.

Let $(a,c) \in A \times C$. Then

$$\begin{aligned}(c,a) \in (S \circ R)^{-1} &\Leftrightarrow (a,c) \in S \circ R \\ &\Leftrightarrow (\exists\, b \in B)\big[(a,b) \in R \wedge (b,c) \in S\big] \\ &\Leftrightarrow (\exists\, b \in B)\big[(c,b) \in S^{-1} \wedge (b,a) \in R^{-1}\big] \\ &\Leftrightarrow (c,a) \in R^{-1} \circ S^{-1}\,.\end{aligned}$$

□

§3.2 Equivalence Relations

Definition

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

1. R is ***reflexive*** on A if $(\forall\, x \in A)(xRx)$.
2. R is ***symmetric*** on A if $\big[\forall\,(x,y) \in A \times A\big](xRy \Leftrightarrow yRx)$.
3. R is ***transitive*** on A if
$$\big[\forall\,(x,y,z) \in A \times A \times A\big]\big[(xRy) \wedge (yRz)\big] \Rightarrow (xRz)\big].$$

A relation R on A which is reflexive, symmetric and transitive is called an ***equivalence relation*** on A.

An equivalence relation is often denoted by $\sim$ (the same symbol as negation but $\sim$ as negation is always in front of a proposition while $\sim$ as an equivalence relation is always between two elements in a set).

§3.2 Equivalence Relations

Example

The relation “divides” on $\mathbb{N}$ is reflexive and transitive, but not symmetric. The relation “is greater than” on $\mathbb{N}$ is only transitive（遞移律）but not reflexive and transitive.

Example

Let A be a set. The relation “is a subset of” on the power set $\mathcal{P}(A)$ is reflexive, transitive but not symmetric.

Example

The relation $S = \left\{(x, y) \in \mathbb{R} \times \mathbb{R} \,\middle|\, x^2 = y^2\right\}$ is reflexive, symmetric and transitive on $\mathbb{R}$.

Example

The relation R on $\mathbb{Z}$ defined by $R = \left\{(x, y) \in \mathbb{Z} \times \mathbb{Z} \,\middle|\, x + y \text{ is even}\right\}$ is reflexive, symmetric and transitive.

§3.2 Equivalence Relations

Definition

Let A be a set and R be an equivalence relation on A. For $x \in A$, the ***equivalence class of*** x ***modulo*** R (or simply x ***mod*** R) is a subset of A given by

$$\bar{x} = \{ y \in A \,|\, xRy \} .$$

Each element of $\bar{x}$ is called a ***representative*** of this class. The collection of all equivalence classes modulo R, called A ***modulo*** R, is denoted by A/R (and is the set $A/R = \{\bar{x} \,|\, x \in A\}$).

Example

The relation $H = \{(1,1),(2,2),(3,3),(1,2),(2,1)\}$ is an equivalence relation on the set $A = \{1,2,3\}$. Then

$$\bar{1} = \bar{2} = \{1,2\} \quad \text{and} \quad \bar{3} = \{3\} .$$

Therefore, $A/H = \{\{1,2\},\{3\}\}$.

§3.2 Equivalence Relations

Theorem

Let A be a non-empty set and R be an equivalence relation on A. For all $x, y \in A$, we have

(a) $x \in \overline{x}$ and $\overline{x} \subseteq A$. (b) xRy if and only if $\overline{x} = \overline{y}$.

(c) $x \not R y$ if and only if $\overline{x} \cap \overline{y} = \varnothing$.

Proof.

It is clear that (a) holds. To see (b) and (c), it suffices to show that "$xRy \Rightarrow \overline{x} = \overline{y}$" and "$x \not R y \Rightarrow \overline{x} \cap \overline{y} = \varnothing$".

Assume that xRy. Then if $z \in \overline{x}$, we have xRz. The symmetry and transitivity of R then implies that yRz; thus $z \in \overline{y}$ which implies that $\overline{x} \subseteq \overline{y}$. Similarly, $\overline{y} \subseteq \overline{x}$; hence we conclude that "$xRy \Rightarrow \overline{x} = \overline{y}$".

Now assume that $\overline{x} \cap \overline{y} \neq \varnothing$. Then for for some $z \in A$ we have $z \in \overline{x} \cap \overline{y}$. Therefore, xRz and yRz. Since R is symmetric and transitive, then xRy which implies that "$x \not R y \Rightarrow \overline{x} \cap \overline{y} = \varnothing$". □

§3.2 Equivalence Relations

Definition

Let m be a fixed positive integer. For $x, y \in \mathbb{Z}$, we say x ***is congruent to*** y ***modulo*** m（以 m 為除數時 x 同餘 y）and write $x = y$ (***mod*** m) if m divides $(x - y)$. The number m is called the ***modulus*** of the congruence.

Example

Using 4 as the modulus, we have

$$\begin{aligned} 3 &= 3 \pmod 4 \text{ because } 4 \text{ divides } 3-3=0\,,\\ 9 &= 5 \pmod 4 \text{ because } 4 \text{ divides } 9-5=4\,,\\ -27 &= 1 \pmod 4 \text{ because } 4 \text{ divides } -27-1=-28\,,\\ 20 &= 8 \pmod 4 \text{ because } 4 \text{ divides } 20-8=12\,,\\ 100 &= 0 \pmod 4 \text{ because } 4 \text{ divides } 100-0=100\,. \end{aligned}$$

§3.2 Equivalence Relations

Theorem

For every fixed positive integer m, the relation "congruence modulo m" is an equivalence relation on $\mathbb{Z}$.

Proof.

1. **(Reflexivity)** It is easy to see that $x = x \pmod{m}$ for all $x \in \mathbb{Z}$. Therefore, congruence modulo m is reflexive on $\mathbb{Z}$.
2. **(Symmetry)** Assume that $x = y \pmod{m}$. Then m divides $x - y$; that is, $x - y = mk$ for some $k \in \mathbb{Z}$. Therefore, $y - x = m(-k)$ which implies that m divides $y - x$; thus $y = x \pmod{m}$.
3. **(Transitivity)** Assume that $x = y \pmod{m}$ and $y = z \pmod{m}$. Then $x - y = mk$ and $y - z = m\ell$ for some $k, \ell \in \mathbb{Z}$. Therefore, $x - z = m(k + \ell)$ which implies that m divides $x - z$; thus $x = z \pmod{m}$. □

§3.2 Equivalence Relations

Definition

The set of equivalence classes for the relation congruence modulo m is denoted by $\mathbb{Z}_m$.

Remark: The elements of $\mathbb{Z}_m$ are sometimes called the ***residue*** (or ***remainder***) classes modulo m.

Example

For congruence modulo 4, there are four equivalence classes:

$$\begin{aligned}
\overline{0} &= \{\cdots,-16,-12,-8,-4,0,4,8,12,16,\cdots\} = \{4k \,|\, k \in \mathbb{Z}\},\\
\overline{1} &= \{\cdots,-15,-11,-7,-3,1,5,9,13,17,\cdots\} = \{4k+1 \,|\, k \in \mathbb{Z}\},\\
\overline{2} &= \{\cdots,-14,-10,-6,-2,2,6,10,14,18,\cdots\} = \{4k+2 \,|\, k \in \mathbb{Z}\},\\
\overline{3} &= \{\cdots,-13,-9,-5,-1,3,7,11,15,19,\cdots\} = \{4k+3 \,|\, k \in \mathbb{Z}\}.
\end{aligned}$$

§3.2 Equivalence Relations

In general, we will prove that the equivalence relation "congruence modulo m" produces m equivalence classes

$$\bar{j} = \left\{mk + j \,\middle|\, k \in \mathbb{Z}\right\}, \qquad j = 0, 1, \cdots, m-1 .$$

The collection of these equivalence classes, by definition $\mathbb{Z}/(\mathrm{mod}\ m)$, is usually denoted by $\mathbb{Z}_m$.

Theorem

Let m be a fixed positive integer. Then

1. *For integers x and y, $x = y \pmod{m}$ if and only if the remainder when x is divided by m equals the remainder when y divided by m.*
2. *$\mathbb{Z}_m$ consists of m distinct equivalence classes:*

$$\mathbb{Z}_m = \left\{\overline{0}, \overline{1}, \cdots, \overline{m-1}\right\}.$$

§3.2 Equivalence Relations

Proof.

1. For a given $x \in \mathbb{Z}$, let $\big(q(x), r(x)\big)$ denote the unique pair in $\mathbb{Z} \times \mathbb{Z}$ obtained by the division algorithm satisfying
$$x = mq(x) + r(x) \quad \text{and} \quad 0 \leqslant r(x) < m\,.$$
Then
$$\begin{aligned} x = y \pmod{m} &\Leftrightarrow m \text{ divides } x - y \\ &\Leftrightarrow m \text{ divides } m\big(q(x) - q(y)\big) + r(x) - r(y) \\ &\Leftrightarrow m \text{ divides } r(x) - r(y) \\ &\Leftrightarrow r(x) - r(y) = 0\,. \end{aligned}$$
where the last equivalence following from the fact that $0 \leqslant r(x), r(y) < m$.

□

§3.2 Equivalence Relations

Proof. (Cont'd).

