基礎數學 MA-1015A

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 $\{x \mid x \in \mathbb{N}, x \text{ is odd, and } x < 14\}$ or $\{x \in \mathbb{N} \mid x \text{ is odd, and } x < 14\}$.

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 contraposition

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
$$\big[(\mathrm{P} \Rightarrow \mathrm{Q}) \wedge (\mathrm{Q} \Rightarrow \mathrm{R})\big] \Rightarrow (\mathrm{P} \Rightarrow \mathrm{R})\,.$$

□

§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 $A = \emptyset$; 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

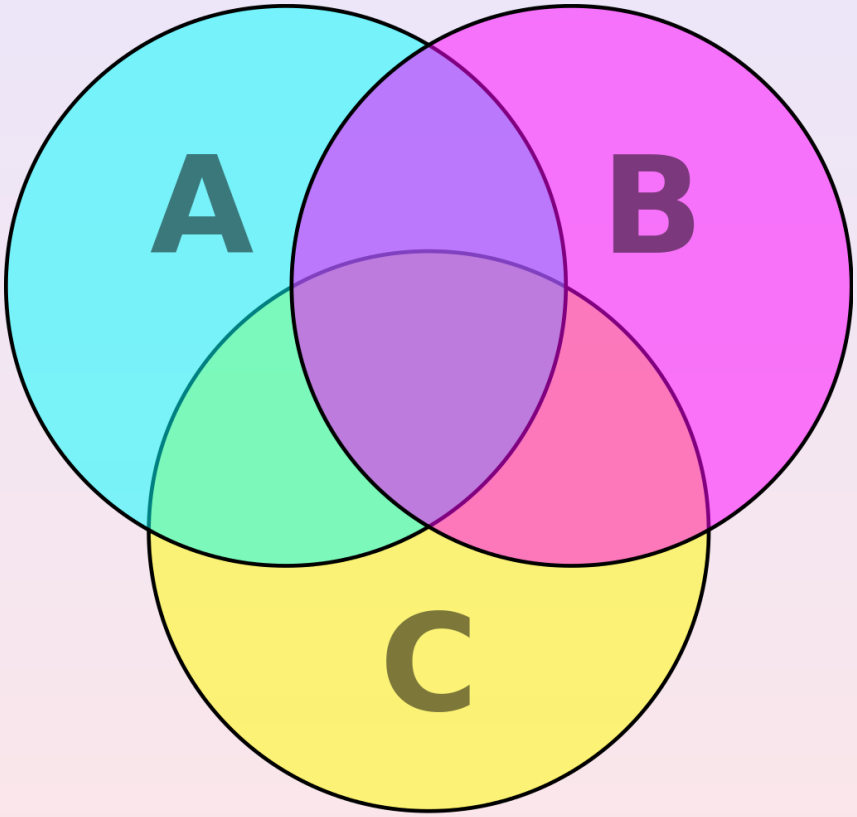
For any sets A and B, if $A \subseteq B$ and $A \neq \emptyset$, then $B \neq \emptyset$.

Proof.

Let A, B be sets, $A \subseteq B$, and $A \neq \emptyset$. 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, $B \neq \emptyset$. □

§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, $\mathcal{P}(A) \equiv \{B \mid B \subseteq A\}$.

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.

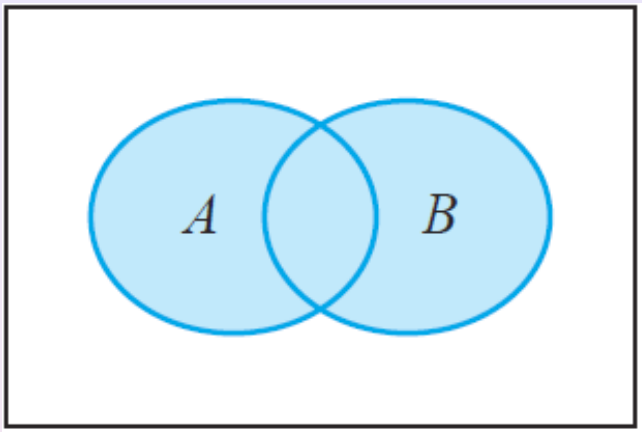
1. The **union of A and B**, denoted by $A \cup B$, is the set
$$\left\{x \middle| (x \in A) \vee (x \in B)\right\}.$$
2. The **intersection of A and B**, denoted by $A \cap B$, is the set
$$\left\{x \middle| (x \in A) \wedge (x \in B)\right\}.$$
3. The **difference of A and B**, denoted by $A - B$,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

