基礎數學 MA-1015A

Chapter 1. Logic and Proofs

§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 true / false exactly when P is false / true.

Definition

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

§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, $(\mathrm{P} \wedge \mathrm{Q}) \vee (\sim\mathrm{R})$ is true.

§1.1 Propositions and Connectives

Definition

A ***tautology*** / ***contradiction*** is a propositional form that is true / false for every assignment of truth values to its component.

Example

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

Example

The logic symbol $\sim(P \vee \sim P) \vee (Q \wedge \sim Q)$ 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) $P \Leftrightarrow \sim(\sim P)$. (**Double Negation Law**)

(b) $P \vee Q \Leftrightarrow Q \vee P$
(c) $P \wedge Q \Leftrightarrow Q \wedge P$
(**Commutative Laws**)

(d) $P \vee (Q \vee R) \Leftrightarrow (P \vee Q) \vee R$
(e) $P \wedge (Q \wedge R) \Leftrightarrow (P \wedge Q) \wedge R$
(**Associative Laws**)

(f) $P \wedge (Q \vee R) \Leftrightarrow (P \wedge Q) \vee (P \wedge R)$
(g) $P \vee (Q \wedge R) \Leftrightarrow (P \vee Q) \wedge (P \vee R)$
(**Distributive Laws**)

(h) $\sim(P \wedge Q) \Leftrightarrow (\sim P) \vee (\sim Q)$
(i) $\sim(P \vee Q) \Leftrightarrow (\sim P) \wedge (\sim Q)$
(**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	$Q \wedge R$	$P \vee (Q \wedge R)$	$P \vee Q$	$P \vee R$	$(P \vee Q) \wedge (P \vee R)$
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 "$P \vee (Q \wedge R)$" is equivalent to "$(P \vee Q) \wedge (P \vee R)$". □

§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 $P \Rightarrow Q$ 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 $P \Rightarrow Q$ is $Q \Rightarrow P$.
2. The ***contrapositive*** of $P \Rightarrow Q$ is $\sim Q \Rightarrow \sim P$.

§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* $P \Rightarrow Q$ *is equivalent to its contrapositive* $\sim Q \Rightarrow \sim P$.

Proof.

Using the truth table

P	Q	$P \Rightarrow Q$	$\sim Q$	$\sim P$	$\sim Q \Rightarrow \sim P$
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 $P \Rightarrow Q$ and $\sim Q \Rightarrow \sim P$ 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	$\mathrm{P} \Leftrightarrow \mathrm{Q}$	$\mathrm{P} \Rightarrow \mathrm{Q}$	$\mathrm{Q} \Rightarrow \mathrm{P}$	$(\mathrm{P} \Rightarrow \mathrm{Q}) \wedge (\mathrm{Q} \Rightarrow \mathrm{P})$
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

$$\text{“}(\forall\, x)\big(\mathrm{P}(x) \Rightarrow \mathrm{Q}(x)\big)\text{”}.$$

(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

$$\text{“}(\exists\, x)\big(\mathrm{P}(x) \wedge \mathrm{Q}(x)\big)\text{”}.$$

§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

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

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

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

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

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

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 $P \Rightarrow Q$, 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 $\mathrm{P} \Rightarrow \mathrm{Q}$ 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)

⋮

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 contradction**:

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：證明在一個宴會中，有兩人在該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 $P \Leftrightarrow Q$; that is, one might establish

$$(P \Leftrightarrow R_1) \wedge (R_1 \Leftrightarrow R_2) \wedge \cdots \wedge (R_{n-1} \Leftrightarrow R_n) \wedge (R_n \Leftrightarrow Q)$$

to prove $P \Leftrightarrow Q$.

2. Often times it is more efficient to show a theorem of the form "P_1, P_2, $\cdots$, P_n are equivalent" (which means P_1, P_2, $\cdots$, P_n have the same truth value) by showing that $P_1 \Rightarrow P_2$, $P_2 \Rightarrow P_3$, $\cdots$, and $P_n \Rightarrow P_1$. In other words, one uses the following relation

$$\big[(P_1 \Leftrightarrow P_2) \wedge (P_2 \Leftrightarrow P_3) \wedge \cdots \wedge (P_{n-1} \Leftrightarrow P_n)\big]$$
$$\Leftrightarrow \big[(P_1 \Rightarrow P_2) \wedge (P_2 \Rightarrow P_3) \wedge \cdots \wedge (P_n \Rightarrow P_1)\big]$$

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 make 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. $\square$

§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 $(P \Rightarrow Q_1 \vee Q_2)$: Note that

$$(P \Rightarrow Q_1 \vee Q_2) \Leftrightarrow \big[(P \wedge \sim Q_1) \Rightarrow Q_2\big].$$

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,

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

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 - 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. $b = aq_1 + r_1, \quad a = r_1 q_2 + r_2, \quad r_1 = r_2 q_3 + r_3, \quad \cdots\cdots,$
   $r_{k-3} = r_{k-2} q_{k-1} + r_{k-1}, \quad r_{k-2} = r_{k-1} q_k + r_k,$
   $r_{k-1} = r_k q_{k+1}$ *(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

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

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

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

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.