2. Using ①, x and y are in the same equivalence classes (produced by the equivalence relation "congruence modulo m") if and only if x and y has the same remainder when they are divided by m. Therefore, we find that

$$\bar{x} = \big\{mk + r(x) \,\big|\, k \in \mathbb{Z}\big\} = \overline{r(x)} \qquad \forall\, x \in \mathbb{Z}\,.$$

Since $r(x)$ has values from $\{0, 1, \cdots, m-1\}$, we find that $\mathbb{Z}_m = \{\bar{0}, \bar{1}, \cdots, \overline{m-1}\}$. The proof is completed if we show that $\bar{k} \cap \bar{j} = \varnothing$ if $k \neq j$ and $k, j \in \{0, 1, \cdots, m-1\}$. However, if $x \in \bar{k} \cap \bar{j}$, then

$$x = mq_1 + k = mq_2 + j$$

which is impossible since $k \neq j$ and $k, j \in \{0, 1, \cdots, m-1\}$. Therefore, there are exactly m equivalence classes. □

§3.3 Partitions

Definition

Let A be a non-empty set. $\mathcal{P}$ is a ***partition*** of A if $\mathcal{P}$ is a collection of subsets of A such that

1. if $X \in \mathcal{P}$, then $X \neq \varnothing$.
2. if $X \in \mathcal{P}$ and $Y \in \mathcal{P}$, then $X = Y$ or $X \cap Y = \varnothing$.
3. $\bigcup\limits_{X \in \mathcal{P}} X = A$.

In other words, a partition of a set A is a pairwise disjoint collection of non-empty subsets of A whose union is A.

§3.3 Partitions

Example

The family $\mathcal{G} = \left\{ [n, n+1) \,\middle|\, n \in \mathbb{Z} \right\}$ is a partition of $\mathbb{R}$.

Example

Each of the following is a partition of $\mathbb{Z}$:

1. $\mathcal{P} = \{E, D\}$, where E is the collection of even integers and D is the collection of odd integers.
2. $\mathcal{X} = \{\mathbb{N}, \{0\}, \mathbb{Z}^-\}$, where $\mathbb{Z}^-$ is the collection of negative integers.
3. $\mathcal{H} = \{A_k \mid k \in \mathbb{Z}\}$, where $A_k = \{3k, 3k+1, 3k+2\}$.

§3.3 Partitions

Theorem

If R is an equivalent relation on a non-empty set A, then A/R is a partition of A.

Proof.

First of all, each equivalence class $\overline{x} \in A/R$ must be non-empty since it contains x. Let $\overline{x}$ and $\overline{y}$ be two equivalence classes in A/R. If $\overline{x} \cap \overline{y} \neq \varnothing$, then there exists $z \in \overline{x} \cap \overline{y}$ which implies that xRz and yRz. By the symmetry and the transitivity of R we have xRy which implies that $\overline{x} = \overline{y}$.

Finally, it is clear that $\displaystyle\bigcup_{\overline{x} \in A/R} \overline{x} \subseteq A$ since each $\overline{x} \subseteq A$. On the other hand, since each $y \in A$ belongs to the equivalence class $\overline{y}$, we must have $\displaystyle A \subseteq \bigcup_{\overline{x} \in A/R} \overline{x}$. Therefore, $\displaystyle A = \bigcup_{\overline{x} \in A/R} \overline{x}$. □

§3.3 Partitions

Theorem

Let $\mathcal{P}$ be a partition of a non-empty set A. For $x, y \in A$, define xQy if and only if there exists $C \in \mathcal{P}$ such that $x, y \in C$. Then

1. *Q is an equivalence relation on A.*
2. *$A/Q = \mathcal{P}$.*

Proof.

It is clear that Q is reflexive and symmetric on A, so it suffices to show the transitivity of Q to complete ①. Suppose that xQy and yQz. By the definition of the relation Q there exists C_1 and C_2 in $\mathcal{P}$ such that $x, y \in C_1$ and $y, z \in C_2$; hence $C_1 \cap C_2 \neq \varnothing$. Then $C_1 = C_2$ by the fact that $\mathcal{P}$ is a partition and $C_1, C_2 \in \mathcal{P}$. Therefore, $x, z \in C_1$ which implies that xQz. □

§3.3 Partitions

Proof. (Cont'd).

Next, we claim that if $C \in \mathcal{P}$, then $x \in C$ if and only if $\bar{x} = C$. It suffices to show the direction "$\Rightarrow$" since $x \in \bar{x}$.

Suppose that $C \in \mathcal{P}$ and $x \in C$.

1. "$C \subseteq \bar{x}$": Let $y \in C$ be given. By the fact that $x \in C$ we must have yQx. Therefore, $y \in \bar{x}$ which shows $C \subseteq \bar{x}$.
2. "$\bar{x} \subseteq C$": Let $y \in \bar{x}$ be given. Then there exists $\widetilde{C} \in \mathcal{P}$ such that $x, y \in \widetilde{C}$. By the fact that $x \in C$, we find that $C \cap \widetilde{C} \neq \varnothing$. Since $\mathcal{P}$ is a partition of A and $C, \widetilde{C} \in \mathcal{P}$, we must have $C = \widetilde{C}$; thus $y \in C$. Therefore, $\bar{x} \subseteq C$. □

§3.3 Partitions

Proof. (Cont'd).

Now we show that $A/Q = \mathcal{P}$. If $C \in \mathcal{P}$, then $C \neq \varnothing$; thus there exists $x \in C$ for some $x \in A$. Then the claim above shows that $C = \overline{x} \in A/Q$. Therefore, $\mathcal{P} \subseteq A/Q$. On the other hand, if $\overline{x} \in A/Q$, by the fact that $\mathcal{P}$ is a partition of A, there exists $C \in \mathcal{P}$ such that $x \in C$. Then the claim above shows that $\overline{x} = C$. Therefore, $A/Q \subseteq \mathcal{P}$. □

Remark: The relation Q defined in the theorem proved above is called ***the equivalence relation associated with the partition*** $\mathcal{P}$.

§3.3 Partitions

Example

Let $A = \{1,2,3,4\}$, and let $\mathcal{P} = \big\{\{1\},\{2,3\},\{4\}\big\}$ be a partition of A with three sets. The equivalence relation Q associated with $\mathcal{P}$ is $\big\{(1,1),(2,2),(3,3),(4,4),(2,3),(3,2)\big\}$. The three equivalence classes for Q are $\overline{1} = \{1\}$, $\overline{2} = \overline{3} = \{2,3\}$ and $\overline{4} = \{4\}$. The collection of all equivalence classes A/Q is precisely $\mathcal{P}$.

Example

The collect $\mathcal{P} = \{A_0, A_1, A_2, A_3\}$, where

$$A_j = \{4k + j \,|\, k \in \mathbb{Z}\} \text{ for } j = \{0,1,2,3\},$$

is a partition of $\mathbb{Z}$ because of the division algorithm. The equivalence relation associated with the partition $\mathcal{P}$ is the relation of congruence modulo 4, and each A_j is the residue class of j modulo 4 for $j = 0,1,2,3$.

§3.4 Modular Arithmetic

Theorem

Let m be a positive integer and a, b, c and d be integers. If $a = c \pmod{m}$ and $b = d \pmod{m}$, then $a + b = c + d \pmod{m}$ and $a \cdot b = c \cdot d \pmod{m}$.

Proof.

Since $a = c \pmod{m}$ and $b = d \pmod{m}$, we have $a - c = mk_1$ and $b - d = mk_2$ for some $k_1, k_2 \in \mathbb{Z}$. Then

$$a + b = c + mk_1 + d + mk_2 = c + d + m(k_1 + k_2)$$

and

$$a \cdot b = (c + mk_1) \cdot (d + mk_2) = c \cdot d + m(c \cdot k_2 + d \cdot k_1 + k_1 \cdot k_2) .$$

Therefore, $a + b = c + d \pmod{m}$ and $a \cdot b = c \cdot d \pmod{m}$. □

§3.4 Modular Arithmetic

Definition

For each natural number m,

1. the ***sum of the classes*** $\overline{x}$ and $\overline{y}$ in $\mathbb{Z}_m$, denoted by $\overline{x}+\overline{y}$, is defined to be the class containing the integer $x+y$;
2. the ***product of the classes*** $\overline{x}$ and $\overline{y}$ in $\mathbb{Z}_m$, denoted by $\overline{x}\cdot\overline{y}$, is defined to be the class containing the integer $x\cdot y$.

In symbols, $\overline{x}+\overline{y}=\overline{x+y}$ and $\overline{x}\cdot\overline{y}=\overline{x\cdot y}$.

Example

In $\mathbb{Z}_6$, $\overline{5}+\overline{3}=\overline{2}$ and $\overline{4}\cdot\overline{5}=\overline{2}$.

Example

In $\mathbb{Z}_8$, $(\overline{5}+\overline{7})\cdot(\overline{6}+\overline{5})=\overline{12}\cdot\overline{11}=\overline{4}\cdot\overline{3}=\overline{12}=\overline{4}$.

§3.4 Modular Arithmetic

Example

Find $\overline{3^{63}}$ in $\mathbb{Z}_7$. Since

$$\overline{3^1}=\overline{3}\,,\quad \overline{3^2}=\overline{2}\,,\quad \overline{3^3}=\overline{6}\,,\quad \overline{3^4}=\overline{4}\,,\quad \overline{3^5}=\overline{5}\,,\quad \overline{3^6}=\overline{1}\,,$$

we have $\overline{3^{63}}=\overline{3^{60}\cdot 3^3}=\overline{6}$.

