Method

(1) Prove based on the definition.

(2) Use known set equalities or inclusions and prove through set algebra

e.g. **Example 3 proof:**

(1) **A ∪ B=B ∪ A (**Commutative Law of Union**)**

Proof: We need to prove that both $A \cup B \subseteq B \cup A$ and $B \cup A \subseteq A \cup B$ hold

$\forall x \quad x \in A \cup B$

$\Rightarrow x \in A$ or $x \in B$, Then $x \in B$ or $x \in A$

$\Rightarrow x \in B \cup A$

Thus, we have proven that $A \cup B \subseteq B \cup A$.

Similarly, we can prove that $B \cup A \subseteq A \cup B$.

(2) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ (Distributive Law of Union over Intersection)

Proof: We need to proof $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$ and $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$

$\forall x \quad x \in A \cup (B \cap C)$

$\Rightarrow x \in A$ *or* $(x \in B$ *and* $x \in C)$

$\Rightarrow (x \in A$ *or* $x \in B)$ *and* $(x \in A$ *or* $x \in C)$

$\Rightarrow x \in (A \cup B) \cap (A \cup C)$

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

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

(3) $A \cup E = E$ (Union with the Universal Set)

Proof: According to the definition of union, we have $E \subseteq A \cup E$.

According to the definition of the universal set, we have $A \cup E \subseteq E$

(4) $A \cap E = A$ (Law of Identity)

Proof: We need to prove $A \subseteq A \cap E$ and $A \cap E \subseteq A$

By the definition of intersection, **we have $A \cap E \subseteq A$.**

For $\forall x$ $x \in A$,

By the definition of the universal set E

$x \in E$, Therefore $x \in A$ *and* $x \in E$,

$\Rightarrow$ $x \in A \cap E$

Thus $A \subseteq A \cap E$.

e.g. Example 4: Prove that $A \cup (A \cap B) = A$ （Absorption Law）

Proof: Using the four identities proven in Example 3 to prove:

$$
\begin{aligned}
& A \cup (A \cap B) \\
&= (A \cap E) \cup (A \cap B) && \text{(Law of Identity)} \\
&= A \cap (E \cup B) && \text{(Distributive Law)} \\
&= A \cap (B \cup E) && \text{(Commutative Law)} \\
&= A \cap E && \text{(Law of Excluded Null)} \\
&= A && \text{(Law of Identity)}
\end{aligned}
$$

i For the remaining basic set identities, we will not prove each one individually (please prove them yourself). From now on, we will use them as known set identities.

e.g. **Example 5: Prove that $(A-B)-C=(A-C)-(B-C)$**

Proof:

$(A-C)-(B-C)$

$= (A\cap\sim C)\cap\sim(B\cap\sim C)$ (Complement Intersection Conversion)

$= (A\cap\sim C)\cap(\sim B\cup\sim\sim C)$ (De Morgan's Law))

$= (A\cap\sim C)\cap(\sim B\cup C)$ (Double Negation Law)

$= (A\cap\sim C\cap\sim B)\cup(A\cap\sim C\cap C)$ (Distributive Law)

$= (A\cap\sim C\cap\sim B)\cup(A\cap\varnothing)$ (Contradiction Law)

$= A\cap\sim C\cap\sim B$ (Zero Law, Identity Law)

$= (A\cap\sim B)\cap\sim C$ (Commutative Law, Associative Law)

$= (A-B)-C$ (Complement Intersection Conversion Law) e.g. **Example 6:** Prove $(A\cup B)\oplus(A\cup C)=(B\oplus C)-A$

Need to prove $(A\cup B)\oplus(A\cup C)$

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

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

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

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

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

$$=(B\oplus C)-A$$

e.g. Example 7:

Let A and B be any sets, with power sets P(A) and P(B).