Definition

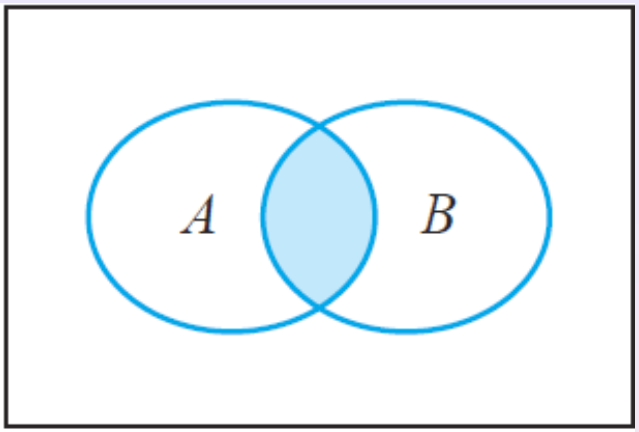
Two sets A and B are said to be ***disjoint*** if $A \cap B = \varnothing$.

§2.2 Set Operations

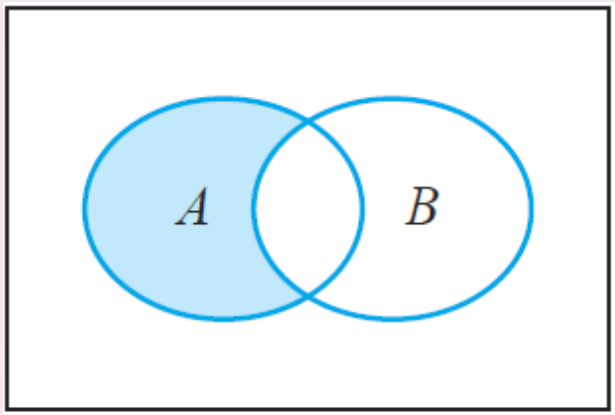
- Venn diagrams:



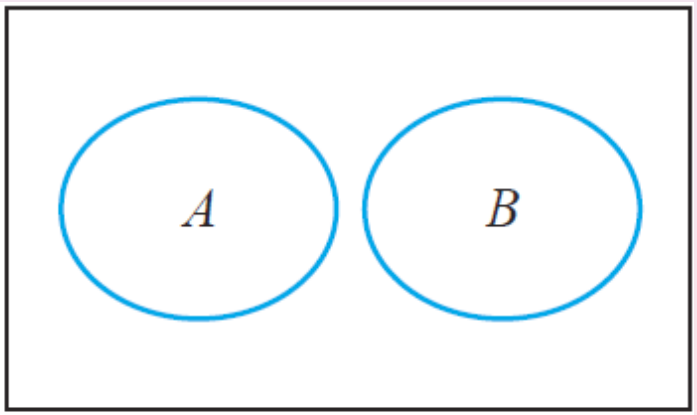
$A \cup B$



$A \cap B$



$A - B$



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) $\varnothing \backslash A = \varnothing$;

(i) $A \cup B = B \cup A$;
(j) $A \cap B = B \cap A$;
} **(commutative laws)**

(k) $A \cup (B \cup C) = (A \cup B) \cup C$;
(ℓ) $A \cap (B \cap C) = (A \cap B) \cap C$;
} **(associative laws)**

(m) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$;
(n) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$;
} **(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

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

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 $\left[(\mathrm{P} \wedge \mathrm{Q}) \vee (\mathrm{P} \wedge \mathrm{R})\right]$ 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

Alternative 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,

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

§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* $A \subseteq B^{\complement}$

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

(h) $(A \cap B)^{\complement} = A^{\complement} \cup B^{\complement}$.

(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) $(A \cup B)^C = A^C \cap B^C$.