Example

For every integer k, 6 divides k^3+5k. In fact, by the division algorithm, for each $k\in\mathbb{Z}$ there exists a unique pair (q,r) such that $k=6q+r$ for some $0\leqslant r<5$. Therefore, in $\mathbb{Z}_6$ we have

$$\begin{aligned}\overline{k^3+5k}&=\overline{(6q+r)^3}+\overline{5(6q+r)}=\overline{r^3}+\overline{5\cdot r}\\&=\overline{r^3}+\overline{(-1)\cdot r}=\overline{r^3-r}\,.\end{aligned}$$

It is clear that then $\overline{k^3+5k}=\overline{0}$ since

$$\overline{0^3-0}=\overline{1^3-1}=\overline{2^3-2}=\overline{3^3-3}=\overline{4^3-4}=\overline{5^3-5}\,.$$

§3.4 Modular Arithmetic

Theorem

Let m be a positive composite integer. Then there exists non-zero equivalence classes $\bar{x}$ and $\bar{y}$ in $\mathbb{Z}_m$ such that $\bar{x} \cdot \bar{y} = \bar{0}$.

Proof.

Since m is a positive composite integer, $m = x \cdot y$ for some $x, y \in \mathbb{N}$, $1 < x, y < m$. Since $1 < x, y < m$, $\bar{x}, \bar{y} \neq \bar{0}$. Therefore, in $\mathbb{Z}_m$ $\bar{0} = \bar{m} = \bar{x} \cdot \bar{y}$ which concludes the theorem. □

Theorem

Let p be a prime. If $\bar{x} \cdot \bar{y} = \bar{0}$ in $\mathbb{Z}_p$, then either $\bar{x} = \bar{0}$ or $\bar{y} = \bar{0}$.

Proof.

Let $\bar{x}, \bar{y} \in \mathbb{Z}_p$ and $\bar{x} \cdot \bar{y} = \bar{0}$. Then $x \cdot y = 0 \pmod{p}$. Therefore, p divides $x \cdot y$. Since p is prime, $p|x$ or $p|y$ which implies that $\bar{x} = \bar{0}$ or $\bar{y} = \bar{0}$. □

§3.4 Modular Arithmetic

Theorem

Let p be a prime. If $xy = xz \pmod{p}$ and $x \neq 0 \pmod{p}$, then $y = z \pmod{p}$.

Proof.

If $xy = xz$ (mod p), then $x(y-z) = 0$ (mod p). By the previous theorem $\overline{x} = \overline{0}$ or $\overline{y-z} = \overline{0}$. Since $x \neq 0$ (mod p), we must have $\overline{y} = \overline{z}$; thus $y = z$ (mod p). □

Corollary (Cancellation Law for $\mathbb{Z}_p$)

Let p be a prime, and $\overline{x}, \overline{y}, \overline{z} \in \mathbb{Z}_p$. If $\overline{x} \cdot \overline{y} = \overline{x} \cdot \overline{z}$, then $\overline{x} \neq \overline{0}$ or $\overline{y} = \overline{z}$.

Chapter 4. Functions

§4.1 Functions as Relations

§4.2 Construction of Functions

§4.3 Functions that are Onto; One-to-One Functions

§4.4 Inverse Functions

§4.5 Set Images

§4.1 Functions as Relations

Recall the usual definition of functions from A to B:

Definition

Let A and B be sets. A ***function*** $f : A \to B$ consists of two sets A and B together with a "rule" that assigns to each $x \in A$ a special element of B denoted by $f(x)$. One writes $x \mapsto f(x)$ to denote that x is mapped to the element $f(x)$. A is called the ***domain*** of f, and B is called the ***target*** or ***co-domain*** of f. The ***range*** of f or the ***image*** of f, is the subset of B defined by $f(A) = \big\{f(x) \,\big|\, x \in A\big\}$.

Each function is associated with a collection of ordered pairs

$$\big\{(x, f(x)) \,\big|\, x \in A\big\} \subseteq A \times B\,.$$

Since a collection of ordered pairs is a relation, we can say that a function is a relation from one set to another.

§4.1 Functions as Relations

However, not every relation can serve as a function. A function is a relation with additional special properties and we have the following

Definition (Alternative Definition of Functions)

A ***function*** (or ***mapping***) from A to B is a relation f from A to B such that

1. the domain of f is A; that is, $(\forall x \in A)(\exists y \in B)((x, y) \in f)$, and
2. if $(x, y) \in f$ and $(x, z) \in f$, then $y = z$.

We write $f : A \to B$, and this is read "f is a function from A to B" or "f maps A to B". The set B is called the ***co-domain*** of f. In the case where $B = A$, we say f is a function on A.

When $(x, y) \in f$, we write $y = f(x)$ instead of xfy. We say that y is the ***image*** of f at x (or value of f at x) and that x is a ***pre-image*** of y.

§4.1 Functions as Relations

Remark:

1. A function has only one domain and one range but many possible co-domains.
2. A function on $\mathbb{R}$ is usually called a real-valued function or simply real function. The domain of a real function is usually understood to be the largest possible subset of $\mathbb{R}$ on which the function takes values.

Definition

A function x with domain $\mathbb{N}$ is called an ***infinite sequence***, or simply a ***sequence***. The image of the natural number n is usually written as x_n instead of $x(n)$ and is called the ***n-th term of the sequence***.

§4.1 Functions as Relations

Definition

Let A, B be sets, and $A \subseteq B$.

1. The the ***identity function/map*** on A is the function $I_A : A \to A$ given by $I_A(x) = x$ for all $x \in A$.
2. The ***inclusion function/map*** from A to B is the function $\iota : A \to B$ given by $\iota(x) = x$ for all $x \in A$.
3. The ***characteristic/indicator function*** of A (defined on B) is the map $\mathbf{1}_A : B \to \mathbb{R}$ given by

$$\mathbf{1}_A(x) = \begin{cases} 1 & \text{if } x \in A\,, \\ 0 & \text{if } x \in B \backslash A\,. \end{cases}$$

§4.1 Functions as Relations

Definition (Cont'd)

4. The ***greatest integer function*** on $\mathbb{R}$ is the function $[\cdot]:\mathbb{R}\to\mathbb{Z}$ given by
$$[x] = \text{the largest integer which is not greater than } x.$$
The function $[\cdot]$ is also called the ***floor function*** or the ***Gauss function***.

5. Let R be an equivalence relation on A. The ***canonical map*** for the equivalence relation R is the map from A to A/R which maps $x \in A$ to $\overline{x}$, the equivalence class of x modulo R.

§4.1 Functions as Relations

Theorem

Two functions f and g are equal if and only if

1. $\mathrm{Dom}(f) = \mathrm{Dom}(g)$, *and*
2. *for all* $x \in \mathrm{Dom}(f)$, $f(x) = g(x)$.

Example

The identity map of A and the inclusion map from A to B are identical functions.

Example

$f(x) = \dfrac{x}{x}$ and $g(x) = 1$ are different functions since they have different domains.

§4.1 Functions as Relations

Remark:
When a rule of correspondence assigns more than one values to an object in the domain, we say "the function is not well-defined", meaning that it is not really a function. A proof that a function is well-defined is nothing more than a proof that the relation defined by a given rule is single valued.

Example

Let $\overline{x}$ denote the equivalence class of x modulo the congruence relation modulo 4 and $\widetilde{y}$ denote the equivalence class of y modulo the congruence relation modulo 10. Define $f(\overline{x}) = \widetilde{2 \cdot x}$. Then this "function" is not really a function since $\overline{0} = \overline{4}$ but $\widetilde{2 \cdot 0} = \widetilde{0}$ while $\widetilde{2 \cdot 4} = \widetilde{8} \neq \widetilde{0}$. In other words, the way f assigns value to $\overline{x}$ is not well-defined.

§4.1 Functions as Relations

Example

Let $\bar{x}$ denote the equivalence class of x modulo the congruence relation modulo 8 and $\tilde{y}$ denote the equivalence class of y modulo the congruence relation modulo 4. The function $f\colon \mathbb{Z}_8 \to \mathbb{Z}_4$ given by $f(\bar{x}) = \widetilde{x+2}$ is well-defined. To see this, suppose that $\bar{x} = \bar{z}$ in $\mathbb{Z}_8$. Then 8 divides $x-z$ which implies that 4 divides $x-z$; thus 4 divides $(x+2)-(z+2)$. Therefore, $x+2 = z+2 \pmod 4$ or equivalently, $\widetilde{x+2} = \widetilde{z+2}$. So f is well-defined.

§4.2 Construction of Functions

Definition

Let $f: A \to B$. The ***inverse*** of f is the relation from B to A:

$$f^{-1} = \left\{(y,x) \in B \times A \,\middle|\, y = f(x)\right\} = \left\{(y,x) \in B \times A \,\middle|\, (x,y) \in f\right\}.$$

When f^{-1} describes a function, f^{-1} is called the ***inverse function/ map*** of f.

Definition

Let $f : A \to B$ and $g : B \to C$ be functions. The ***composite*** of f and g is the relation from A to C:

$$g \circ f = \left\{(x,z) \in A \times C \,\middle|\, \text{there exists (a unique) } y \in B \text{ such that } (x,y) \in f \text{ and } (y,z) \in g\right\}.$$

§4.2 Construction of Functions

Remark: Using the notation in the definition of functions, if $(x, z) \in g \circ f$, then $z = (g \circ f)(x)$. On the other hand, if $(x, z) \in g \circ f$, there exists (a unique) $y \in B$ such that $(x, y) \in f$ and $(y, z) \in g$. Then $y = f(x)$ and $z = g(y)$. Therefore, we also have $z = g(f(x))$; thus $(g \circ f)(x) = g(f(x))$.

Theorem

Let A, B and C be sets, and $f : A \to B$ and $g : B \to C$ be functions. Then $g \circ f$ is a function from A to C.

§4.2 Construction of Functions

Proof of $g \circ f$ is a function from A to C.

By the definition of composition of relations, $g \circ f$ is a relation from A to C.