Prove that: $If\ A \subseteq B,\ then\ P(A) \subseteq P(B)$

Proof : $\forall x\ \ x \in P(A) \Leftrightarrow x \subseteq A$

$\Rightarrow x \subseteq B$ (Since $A \subseteq B$)

$\Leftrightarrow x \in P(B)$

e.g. **Example8: Proof $A \oplus B = A \cup B - A \cap B$.**

Proof $A \oplus B = (A \cap \sim B) \cup (\sim A \cap B)$

$= (A \cup \sim A) \cap (A \cup B) \cap (\sim B \cup \sim A) \cap (\sim B \cup B)$

$= (A \cup B) \cap (\sim B \cup \sim A)$

$= (A \cup B) \cap \sim(A \cap B)$

$= A \cup B - A \cap B$

- Direct Proof Method
- Indirect Proof Method
- Reductio ad Absurdum (Proof by Contradiction)
- Exhaustive Method
- Constructive Proof Method
- Vacuous Proof Method
- Trivial Proof Method
- Mathematical Induction
- Counterexample—Proof that a Proposition is False

- **Form 1:** If A, then B
- **Form 2:** A if and only if B
- **Form 3:** Prove B
- All can be reduced to **Form 1**

- **Method:** Assume A is true, prove B is true.

e.g. **Example 1:** If n is odd, then n^2 is also odd.

Proof:

Assume n is odd, then there exists $k \in N$,

such that $n = 2k + 1$.

Therefore,

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

Thus, n^2 is odd.

- **Indirect proof method** is a generalized proof technique that encompasses any method of proof that does not directly derive the conclusion from the premise.
- **Logical fact：** A proposition and its contrapositive are logically equivalent.
- **Method:** To prove "$A \to B$", it is sufficient to prove "$\neg B \to \neg A$", that is, "If B is not true, then A is not true."

e.g. **Example 2:** If n^2 is odd, then n is also odd.

Proof: It suffices to prove that: If n is even, then n^2 is even. That is, prove the original proposition is true.

Assume n is even, then there exists $k \in N$, such that $n = 2k$. Therefore,

$n^2 = (2k)^2 = 2(2k^2)$

Thus, n^2 is even.

- **Proof by Contradiction** begins by assuming that the negation of the proposition to be proven is true, and then through logical reasoning, a contradiction or an impossible result is derived.
- **Method:** Let A be true, assume B is not true, and derive a contradiction.

e.g. **Example 3:** If $A-B=A$, then $A\cap B=\emptyset$.

Proof: Using proof by contradiction, assume $A\cap B\neq\emptyset$. Then there exists an element x such that

$x\in A\cap B \iff x\in A$ and $x\in B$.

Since $A-B=A$, it follows that $x\in A-B$ and $x\in B$

$\iff (x\in A$ and $x\notin B)$ and $x\in B$

$\implies x\notin B$ and $x\in B$,

which is a contradiction.

e.g. Example 4: Prove that $\sqrt{2}$ is irrational.

Proof: Assume $\sqrt{2}$ is rational. Then there exist positive integers m and n such that $\sqrt{2} = \frac{m}{n}$, where n≠0 and m and n have no common factors (i.e., $\frac{m}{n}$ is in lowest terms).

Then $m=n\sqrt{2}$, squaring both sides gives $m^2=2n^2$. This implies m^2 is even, and therefore m is even. Let $m=2k$. Substituting back, we get $(2k)^2 = 2n^2$, which simplifies to $4k^2=2n^2$ or $n^2=2k^2$. This implies n^2 is even, and hence n is also even. This contradicts the assumption that $\frac{m}{n}$ is in lowest terms.

ⓘ **Proof by Contradiction** is a special form of indirect proof: by showing that the negation of the conclusion leads to the negation of the premise, thereby contradicting the initial assumption.

- **Definition:** Exhaustive method (also known as the method of exhaustion) is a technique used to prove a proposition by verifying all possible cases. This method is typically applied when the number of possible situations is finite and can be explicitly listed.
- **Scope of application:** It is suitable for problems where the solution space is small and manageable.
- **Proof process:** The prover needs to examine each possible case one by one and demonstrate that the proposition holds true in all these situations.
- **Characteristics:** The key to the exhaustive method lies in its completeness, ensuring that all possible cases are considered. However, it is generally impractical when dealing with a large solution space.