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

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

Alternative proof of (g) $(A \cup B)^C = A^C \cap B^C$.

Let x be an element in the universe.

$x \in (A \cup B)^C$ if and only if $x \notin A \cup B$

if and only if it is not the case that $x \in A$ or $x \in B$

if and only if $x \notin A$ and $x \notin B$

if and only if $x \in A^C$ and $x \in B^C$

if and only if $x \in A^C \cap B^C$. $\square$

§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

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

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

§2.3 Indexed Family of Sets

Theorem

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

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

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

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

(d) $\left(\bigcap_{A\in\mathcal{F}} A\right)^{\complement} = \bigcup_{A\in\mathcal{F}} A^{\complement}$.

(e) $\left(\bigcup_{A\in\mathcal{F}} A\right)^{\complement} = \bigcap_{A\in\mathcal{F}} A^{\complement}$.

(De Morgan's Law)

§2.3 Indexed Family of Sets

Proof of (d) $\left(\bigcap_{A\in\mathcal{F}} A\right)^{C} = \bigcup_{A\in\mathcal{F}} A^{C}$.

Let x be an element in the universe. Then

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

□

§2.3 Indexed Family of Sets

Theorem

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

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

Proof.

1. Suppose that $B \subseteq A$ for all $A \in \mathcal{F}$, and $x \in B$. Then $x \in A$ for all $A \in \mathcal{F}$. Therefore, $(\forall\, A \in \mathcal{F})(x \in A)$ or equivalently, $x \in \bigcap_{A \in \mathcal{F}} A$.
2. Supposethat $A \subseteq B$ for all $A \in \mathcal{F}$, and $x \in \bigcup_{A \in \mathcal{F}} A$.Then $x \in A$ for some $A \in \mathcal{F}$. 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 $\bigcup_{A\in\mathcal{F}} A = \mathbb{R}$ and $\bigcap_{A\in\mathcal{F}} = [0,1)$. $\left(\text{We also write } \bigcup_{A\in\mathcal{F}} A \text{ and } \bigcap_{A\in\mathcal{F}} A \text{ as } \bigcup_{r\geqslant 0}[-r, r^2+1) \text{ and } \bigcap_{r\geqslant 0}[-r, r^2+1), \text{ respectively.}\right)$

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, $\mathbb{R} \subseteq \bigcup_{A\in\mathcal{F}} A$.
2. If $x \in [0,1)$, then $x \in [-r, r^2+1)$ for all $r \geqslant 0$; thus $[0,1) \subseteq \bigcap_{A\in\mathcal{F}} A$. If $x \in \bigcap_{A\in\mathcal{F}} A$, 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 $\{A_\alpha \mid \alpha \in \Delta\}$ 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 $\mathcal{F} = \{A_\alpha \mid \alpha \in \Delta\}$ is an indexed family of sets, we also write $\bigcup_{A \in \mathcal{F}} A$ as $\bigcup_{\alpha \in \Delta} A_\alpha$ and write $\bigcap_{A \in \mathcal{F}} A$ as $\bigcap_{\alpha \in \Delta} A_\alpha$.

§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 $n \in \mathbb{N}$, $\prod_{k=1}^{n+1} x_k = \left(\prod_{k=1}^{n} x_k \right) \cdot x_{n+1}$.

§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 $S = \{n \in \mathbb{N} \mid n^2 - n - 20 > 0\}$.

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 $S = \{n \in \mathbb{N} \mid n \geqslant 6\}$. □

§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 $\varnothing$.

§2.5 Equivalent Forms of Induction

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** $\Rightarrow$ **WOP** $\Rightarrow$ **PCI** $\Rightarrow$ **PMI**.

§2.5 Equivalent Forms of Induction

Proof of PMI $\Rightarrow$ 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 $T_0 = \left\{ n \in \mathbb{N} \middle| \{1, 2, \cdots, n\} \subseteq T \right\}$ (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

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

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 the property above, $k \in S$ 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

$$\text{(a) } 1 \in S, \text{ and} \qquad \text{(b) } n+1 \in S \text{ whenever } n \in S.$$

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

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

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,

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

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 $0 \notin S$ (so 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 $q_1 = q_2$. □