1. First, we show that $\mathrm{Dom}(g \circ f) = A$. Clearly $\mathrm{Dom}(g \circ f) \subseteq A$, so it suffices to show that $A \subseteq \mathrm{Dom}(g \circ f)$. Let $x \in A$. Since $f : A \to B$ is a function, there exists $y \in B$ such that $(x, y) \in f$. Since $g : B \to C$ is a function, there exists $z \in C$ such that $(y, z) \in g$. This shows that for every $x \in A$, there exists $z \in C$ such that $(x, z) \in g \circ f$; thus $\mathrm{Dom}(g \circ f) = A$.
2. Next, we show that if $(x, z_1) \in g \circ f$ and $(x, z_2) \in g \circ f$, then $z_1 = z_2$. Suppose that $(x, z_1) \in g \circ f$ and $(x, z_2) \in g \circ f$. Then there exists $y_1, y_2 \in B$ such that $(x, y_1) \in f$ and $(y_1, z_1) \in g$, while $(x, y_2) \in f$ and $(y_2, z_2) \in g$. Since f is a function, $y_1 = y_2$; thus that g is a function implies that $z_1 = z_2$. □

§4.2 Construction of Functions

Recall that if A, B, C, D are sets, R be a relation from A to B, S be a relation from B to C, and T be a relation from C to D. Then

1. $T \circ (S \circ R) = (T \circ S) \circ R$.
2. $I_B \circ R = R$ and $R \circ I_A = R$.

Theorem

Let A, B, C, D be sets, and $f : A \to B$, $g : B \to C$, $h : C \to D$ be functions. Then $h \circ (g \circ f) = (h \circ g) \circ f$.

Theorem

Let $f : A \to B$ be a function. Then $f \circ I_A = f$ and $I_B \circ f = f$.

Theorem

Let $f : A \to B$ be a function, and $C = \mathrm{Rng}(f)$. If $f^{-1} : C \to A$ is a function, then $f^{-1} \circ f = I_A$ and $f \circ f^{-1} = I_C$.

§4.2 Construction of Functions

Definition

Let $f: A \to B$ be a function, and $D \subseteq A$. The ***restriction*** of f to D, denoted by $f|_D$, is the function

$$f|_D = \{(x, y) \mid y = f(x) \text{ and } x \in D\} .$$

If g and h are functions and g is a restriction of h, the h is called an ***extension*** of g.

Example

Let F and G be functions

$$F = \{(1, 2), (2, 6), (3, -9), (5, 7)\} ,$$
$$G = \{(1, 8), (2, 6), (4, 8), (5, 7), (8, 3)\} .$$

Then $F \cap G = \{(2, 6), (5, 7)\}$ is a function with domain $\{2, 5\}$ which is a proper subset of $\text{Dom}(F) \cap \text{Dom}(G) = \{1, 2, 5\}$.

On the other hand, $\{(1, 2), (1, 8)\} \subseteq F \cup G$; thus $F \cup G$ cannot be a function.

§4.2 Construction of Functions

Theorem

Suppose that f and g are functions. Then $f \cap g$ is a function with domain $A = \{x \,|\, f(x) = g(x)\}$, and $f \cap g = f|_A = g|_A$.

Proof.

Let $(x, y) \in f \cap g$. Then $y = f(x) = g(x)$; thus

$$\mathrm{Dom}(f \cap g) = \{x \,|\, f(x) = g(x)\} (\equiv A)\,.$$

If $(x, y_1), (x, y_2) \in f \cap g$, $(x, y_1), (x, y_2) \in f$ which, by the fact that f is a function, implies that $y_1 = y_2$. Therefore, $f \cap g$ is a function. Moreover,

$$f \cap g = \{(x, y) \,|\, \exists\, x \in A, y = f(x)\}$$

which implies that $f \cap g = f|_A$. □

§4.2 Construction of Functions

For $f \cup g$ being a function, it is (sufficient and) necessary that if $x \in \text{Dom}(f) \cap \text{Dom}(g)$, then $f(x) = g(x)$. Moreover, if $f \cup g$ is a function, then $f = (f \cup g)|_{\text{Dom}(f)}$ and $g = (f \cup g)|_{\text{Dom}(g)}$. In particular, we have the following

Theorem

Let f and g be functions with $\mathrm{Dom}(f) = A$ and $\mathrm{Dom}(g) = B$. If $A \cap B = \varnothing$, then $f \cup g$ is a function with domain $A \cup B$. Moreover,

$$(f \cup g)(x) = \begin{cases} f(x) & \text{if } x \in A\,, \\ g(x) & \text{if } x \in B\,. \end{cases}$$

§4.2 Construction of Functions

Theorem

Let f and g be functions with $\mathrm{Dom}(f) = A$ *and* $\mathrm{Dom}(g) = B$. *If* $A \cap B = \varnothing$, *then* $f \cup g$ *is a function with domain* $A \cup B$. *Moreover,*

$$(f \cup g)(x) = \begin{cases} f(x) & \text{if } x \in A\,, \\ g(x) & \text{if } x \in B\,. \end{cases} \tag{$\star$}$$

Proof.

Clearly $\mathrm{Dom}(f \cup g) = A \cup B$. Suppose that $(x, y_1), (x, y_2) \in f \cup g$. If $(x, y_1) \in f$, then $x \in \mathrm{Dom}(f)$; thus by the fact that $A \cap B = \varnothing$, we must have $(x, y_2) \in f$. Since f is a function, $y_1 = f(x) = y_2$. Similarly, if $(x, y_1) \in g$, then $(x, y_2) \in g$ which also implies that $y_1 = g(x) = y_2$. Therefore, $f \cup g$ is a function and $(\star)$ is valid. □

§4.2 Construction of Functions

Definition

Let f be a real-valued function defined on an interval $I \subseteq \mathbb{R}$.

1. The function f is said to be ***increasing*** / ***decreasing*** on I if $x \leqslant y$ implies that $f(x) \leqslant f(y)$ / $f(x) \geqslant f(y)$ for all $x, y \in I$.
2. The function f is said to be ***strictly increasing*** / ***strictly decreasing*** on I if $x < y$ implies that $f(x) < f(y)$ / $f(x) > f(y)$ for all $x, y \in I$.

§4.3 Functions that are Onto; One-to-One Functions

Definition

Let $f\colon A \to B$ be a function.

1. The function f is said to be ***surjective*** or ***onto*** B if $\mathrm{Rng}(f) = B$. When f is surjective, f is called a surjection, and we write $f\colon A \xrightarrow{\text{onto}} B$.
2. The function f is said to be ***injective*** or ***one-to-one*** if it holds that "$f(x) = f(y) \Rightarrow x = y$". When f is injective, f is called a injection, and we write $f\colon A \xrightarrow{1-1} B$.
3. The function f is called a ***bijection*** if it is both injective and surjective. When f is a bijection, we write $f\colon A \xrightarrow[\textit{onto}]{1-1} B$.

§4.3 Functions that are Onto; One-to-One Functions

Remark:

1. It is always true that $\mathrm{Rng}(f) \subseteq B$; thus $f : A \to B$ is onto if and only if $B \subseteq \mathrm{Rng}(f)$. In other words, $f : A \to B$ is onto if and only if every $b \in B$ has a pre-image. Therefore, to prove that $f : A \to B$ is onto B, it is sufficient to show that for every $b \in B$ there exists $a \in A$ such that $f(a) = b$.

2. The direct proof of that $f : A \to B$ is injective is to verify the property that "$f(x) = f(y) \Rightarrow x = y$". A proof of the injectivity of f by contraposition assumes that $x \neq y$ and one needs to show that $f(x) \neq f(y)$.

§4.3 Functions that are Onto; One-to-One Functions

Theorem

1. *If $f : A \to B$ is onto B and $g : B \to C$ is onto C, then $g \circ f$ is onto C.*
2. *If $f : A \to B$ is one-to-one and $g : B \to C$ is one-to-one, then $g \circ f$ is one-to-one.*

Proof.

1. Let $c \in C$. By the surjectivity of g, there exists $b \in B$ such that $g(b) = c$. The surjectivity of f then implies the existence of $a \in A$ such that $f(a) = b$. Therefore, $(g \circ f)(a) = g(f(a)) = g(b) = c$ which concludes ①.
2. Assume that $(g \circ f)(x) = (g \circ f)(y)$. Then $g(f(x)) = g(f(y))$; thus by the injectivity of g, $f(x) = f(y)$. Therefore, the injectivity of f implies that $x = y$ which concludes ②. □

§4.3 Functions that are Onto; One-to-One Functions

Theorem

If $f : A \to B$, $g : B \to C$ are bijections, then $g \circ f : A \to C$ is a bijection.

Theorem

Let $f : A \to B$ and $g : B \to C$ be functions.

1. *If $g \circ f$ is onto C, then g is onto C.*
2. *If $g \circ f$ is one-to-one, then f is one-to-one.*

Proof.

1. Let $c \in C$. Since $g \circ f$ is onto C, there exists $a \in A$ such that $(g \circ f)(a) = c$. Let $b = f(a)$. Then $g(b) = g(f(a)) = (g \circ f)(a) = c$.
2. Suppose that $f(x) = f(y)$. Then $(g \circ f)(x) = g(f(x)) = g(f(y)) = (g \circ f)(y)$, and the injectivity of $g \circ f$ implies that $x = y$. □

§4.3 Functions that are Onto; One-to-One Functions

Remark:

1. In part ① of the theorem above, we cannot conclude that f is also onto B since there might be a proper subset $\widetilde{B} \subsetneq B$ such that $f: A \to \widetilde{B}$, $g: \widetilde{B} \to C$ and $g \circ f$ is onto C. For example, Let $A = B = \mathbb{R}$, $C = \mathbb{R}^+ \cup \{0\}$, and $f(x) = g(x) = x^2$. Then clearly f is not onto B but $g \circ f$ is onto C.
2. In part ② of the theorem above, we cannot conclue that g is one-to-one since it might happen that g is one-to-one on $\text{Rng}(f) \subsetneq B$ but g is not one-to-one on B. For example, let $A = C = \mathbb{R}^+ \cup \{0\}$, $B = \mathbb{R}$, and $f(x) = x^2$, $g(x) = \log(1 + |x|)$. Then clearly g is not one-to-one, but $g \circ f$ is one-to-one.