- **Definition:** **Proof by cases** is a method where the original problem is decomposed into several smaller, more manageable sub-problems, each of which is proven individually. The sum of these sub-problems covers all situations of the original problem.
- **Usage Scenario:** It is applicable when the problem inherently possesses natural classifications or when the solution can be simplified through logical division.
- **Proof Process:** The prover decomposes the problem into several non-overlapping cases based on different characteristics or conditions and proves the correctness of the proposition for each case individually.
- **Characteristics:** The focus of proof by cases lies in the effective division of the problem and the independent handling of each sub-case. This method may employ different proof strategies in different situations.

- **Definition:** The proposition to be proven is of the form = $A_1 \vee A_2 \vee \ldots \vee A_k \rightarrow B$.
- **Method:** Prove that $A_1 \rightarrow B$, $A_2 \rightarrow B$,…, $A_k \rightarrow B$ are all true.

e.g. **Example 5:** Prove that max(a,max(b,c))=max(max(a,b),c).

Proof:

情况	u=max(b,c)	max(a,u)	v=max(a,b)	max(v,c)
$a \le b \le c$	c	c	b	c
$a \le c \le b$	b	b	b	b
$b \le a \le c$	c	c	a	c
$b \le c \le a$	c	a	a	a
$c \le a \le b$	b	b	b	b
$c \le b \le a$	b	a	a	a

- **Definition:** A proof by construction involves creating a specific example or object to prove the truth of a proposition. This method is typically used for "existence proofs."
- **Method:** Under the condition that A is true, construct an object with this property.

e.g. **Example 6:** For every positive integer n, there exist n consecutive positive composite numbers.

Proof: Let x=(n+1)!.

Then x+2,x+3,…,x+n+1 are n consecutive positive composite numbers:

For i=2,3,…,n+1, x+i is composite.

- **Constructive Proof:** A constructive proof provides one or more specific instances or examples to prove a proposition. It is applicable when demonstrating that there exist particular objects or numbers that satisfy certain conditions.
- **Non-Constructive Proof:** A non-constructive proof establishes the truth of a proposition without directly presenting specific examples. This method often relies on logical reasoning, existing theories, or theorems, or employs techniques such as proof by contradiction.
- When it is difficult to directly construct an instance that meets the required conditions, non-constructive proofs allow us to prove the existence of certain entities or the truth of certain propositions.

↳Vacuous Proof Method (Proof by Vacuity)

- A vacuous proof is commonly used to prove statements of the form "All objects satisfying a particular property P also satisfy another property Q" (P→Q). This method is particularly applicable when no objects satisfy the initial property P. In such cases, the statement is considered true because there are no counterexamples to invalidate it.
- A conditional statement P→Q is false only when P is true, and Q is false. Therefore, to prove P→Q is always true using the vacuous proof method, it suffices to show that P is always false.

e.g. **Example:**

Let n $\in$ N. Define P(n): If n > 1, then $n^2 > 1$. Prove that P(0) is true.

P(0): If 0 > 1, then $0^2 > 1$.

Since the premise 0 > 1 is always false, by the vacuous proof method, we can assert that P(0) is true.

同济经管 TONGJI SEM

- **Trivial Proof Method (**Proof by Showing the Consequent is True**)**
- The trivial proof method is used to prove propositions that are clearly true under specific conditions.
- **Method:**

  Prove that **B** is always true, without needing to assume **A** is true.

e.g. **Example:**

If a≤b, then $\mathbf{a^0 \le b^0}$.

Proof:

Based on a universally accepted mathematical fact, any number raised to the power of 0 equals 1. Therefore, regardless of the size relationship between a and b, both $\mathbf{a^0}$ and $\mathbf{a^0 \le b^0}$ equal 1. Hence, $\mathbf{a^0 \le b^0}$holds.