§4.3 Functions that are Onto; One-to-One Functions

Theorem

If $f : A \to B$ is one-to-one, then every restriction of f is one-to-one.

In the following we consider the function $f \cup g$. Recall that if $\mathrm{Dom}(f) \cap \mathrm{Dom}(g) = \varnothing$, then $(f \cup g)(x) \overset{(\star)}{=} \begin{cases} f(x) & \text{if } x \in \mathrm{Dom}(f)\,, \\ g(x) & \text{if } x \in \mathrm{Dom}(g)\,. \end{cases}$

Theorem

Let $f : A \to C$ and $g : B \to D$ be functions. Suppose that A and B are disjoint sets.

1. *If f is onto C and g is onto D, then $f \cup g : A \cup B \to C \cup D$ is onto $C \cup D$.*
2. *If f is one-to-one, g is one-to-one, and C and D are disjoint, then $f \cup g : A \cup B \to C \cup D$ is one-to-one.*

§4.3 Functions that are Onto; One-to-One Functions

Proof.

We note that $f \cup g : A \cup B \to C \cup D$ is a function.

1. Let $y \in C \cup D$. Then $y \in C$ or $y \in D$. W.L.O.G., we can assume that $y \in C$. Since $f : A \to C$ is onto C, there exists $x \in A$ such that $(x, y) \in f$. Using ($\star$), $(f \cup g)(x) = f(x) = y$. Therefore, $f \cup g$ is onto $C \cup D$.
2. Suppose that $(x_1, y), (x_2, y) \in f \cup g \subseteq (A \times C) \cup (B \times D)$. Then $(x_1, y) \in f$ or $(x_1, y) \in g$. W.L.O.G., we can assume that $(x_1, y) \in f$. Since $f \subseteq A \times C$ and $g \subseteq B \times D$, by the fact that $C \cap D = \varnothing$ we must have $(x_2, y) \in f$ for otherwise $y \in C \cap D$, a contradiction. Now, since $(x_1, y), (x_2, y) \in f$, the injectivity of f then implies that $x_1 = x_2$. □

§4.4 Inverse Functions

Recall that the inverse of a relation $f : A \to B$ is the relation f^{-1} satisfying

$$yf^{-1}x \quad \Leftrightarrow \quad xfy \quad \Leftrightarrow \quad (x, y) \in f \quad \Leftrightarrow \quad y = f(x)\,.$$

This relation is a function, called the inverse function of f, if the relation itself is a function with certain domain.

Definition

A function $f : A \to B$ is said to be a ***one-to-one correspondence*** if f is a bijection.

§4.4 Inverse Functions

Theorem

Let $f: A \to B$ be a function.

1. *f^{-1} is a function from $\mathrm{Rng}(f)$ to A if and only if f is one-to-one.*
2. *If f^{-1} is a function, then f^{-1} is one-to-one.*

Proof.

1. "$\Rightarrow$" If $(x_1, y), (x_2, y) \in f$, then $(y, x_1), (y, x_2) \in f^{-1}$. Since f^{-1} is a function, we must have $x_1 = x_2$. Therefore, f is one-to-one. "$\Leftarrow$" If $(y, x_1), (y, x_2) \in f^{-1}$, then $(x_1, y), (x_2, y) \in f$, and the injectivity of f implies that $x_1 = x_2$. Therefore, by the fact that $\mathrm{Rng}(f) = \mathrm{Dom}(f^{-1})$, f^{-1} is a function with domain $\mathrm{Rng}(f)$.
2. Suppose that f^{-1} is a function, and $(y_1, x), (y_2, x) \in f^{-1}$. Then $(x, y_1), (x, y_2) \in f$ which, by the fact that f is a function, implies that $y_1 = y_2$. Therefore, f^{-1} is one-to-one. □

§4.4 Inverse Functions

Corollary

The inverse of a one-to-one correspondence is a one-to-one correspondence.

Theorem

Let $f : A \to B$, $g : B \to A$ be functions. Then

1. $g = f^{-1}$ *if and only if* $g \circ f = I_A$ *and* $f \circ g = I_B$ *(if and only if* $f = g^{-1}$*).*
2. *If f is surjective, and $g \circ f = I_A$, then $g = f^{-1}$.*
3. *If f is injective, and $f \circ g = I_B$, then $g = f^{-1}$.*

Recall that "If $C = \text{Rng}(f)$ and $f^{-1} : C \to A$ is a function, then $f^{-1} \circ f = I_A$ and $f \circ f^{-1} = I_C$". Therefore, the ⇒ direction in ① has already been proved.

§4.4 Inverse Functions

Proof.

We first prove the following two claims:

(a) If $g \circ f = I_A$, then $f^{-1} \subseteq g$. (b) If $f \circ g = I_B$, then $g \subseteq f^{-1}$.

To see (a), let $(y, x) \in f^{-1}$ be given. Then $(x, y) \in f$ or $y = f(x)$. Since $(g \circ f) = I_A$, we must have

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

or equivalently, $(y, x) \in g$. Therefore, $f^{-1} \subseteq g$.

To see (b), let $(y, x) \in g$ be given. Then $x = g(y)$; thus the fact that $(f \circ g) = I_B$ implies that

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

or equivalently, $(x, y) \in f$. Therefore, $(y, x) \in f^{-1}$; thus $g \subseteq f^{-1}$.

1. "$\Rightarrow$" Done.

   "$\Leftarrow$" This direction is a direct consequence of the claims. □

§4.4 Inverse Functions

Proof. (Cont'd).

2. Suppose that $f\colon A \to B$ is surjective and $g \circ f = I_A$. Then claim (a) implies that $f^{-1} \subseteq g$; thus it suffices to show that $g \subseteq f^{-1}$. Let $(y, x) \in g$. Then by the surjectivity of f there exists $x_1 \in A$ such that $y = f(x_1)$ or equivalently, $(y, x_1) \in f^{-1}$. On the other hand,
$$x = g(y) = g(f(x_1)) = (g \circ f)(x_1) = I_A(x_1) = x_1 \,.$$
Therefore, $g \subseteq f^{-1}$.
3. Now suppose that $f\colon A \to B$ is injective and $f \circ g = I_B$. Then claim (b) implies that $g \subseteq f^{-1}$; thus it suffices to show that $f^{-1} \subseteq g$. Let $(y, x) \in f^{-1}$ or equivalently, $(x, y) \in f$ or $y = f(x)$. By the fact that $f \circ g = I_B$, we have $f(g(y)) = y$; thus the injectivity of f implies that $g(y) = x$ or $(y, x) \in g$. Therefore, $f^{-1} \subseteq g$ which completes the proof. □

§4.4 Inverse Functions

Since we have shown in the previous theorem that for functions $f : A \to B$ and $g : B \to A$,

1. $g = f^{-1}$ if and only if $g \circ f = I_A$ and $f \circ g = I_B$,
2. If f is surjective, and $g \circ f = I_A$, then $g = f^{-1}$,
3. If f is injective, and $f \circ g = I_B$, then $g = f^{-1}$,

we can conclude the following

Corollary

If $f : A \to B$ is an one-to-one correspondence, and $g : B \to A$ be a function. Then $g = f^{-1}$ if and only if $g \circ f = I_A$ or $f \circ g = I_B$.

Example

Let $A = \mathbb{R}$ and $B = \{x | x \geqslant 0\}$. Define $f : A \to B$ by $f(x) = x^2$ and $g : B \to A$ by $g(y) = \sqrt{y}$. Then $f \circ g = I_B$ but g is not inverse function of f since $(g \circ f)(x) = |x|$ for all $x \in A$.

§4.4 Inverse Functions

Definition

Let A be a non-empty set. A ***permutation*** of A is a one-to-one correspondence from A onto A.

Theorem

Let A be a non-empty set. Then

1. *the identity map I_A is a permutation of A.*
2. *the composite of permutations of A is a permutation of A.*
3. *the inverse of a permutation of A is a permutation of A.*
4. *if f is a permutation of A, then $f \circ I_A = I_A \circ f = f$.*
5. *if f is a permutation of A, then $f \circ f^{-1} = f^{-1} \circ f = I_A$.*
6. *if f and g are permutations of A, then $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.*

§4.5 Set Images

Definition

Let $f: A \to B$ be a function, and $X \subseteq A$, $Y \subseteq B$. The ***image*** of X (under f) or ***image set*** of X, denoted by $f(X)$, is the set

$$f(X) = \{y \in B \,|\, y = f(x) \text{ for some } x \in X\} = \{f(x) \,|\, x \in X\},$$

and the ***pre-image*** of Y (under f) or the ***inverse image*** of Y, denoted by $f^{-1}(Y)$, is the set

$$f^{-1}(Y) = \{x \in A \,|\, f(x) \in Y\}.$$

Remark: Here are some facts about images of sets that follow from the definitions:

(a) If $a \in D$, then $f(a) \in f(D)$.

(b) If $a \in f^{-1}(E)$, then $f(a) \in E$.

(c) If $f(a) \in E$, then $a \in f^{-1}(E)$.

(d) If $f(a) \in f(D)$ and f is one-to-one, then $a \in D$.