ⓘ This method often appears in the base case of induction proofs.

- **Induction** is a logical reasoning method that starts from specific cases or instances and generalizes to universal laws or principles. A **conjecture** is an unproven hypothesis or theory proposed based on existing knowledge and intuition.
- **Induction and conjecture** often interact in the research process. Induction may lead to the formation of new conjectures, while conjectures can potentially gain support through induction from experimental or observational data.

For example, observation

$1=1^2$

$1+3=2^2$

$1+3+5=3^2$

$1+3+5+7=4^2$

… …

Conjecture: The sum of the first n odd numbers equals n^2,

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

- Proposition **form**: $\forall x(x \in N \land x \geq n_0), P(x)$
- **Base case**: Prove $P(n_0)$ is true
- Inductive **step**: For all $x(x \geq n_0)$, assume $P(x)$ is true, prove $P(x+1)$ is true.
  The statement "P(x) is true" is called the **induction hypothesis**.

e.g. »» **Example 8:** Proof: For all $n \geq 1$, $1+3+5+\ldots+(2n-1)=n^2$

Proof:

Base case: When $n=1$, $1=1^2$, the conclusion holds.

Inductive step: Assume the conclusion holds for $n \geq 1$, then

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

Thus, the conclusion also holds when n+1.

TONGJI SEM

- Note: Both the base case and the inductive step are essential.

e.g. Example(1) Proposition: For all n≥1, $\mathbf{2^1+2^2+ \ldots + 2^n= 2^{n+1} - 2}$

Proof:

Base case: When n=1, $\mathbf{2^1 = 2^{1+1} - 2=2}$.

Inductive hypothesis: Assume the statement holds for some arbitrary n≥1. Then,

$\mathbf{2^1+2^2+ \ldots + 2^n+2^{n+1}= 2^{n+1}+2^{n+1} -2= 2^{n+2} - 2}$.

Thus, the proposition holds for n+1.

- The method of **counterexamples** involves finding one or more examples to refute a universal statement. This method is typically used to prove that a proposition is incorrect.

e.g. **Example(2):** Observe whether $2^{n-1}-1$ is divisible by n.

n	$2^{n-1}-1$	divisible	N	$2^{n-1}-1$	divisible
3	3	Y	10	511	N
4	7	N	11	1023	Y
5	15	Y	12	2047	N
6	31	N	13	4095	Y
7	63	Y	14	8191	N
8	127	N	15	16383	N
9	255	N	16	32767	N

n	$2^{n-1}-1$	整除	n	$2^{n-1}-1$	整除
17	65535	Y	21	1048575	N
18	131071	N	22	2097151	N
19	262143	Y	23	4194303	Y
20	524287	N	24	8388607	N

- From the table, we might induce the following proposition:

Let n≥3. A necessary and sufficient condition for n to be a prime number is that $2^{n-1}-1$ is divisible by n. However, this proposition is not true.

Counterexample: 561=3×11×17 is a composite number, yet 2560−1 is divisible by 561.

- **Complete Induction** (also known as **Strong Induction**) is a proof technique used to establish the truth of a statement for all integers greater than or equal to a certain number. It is an extension of the principle of mathematical induction, where, instead of assuming the truth of the statement only for the immediate predecessor (i.e., P(k)), it assumes the truth of the statement for all values from the base case up to k.
- **Base Case:** Prove that $P(n_0)$ is true.
- **Inductive Step:** For all x (where $x \geq n_0$), **assume** $P(n_0), P(n_0+1), \ldots, P(x)$ are true, and prove that P(x+1) is true.
- **Inductive Hypothesis:** For all y (where $n_0 \leq y \leq x$), P(y) is true.

e.g. **Example 9:** Every integer greater than or equal to 2 can be expressed as a product of prime numbers.

Proof:

Base Case: For n=2, the statement is obviously true.

Inductive Step: Assume that for all integers k such that $2 \le k \le n$, the statement holds true. We need to show that the statement also holds for n+1.