§4.5 Set Images

Theorem

Let $f : A \to B$ be a function. Suppose that C, D are subsets of A, and E, F are subsets of B. Then

1. $f(C \cap D) \subseteq f(C) \cap f(D)$. *In particular, if $C \subseteq D$, then $f(C) \subseteq f(D)$.*
2. $f(C \cup D) = f(C) \cup f(D)$.
3. $f^{-1}(E \cap F) = f^{-1}(E) \cap f^{-1}(F)$. *In particular, if $E \subseteq F$, then $f^{-1}(E) \subseteq f^{-1}(F)$.*
4. $f^{-1}(E \cup F) = f^{-1}(E) \cup f^{-1}(F)$.
5. $C \subseteq f^{-1}(f(C))$.
6. $f(f^{-1}(E)) \subseteq E$.

§4.5 Set Images

Proof of $f(C \cap D) \subseteq f(C) \cap f(D)$.

Let $y \in f(C \cap D)$. Then there exists $x \in C \cap D$ such that $y = f(x)$. Therefore, $y \in f(C)$ and $y \in f(D)$; thus $y \in f(C) \cap f(D)$. □

Remark: It is possible that $f(C \cap D) \subsetneq f(C) \cap f(D)$. For example, $f(x) = x^2$, $C = (-\infty, 0)$ and $D = (0, \infty)$. Then $C \cap D = \varnothing$ which implies that $f(C \cap D) = \varnothing$; however, $f(C) = f(D) = (0, \infty)$.

Proof of $f(C \cup D) = f(C) \cup f(D)$.

Let $y \in B$ be given. Then

$$\begin{aligned} y \in f(C \cup D) &\Leftrightarrow (\exists\, x \in C \cup D)\big(y = f(x)\big) \\ &\Leftrightarrow (\exists\, x \in C)\big(y = f(x)\big) \vee (\exists\, x \in D)\big(y = f(x)\big) \\ &\Leftrightarrow \big(y \in f(C)\big) \vee \big(y \in f(D)\big) \\ &\Leftrightarrow y \in f(C) \cup f(D)\,. \end{aligned}$$

□

§4.5 Set Images

Proof of $f^{-1}(E \cap F) = f^{-1}(E) \cap f^{-1}(F)$.

Let $x \in A$ be given. Then

$$\begin{aligned} x \in f^{-1}(E \cap F) &\Leftrightarrow f(x) \in E \cap F \\ &\Leftrightarrow \big(f(x) \in E\big) \wedge \big(f(x) \in F\big) \\ &\Leftrightarrow \big(x \in f^{-1}(E)\big) \wedge \big(x \in f^{-1}(F)\big) \\ &\Leftrightarrow x \in f^{-1}(E) \cap f^{-1}(F)\,. \end{aligned}$$

□

Proof of $f^{-1}(E \cup F) = f^{-1}(E) \cup f^{-1}(F)$.

Let $x \in A$ be given. Then

$$\begin{aligned} x \in f^{-1}(E \cup F) &\Leftrightarrow f(x) \in E \cup F \\ &\Leftrightarrow \big(f(x) \in E\big) \vee \big(f(x) \in F\big) \\ &\Leftrightarrow \big(x \in f^{-1}(E)\big) \vee \big(x \in f^{-1}(F)\big) \\ &\Leftrightarrow x \in f^{-1}(E) \cup f^{-1}(F)\,. \end{aligned}$$

□

§4.5 Set Images

Proof of $C \subseteq f^{-1}(f(C))$.

Let $x \in C$. Then $f(x) \in f(C)$; thus $x \in f^{-1}(f(C))$. Therefore, $C \subseteq f^{-1}(f(C))$. □

Remark: It is possible that $C \subsetneq f^{-1}(f(C))$. For example, if $f(x) = x^2$ and $C = [0,1]$, then $f^{-1}(f(C)) = f^{-1}([0,1]) = [-1,1] \supsetneq [0,1]$.

Proof of $f(f^{-1}(E)) \subseteq E$.

Suppose that $y \in f(f^{-1}(E))$. Then there exists $x \in f^{-1}(E)$ such that $f(x) = y$. Since $x \in f^{-1}(E)$, there exists $z \in E$ such that $f(x) = z$. Then $y = z$ which implies that $y \in E$. Therefore, $f(f^{-1}(E)) \subseteq E$. □

Remark: It is possible that $f(f^{-1}(E)) \subsetneq E$. For example, if $f(x) = x^2$ and $E = [-1,1]$, then $f(f^{-1}(E)) = f([0,1]) = [0,1] \subsetneq [-1,1]$.

Chapter 5. Cardinality

§5.1 Equivalent Sets; Finite Sets

§5.2 Infinite Sets

§5.3 Countable Sets

§5.1 Equivalent Sets; Finite Sets

Definition

Two sets A and B are ***equivalent*** if there exists a one-to-one function from A onto B. The sets are also said to be ***in one-to-one correspondence***, and we write $A \approx B$. In notation,

$$A \approx B \Leftrightarrow (\exists\, f\colon A \to B)(f \text{ is a bijection}).$$

If A and B are not equivalent, we write $A \not\approx B$.

Example

The set of even integers is equivalent to the set of odd integers: the function $f(x) = x + 1$ does the job.

Example

The set of even numbers is equivalent to the set of integers: the function $f(x) = \dfrac{x}{2}$ does the job.

§5.1 Equivalent Sets; Finite Sets

Example

The set of natural numbers is equivalent to the set of integers.

Example

For $a, b, c, d \in \mathbb{R}$, with $a < b$ and $c < d$, the open intervals (a, b) and (c, d) are equivalent. Therefore, any two open intervals are equivalent, even when the intervals have different length.

Example

Let $\mathcal{F}$ be the set of all binary sequences; that is, the set of all functions from $\mathbb{N} \to \{0, 1\}$. Then $\mathcal{F} \approx \mathcal{P}(\mathbb{N})$, the power set of $\mathbb{N}$. To see this, we define $\phi : \mathcal{F} \to \mathcal{P}(\mathbb{N})$ by $\phi(x) \equiv \left\{k \in \mathbb{N} \,\middle|\, x_k = 1\right\}$ for all $x \in \mathcal{F}$. Then ϕ is well-defined and $\phi : \mathcal{F} \xrightarrow[onto]{1-1} \mathcal{P}(\mathbb{N})$.

§5.1 Equivalent Sets; Finite Sets

Theorem

Equivalence of sets is an equivalence relation on the class of all sets.

Proof.

1. **Reflexivity**: for all sets A, the identity map I_A is an one-to-one correspondence on A.
2. **Symmetry**: Suppose that $A \approx B$; that is, there exists a one-to-one correspondence ϕ from A to B. Then ϕ^{-1} is an one-to-one correspondence from B to A; thus $B \approx A$.
3. **Transitivity**: Suppose that $A \approx B$ and $B \approx C$. Then there exist one-to-one correspondences $\phi : A \xrightarrow[onto]{1-1} B$ and $\psi : B \xrightarrow[onto]{1-1} C$. Then $\psi \circ \phi : A \to C$ is an one-to-one correspondence; thus $A \approx C$.

□

§5.1 Equivalent Sets; Finite Sets

Lemma

Suppose that A, B, C and D are sets with $A \approx C$ and $B \approx D$.

1. *If A and B are disjoint and C and D are disjoint, then $A \cup B \approx C \cup D$.*
2. $A \times B \approx C \times D$.

Proof.

Suppose that $\phi : A \xrightarrow[onto]{1-1} C$ and $\psi : B \xrightarrow[onto]{1-1} D$.

1. Then $\phi \cup \psi : A \cup B \to C \cup D$ is an one-to-one correspondence.
2. Let $f \colon A \times B \to C \times D$ be given by
$$f(a, b) = \big(\phi(a), \psi(b)\big) .$$
Then f is an one-to-one correspondence from $A \times B$ to $C \times D$.

□

§5.1 Equivalent Sets; Finite Sets

Definition

For each natural number k, let $\mathbb{N}_k = \{1, 2, \cdots, k\}$. A set S is ***finite*** if $S = \varnothing$ or $S \approx \mathbb{N}_k$ for some $k \in \mathbb{N}$. A set S is ***infinite*** if S is not a finite set.

Theorem

For $k, j \in \mathbb{N}$, $\mathbb{N}_j \approx \mathbb{N}_k$ if and only if $k = j$.

Proof.

It suffices to prove the $\Rightarrow$ direction. Suppose that $\phi : \mathbb{N}_k \to \mathbb{N}_j$ is a one-to-one correspondence. W.L.O.G. we can assume that $k \leqslant j$. If $k < j$, then $\phi(\mathbb{N}_k) = \big\{\phi(1), \phi(2), \cdots, \phi(k)\big\} \neq \mathbb{N}_j$ since the number of elements in $\phi(\mathbb{N}_k)$ and $\mathbb{N}_j$ are different. In other words, if $k < j$, $\phi : \mathbb{N}_k \to \mathbb{N}_j$ cannot be surjective. This implies that $\mathbb{N}_k \approx \mathbb{N}_j$ if and only if $k = j$. □

§5.1 Equivalent Sets; Finite Sets

Definition

Let S be a finite set. If $S = \varnothing$, then S has ***cardinal number*** 0 (or ***cardinality*** 0), and we write $\#S = 0$. If $S \approx \mathbb{N}_k$ for some natural number k, then S has ***cardinal number*** k (or ***cardinality*** k), and we write $\#S = k$.

Remark: The cardinality of a set S can also be denoted by $n(S)$, $\overline{\overline{S}}$, $\text{card}(S)$ as well.

Theorem

If A is finite and $B \approx A$, then B is finite.

Lemma

If S is a finite set with cardinality k and x is any object not in S, then $S \cup \{x\}$ is finite and has cardinality $k+1$.

§5.1 Equivalent Sets; Finite Sets

Lemma

For every $k \in \mathbb{N}$, every subset of $\mathbb{N}_k$ is finite.

Proof.

Let $S = \left\{ k \in \mathbb{N} \,\middle|\, \text{the statement “every subset of } \mathbb{N}_k \text{ is finite” holds} \right\}$.

1. There are only two subsets of $\mathbb{N}_1$, namely $\varnothing$ and $\mathbb{N}_1$. Since $\varnothing$ and $\mathbb{N}_1$ are both finite, we have $1 \in S$.
2. Suppose that $k \in S$. Then every subset of $\mathbb{N}_k$ is finite. Since $\mathbb{N}_{k+1} = \mathbb{N}_k \cup \{k+1\}$, every subset of $\mathbb{N}_{k+1}$ is either a subset of $\mathbb{N}_k$, or the union of a subset of $\mathbb{N}_k$ and $\{k+1\}$. By the fact that $k \in S$, we conclude from the previous lemma that every subset of $\mathbb{N}_{k+1}$ is finite.

Therefore, **PMI** implies that $S = \mathbb{N}$. □

§5.1 Equivalent Sets; Finite Sets

Theorem

Every subset of a finite set is finite.

Proof.

Let $A \subseteq B$ and B is a finite set.

1. If $A = \varnothing$, then A is a finite set (and $\#A = 0$).
2. If $A \neq \varnothing$, then $B \neq \varnothing$. Since B is finite, there exists $k \in \mathbb{N}$ such that $B \approx N_k$; thus there exists a one-to-one correspondence $\phi : \mathbb{N}_k \to B$. Therefore, $\phi^{-1}(A)$ is a non-empty subset of $\mathbb{N}_k$, and the previous lemma implies that $\phi^{-1}(A)$ is finite. Since $A \approx \phi^{-1}(A)$, we conclude that A is a finite set. □

§5.1 Equivalent Sets; Finite Sets

Theorem

1. *If A and B are disjoint finite sets, then $A \cup B$ is finite, and*
$$\#(A \cup B) = \#A + \#B .$$
2. *If A and B are finite sets, then $A \cup B$ is finite, and*
$$\#(A \cup B) = \#A + \#B - \#(A \cap B) .$$
3. *If $A_1, A_2, \cdots, A_n$ are finite sets, then $\bigcup_{k=1}^{n} A_k$ is finite.*

Proof.

1. W.L.O.G., we assume that $A \approx \mathbb{N}_k$ and $B \approx \mathbb{N}_\ell$ for some $k, \ell \in \mathbb{N}$. Let $H = \{k+1, k+2, \cdots, k+\ell\}$. Then $\mathbb{N}_\ell \approx H$ since $\phi(x) = k + x$ is a one-to-one correspondence from $\mathbb{N}_\ell \to \{k+1, k+2, \cdots, k+\ell\}$. Therefore, $A \cup B \approx \mathbb{N}_k \cup H = \mathbb{N}_{k+\ell}$; thus $\#(A \cup B) = \#A + \#B$. □

§5.1 Equivalent Sets; Finite Sets

Proof of $\#(A \cup B) = \#A + \#B - \#(A \cap B)$.

2. Note that $A \cup B$ is the disjoint union of A and $B - A$, where $B - A$ is a subset of a finite set B which makes $B - A$ a finite set. Therefore, $A \cup B$ is finite.

   To see $\#(A \cup B) = \#A + \#B - \#(A \cap B)$, using ① it suffices to show that $\#(B - A) = \#B - \#(A \cap B)$. Nevertheless, note that $B = (B - A) \cup (A \cap B)$ in which the union is in fact a disjoint union; thus ① implies that

   $$\#B = \#(B - A) + \#(A \cap B)$$

   or equivalently,

   $$\#(B - A) = \#B - \#(A \cap B)\,.$$

□

§5.1 Equivalent Sets; Finite Sets

Proof.

3. Let $A_1, A_2, \cdots$ be finite sets, and

$$S = \left\{ n \in \mathbb{N} \,\middle|\, \bigcup_{k=1}^{n} A_k \text{ is finite} \right\}.$$

Then $1 \in S$ by assumption. Suppose that $n \in S$. Then $n+1 \in S$ because of ②. **PMI** then implies that $S = \mathbb{N}$. □

§5.1 Equivalent Sets; Finite Sets

Lemma

Let $k \geqslant 2$ be a natural number. For $x \in \mathbb{N}_k$, $\mathbb{N}_k \backslash \{x\} \approx \mathbb{N}_{k-1}$.

Theorem (Pigeonhole Principle - 鴿籠原理)

Let $n, r \in \mathbb{N}$ and $f : \mathbb{N}_n \to \mathbb{N}_r$ be a function. If $n > r$, then f is not injective.

Corollary

If $\#A = n$, $\#B = r$ and $r < n$, then there is no one-to-one function from A to B.

Corollary

If A is finite, then A is not equivalent to any of its proper subsets.

§5.2 Infinite Sets

Recall that a set A is infinite if A is not finite. By the last corollary in the previous section, if a set is equivalent to one of its proper subset, then that set cannot be finite. Therefore, $\mathbb{N}$ is not finite since there is a one-to-one correspondence from $\mathbb{N}$ to the set of even numbers.

The set of natural numbers $\mathbb{N}$ is a set with infinite cardinality. The standard symbol for the cardinality of $\mathbb{N}$ is $\aleph$. There are two kinds of infinite sets, denumerable（無窮可數）sets and uncountable（不可數）sets.

Definition

A set S is said to be ***denumerable*** if $S \approx \mathbb{N}$. For a denumerable set S, we say S has cardinal number $\aleph_0$ (or cardinality $\aleph_0$) and write $\#S = \aleph_0$.

§5.2 Infinite Sets

Example

The set of even numbers and the set of odd numbers are denumerable.

Example

The set $\{p, q, r\} \cup \{n \in \mathbb{N} \mid n \neq 5\}$ is denumerable.

Theorem

The set $\mathbb{Z}$ is denumerable.

Proof.

Consider the function $f : \mathbb{N} \to \mathbb{Z}$ given by

$$f(x) = \begin{cases} \dfrac{x}{2} & \text{if } x \text{ is even}\,, \\ \dfrac{1-x}{2} & \text{if } x \text{ is odd}\,. \end{cases}$$

□

§5.2 Infinite Sets

Theorem

1. *The set* $\mathbb{N} \times \mathbb{N}$ *is denumerable.*
2. *If* A *and* B *are denumerable sets, then* $A \times B$ *is denumerable.*

Proof.

1. Consider the function $F : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ defined by $F(m, n) = 2^{m-1}(2n - 1)$. Then $F : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ is bijective.
2. If A and B are denumerable sets, then $A \approx \mathbb{N}$ and $B \approx \mathbb{N}$. Then $A \times B \approx \mathbb{N} \times \mathbb{N}$; thus $A \times B \approx \mathbb{N}$ since $\approx$ is an equivalence relation. □

Definition

A set S is said to be ***countable*** if S is finite or denumerable. We say S is ***uncountable*** if S is not countable.

§5.2 Infinite Sets

Theorem

The open interval $(0,1)$ *is uncountable.*

Proof.

Assume the contrary that there exists a bijection $f:\mathbb{N}\to(0,1)$. Write $f(k)$ in decimal expansion (十進位展開); that is,

$$\begin{aligned} f(1) &= 0.d_{11}d_{21}d_{31}\cdots \\ f(2) &= 0.d_{12}d_{22}d_{32}\cdots \\ &\ \ \vdots \\ f(k) &= 0.d_{1k}d_{2k}d_{3k}\cdots \\ &\ \ \vdots \end{aligned}$$

Here we note that repeated 9's are chosen by preference over terminating decimals; that is, for example, we write $\frac{1}{4}=0.249999\cdots$ instead of $\frac{1}{4}=0.250000\cdots$. □

§5.2 Infinite Sets

Proof. (Cont'd).

Let $x \in (0,1)$ be such that $x = 0.d_1 d_2 \cdots$, where

$$d_k = \begin{cases} 5 & \text{if} \quad d_{kk} \neq 5\,, \\ 3 & \text{if} \quad d_{kk} = 5\,. \end{cases}$$

（建構一個 x 使其小數點下第 k 位數與 $f(k)$ 的小數點下第 k 位數不相等）. Then $x \neq f(k)$ for all $k \in \mathbb{N}$, a contradiction; thus $(0,1)$ is uncountable. □

Definition

A set S has cardinal number $\mathbf{c}$ (or cardinality $\mathbf{c}$) if S is equivalent to $(0,1)$. We write $\#S = \mathbf{c}$, which stands for ***continuum***.

§5.2 Infinite Sets

Theorem

1. *Even open interval (a, b) is uncountable and has cardinality* $\mathbf{c}$.
2. *The set $\mathbb{R}$ of all real numbers is uncountable and has cardinality* $\mathbf{c}$.

Proof.

1. The function $f(x) = a + (b - a)x$ maps from $(0, 1)$ to (a, b) and is a one-to-one correspondence.
2. Using ①, $(0, 1) \approx \left(-\frac{\pi}{2}, \frac{\pi}{2}\right)$. Moreover, the function $f(x) = \tan x$ maps from $\left(-\frac{\pi}{2}, \frac{\pi}{2}\right)$ to $\mathbb{R}$ and is a one-to-one correspondence; thus $\left(-\frac{\pi}{2}, \frac{\pi}{2}\right) \approx \mathbb{R}$. Since $\approx$ is an equivalence relation, $(0, 1) \approx \mathbb{R}$. □

§5.2 Infinite Sets

Example

The circle with the north pole removed is equivalent to the real line.