- If n+1 is a prime number, then the statement is true.
- If n+1 is not a prime number, then it can be expressed as $n+1=a \times b$, where $2 \le a,b<n$.
- By the inductive hypothesis, both a and b can be expressed as products of prime numbers. Therefore, n+1 can also be expressed as a product of prime numbers. **Thus**, the statement holds for n+1.

The base case of strong induction does not merely assume that the proposition holds for a specific natural number n; instead, it assumes that the proposition holds for all natural numbers less than or equal to n. Based on this stronger assumption, we then prove that the proposition holds for n + 1.

e.g. »» **Example 10:** Any postal fee of n cents (where n≥12) can be composed using 4-cent and 5-cent stamps.

Proof:

Base Case: For n=12,13,14,15, the following combinations are possible:

$12=3\times 4$,
$13=2\times 4+5$,
$14=2\times 5+4$,
$15=3\times 5$.

Thus, the conclusion holds for n=12,13,14,15.

> ⓘ The base case of strong induction does not merely assume that the proposition holds for a specific natural number n; instead, it assumes that the proposition holds for all natural numbers less than or equal to n. Based on this stronger assumption, we then prove that the proposition holds for n + 1.

Inductive Step: Let n≥15, and assume that the conclusion holds for all integers from 12 to n.

- Consider n+1. Since n−3≥12 and by the inductive hypothesis, n−3 cents can be composed using 4-cent and 5-cent stamps.
- By adding one 4-cent stamp to the composition of n−3 cents, we obtain n+1 cents.

Therefore, the conclusion holds for n+1.

■ The **Proof by Counterexample** is a logical proof technique used to demonstrate that a general statement or conjecture is false by providing a specific example that contradicts the statement

e.g. »»**Example 11:** Prove that the following statement does not hold:

If $A \cap B = A \cap C$, then $B = C$.

Proof:

- ***Counterexample:*** Let A={a,b}, B={a,b,c}, and C={a,b,d}.
- Then, $A \cap B=\{a,b\}$, $A \cap C=\{a,b\}$. Thus, $A \cap B=A \cap C$.
- However, $B \neq C$ because $c \notin C$ and $d \notin B$.
- **Therefore**, the statement does not hold

- **Recursive Definition** is a process where a concept is defined in terms of itself.
- **Example:** The sequence an can be recursively defined as follows:

$a^0=1$, $a^n= a^{n-1}\cdot \mathbf{a}$, for n=1,2,…

e.g. **Example 12:** The Fibonacci sequence $\{f_n\}$ is recursively defined as follows:

- $f_0=1$, $f_1=1$, $f_n=f_{n-1}+ f_{n-2}$, for n=2,3,…Calculating the first few terms:

  $f_0=1$, $f_1=1$, $f_2=2$, $f_3=3$, $f_4=5$, $f_5=8$, $f_6=13$

e.g. **Example 13:** The set A is recursively defined as follows:

- **Base Step:** $3 \in A$
- **Recursive Step(Rule):**

(1) If $x, y \in A$, then $x + y \in A$.

(2) All numbers obtained by applying the recursive step a finite number of times belong to the set A.

$$A=\{3n \mid n\in Z^{+}\}$$

In 2024, Meituan Delivery was the most popular online food delivery app in China, boasting approximately 83 million mo

e.g. **Example 14:** **Arithmetic expressions** are defined inductively as follows:

(1) Any real **number and variable** is an arithmetic expression.

(2) If f and g are arithmetic expressions, then $(f + g)$, $(f - g)$, and $(f \times g)$ are also arithmetic expressions.

(3) If f and g are arithmetic expressions and $g \neq 0$, then (f/g) is an arithmetic expression.

(4) If f is an arithmetic expression, then for all $n \in \mathbf{Z}^+$, f^n (or $f \uparrow n$) is an arithmetic expression.

(5) Only those expressions obtained by a finite number of applications of rules (1) through (4) are considered arithmetic expressions.

Objective :

Key Concepts ：