Example

The set $A = (0,2) \cup [5,6)$ has cardinality $\mathbf{c}$ since the function $f\colon (0,1) \to A$ given by

$$f(x) = \begin{cases} 4x & \text{if } 0 < x < \dfrac{1}{2}, \\ 2x+4 & \text{if } \dfrac{1}{2} \leqslant x < 1 \end{cases}$$

is a one-to-one correspondence from $(0,1)$ to A.

§5.3 Countable Sets

Theorem

Let S be a non-empty set. The following statements are equivalent:

1. *S is countable;*
2. *there exists a surjection $f\colon \mathbb{N} \to S$;*
3. *there exists an injection $f\colon S \to \mathbb{N}$.*

Proof.

"① ⇒ ②" First suppose that $S = \{x_1, \cdots, x_n\}$ is finite. Define $f\colon \mathbb{N} \to S$ by

$$f(k) = \begin{cases} x_k & \text{if } k < n\,, \\ x_n & \text{if } k \geqslant n\,. \end{cases}$$

Then $f : \mathbb{N} \to S$ is a surjection. Now suppose that S is denumerable. Then by definition of countability, there exists $f\colon \mathbb{N} \xrightarrow[\textit{onto}]{1-1} S$.

□

§5.3 Countable Sets

1. S is countable;
2. there exists a surjection $f\colon \mathbb{N} \to S$;

Proof. (Cont'd).

"①$\Leftarrow$②" W.L.O.G. we assume that S is an infinite set. Let $k_1 = 1$. Since $\#(S) = \infty$, $S_1 \equiv S - \{f(k_1)\} \neq \varnothing$; thus $N_1 \equiv f^{-1}(S_1)$ is a non-empty subset of $\mathbb{N}$. By the well-ordered principle (**WOP**) of $\mathbb{N}$, N_1 has a smallest element denoted by k_2. Since $\#(S) = \infty$, $S_2 = S - \{f(k_1), f(k_2)\} \neq \varnothing$; thus $N_2 \equiv f^{-1}(S_2)$ is a non-empty subset of $\mathbb{N}$ and possesses a smallest element denoted by k_3. We continue this process and obtain a set $\{k_1, k_2, \cdots\} \subseteq \mathbb{N}$, where $k_1 < k_2 < \cdots$, and k_j is the smallest element of $N_{j-1} \equiv f^{-1}(S - \{f(k_1), f(k_2), \cdots, f(k_{j-1})\})$. □

§5.3 Countable Sets

Proof. (Cont'd).

Claim: $f\colon\{k_1,k_2,\cdots\}\to S$ is one-to-one and onto.

Proof of claim: The injectivity of f is easy to see since $f(k_j)\notin\{f(k_1),f(k_2),\cdots,f(k_{j-1})\}$ for all $j\geqslant 2$. For surjectivity, assume the contrary that there is $s\in S$ such that $s\notin f(\{k_1,k_2,\cdots\})$. Since $f\colon\mathbb{N}\to\mathbb{S}$ is onto, $f^{-1}(\{s\})$ is a non-empty subset of $\mathbb{N}$; thus possesses a smallest element k. Since $s\notin f(\{k_1,k_2,\cdots\})$, there exists $\ell\in\mathbb{N}$ such that $k_\ell<k<k_{\ell+1}$. Therefore, $k\in N_\ell$ and $k<k_{\ell+1}$ which contradicts to the fact that $k_{\ell+1}$ is the smallest element of N_ℓ. □

Let $g:\mathbb{N}\to\{k_1,k_2,\cdots\}$ be defined by $g(j)=k_j$. Then g is one-to-one and onto; thus $h=g\circ f\colon\mathbb{N}\xrightarrow[onto]{1-1}S$. □

§5.3 Countable Sets

1. S is countable;
3. there exists an injection $f\colon S \to \mathbb{N}$.

Proof. (Cont'd).

"① ⇒ ③" If $S = \{x_1, \cdots, x_n\}$ is finite, we simply let $f\colon S \to \mathbb{N}$ be $f(x_n) = n$. Then f is clearly an injection. If S is denumerable, by definition there exists $g : \mathbb{N} \xrightarrow[onto]{1-1} S$ which implies that $f = g^{-1} : S \to \mathbb{N}$ is an injection. □

§5.3 Countable Sets

1. S is countable;
3. there exists an injection $f\colon S \to \mathbb{N}$.

Proof. (Cont'd).

"①$\Leftarrow$③" Let $f\colon S \to \mathbb{N}$ be an injection. If f is also surjective, then $f\colon S \xrightarrow[onto]{1-1} \mathbb{N}$ which implies that S is denumerable. Now suppose that $f(S) \subsetneq \mathbb{N}$. Since S is non-empty, there exists $s \in S$. Let $g : \mathbb{N} \to S$ be defined by

$$g(n) = \begin{cases} f^{-1}(n) & \text{if } n \in f(S)\,, \\ s & \text{if } n \notin f(S)\,. \end{cases}$$

Then clearly $g : \mathbb{N} \to S$ is surjective; thus the equivalence between ① and ② implies that S is countable. □

§5.3 Countable Sets

Example

We have seen that the set $\mathbb{N} \times \mathbb{N}$ is countable. Now consider the map $f\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ defined by $f(m,n) = 2^m 3^n$. This map is not a bijection; however, it is an injection; thus the theorem above implies that $\mathbb{N} \times \mathbb{N}$ is countable.

Example

The set $\mathbb{Q}^+$ of positive rational numbers is denumerable. Since $\mathbb{Q}^+$ is infinite, it suffice to check the countability of $\mathbb{Q}^+$. Consider the map $f\colon \mathbb{N}^2 \to \mathbb{Q}^+$ defined by $f(m,n) = \dfrac{m}{n}$. Then f is onto $\mathbb{Q}^+$; thus the theorem above implies that $\mathbb{Q}^+$ is countable.

§5.3 Countable Sets

Theorem

Any non-empty subset of a countable set is countable.

Proof.

Let S be a countable set, and A be a non-empty subset of S. Since S is countable, by the previous theorem there exists a surjection $f : \mathbb{N} \to S$. On the other hand, since A is a non-empty subset of S, there exists $a \in A$. Define

$$g(x) = \begin{cases} x & \text{if } x \in A\,, \\ a & \text{if } x \notin A\,. \end{cases}$$

Then $g : S \to A$ is a surjection; thus $h = g \circ f : \mathbb{N} \to A$ is also a surjection. The previous theorem shows that A is countable. □

Corollary

A set A is countable if and only if $A \approx S$ for some $S \subseteq \mathbb{N}$.

§5.3 Countable Sets

Theorem

The union of denumerable denumerable sets is denumerable. In other words, if $\mathcal{F}$ is a denumerable collection of denumerable sets, then $\bigcup\limits_{A\in\mathcal{F}} A$ is denumerable.

Proof.

Let $\mathcal{F} = \left\{A_i \,\middle|\, i \in \mathbb{N}, A_i \text{ is denumerable}\right\}$ be an indexed family of denumerable sets, and define $A = \bigcup\limits_{i=1}^{\infty} A_i$. Since A_i is denumerable, we write $A_i = \{x_{i1}, x_{i2}, x_{i3}, \cdots\}$. Then $A = \left\{x_{ij} \,\middle|\, i, j \in \mathbb{N}\right\}$. Let $f : \mathbb{N}\times\mathbb{N} \to A$ be defined by $f(i,j) = x_{ij}$. Then $f : \mathbb{N}\times\mathbb{N} \to A$ is a surjection. Moreover, since $\mathbb{N}\times\mathbb{N} \approx \mathbb{N}$, there exists a bijection $g : \mathbb{N} \to \mathbb{N}\times\mathbb{N}$; thus $h = f\circ g : \mathbb{N} \to A$ is a surjection which implies that A is countable. Since $A_1 \subseteq A$, A is infinite; thus A is denumerable. □

§5.3 Countable Sets

Corollary

The union of countable countable sets is countable（可數個可數集的聯集是可數的）.

Proof.

By adding empty sets into the family or adding $\mathbb{N}$ into a finite set if necessary, we find that the union of countable countable sets is a subset of the union of denumerable denumerable sets. Since a (non-empty) subset of a countable set is countable, we find that the union of countable countable sets is countable. □

§5.3 Countable Sets

Corollary

The set of rational numbers $\mathbb{Q}$ is countable.

Proof.

Let $\mathbb{Q}^+$ and $\mathbb{Q}^-$ denote the collection of positive and negative rational numbers, respectively. We have shown that the set $\mathbb{Q}^+$ is countable. Since $\mathbb{Q}^+ \approx \mathbb{Q}^-$ (between them there exists a one-to-one correspondence $f(x) = -x$), $\mathbb{Q}^-$ is also countable. Therefore, the previous theorem $\mathbb{Q} = \mathbb{Q}^+ \cup \mathbb{Q}^- \cup \{0\}$ is countable. □

§5.3 Countable Sets

Corollary

1. *If $\mathfrak{F}$ is a finite pairwise disjoint family of denumerable sets, then $\bigcup\limits_{A\in\mathfrak{F}} A$ is countable.*
2. *If A and B are countable sets, then $A \cup B$ is countable.*
3. *If $\mathfrak{F}$ is a finite collection of countable sets, then $\bigcup\limits_{A\in\mathfrak{F}} A$ is countable.*
4. *If $\mathfrak{F}$ is a denumerable family of countable sets, then $\bigcup\limits_{A\in\mathfrak{F}} A$ is countable.*