CH 3 - Proving Mathematical Statements

Luke Lu • 2025-12-17

Definitions

1. **Proposition** — a statement to be proved true
2. **Theorem** — a significant proposition
3. **Lemma** — a subsidiary proposition
4. **Corollary** — a proposition that follows almost immediately from a theorem

Proving Universally Quantified Statements

1. Choose a representative object $x \in S$ (let x be arbitrary in S)
2. Show the open sentence is true for this x using facts about S

Example

Prove $\forall x, y \in \mathbb{R}, x^4 + x^2 y + y^2 \geq 5x^2 y - 3y^2$

Discovery

If $x^4 + x^2 y + y^2 \geq 5x^2 y - 3y^2 \Rightarrow x^4 - 4x^2 y + 4y^2 \geq 0 \Rightarrow \left(x^2 - 2y\right)^2 \geq 0$

This is a discovery, not a proof

Proof

Let $x, y \in \mathbb{R}$ be arbitrary

Then $\left(x^2 - 2y\right)^2 \geq 0$

So $x^4 - 4x^2 y + 4y^2 \geq 0$

Hence $x^4 + x^2 y + y^2 - 5x^2 y + 3y^2 \geq 0$

$\forall x, y \in \mathbb{R}, x^4 + x^2 y + y^2 \geq 5x^2 y - 3y^2$

Disprove Universally Quantified Statement

To disprove $\forall x \in S, P(x)$, find $x \in S$ with $\neg P(x)$

Example

Disprove $\forall x \in \mathbb{Z}, x^2 = 5$

Proof

Let $x = 0$

Then $x^2 = 0 \neq 5$

$\exists x \in \mathbb{R}$ with $x^2 \neq 5$, so $\forall x \in \mathbb{Z}, x^2 = 5$ is false

Prove Existentially Quantified Statement

Find a specific $x \in S$ that makes the sentence true

Example 1

Prove $\exists m \in \mathbb{Z}$ s.t. $\frac{m-7}{2m+4} = 5$

Proof

$m - 7 = 5(2m + 4) \Rightarrow m - 7 = 10m + 10 \Rightarrow -27 = 9m \Rightarrow m = -3$

Let $m = -3$ and note $2m + 4 = -2 \neq 0$

Then $\frac{m-7}{2m+4} = \frac{-3-7}{2(-3)+4} = \frac{-10}{-6+4} = \frac{-10}{-2} = 5$

$\exists m \in \mathbb{Z}$ with $\frac{m-7}{2m+4} = 5$

Example 2

Prove there exists a perfect square k s.t. $k^2 - \frac{31}{2}k = 8$

Proof

Let $k = 16 = 4^2$

Then $k^2 - \frac{31}{2}k = 256 - 248 = 8$

There exists a perfect square k with $k^2 - \frac{31}{2}k = 8$

Disprove Existentially Quantified Statement

To disprove $\exists x \in S, P(x)$, prove $\forall x \in S, \neg P(x)$

Example

Disprove $\exists x \in \mathbb{R}$ s.t. $\cos(2x) + \sin(2x) = 3$

Proof

For all $x \in \mathbb{R}$, we have $-1 \leq \cos(2x) \leq 1$ and $-1 \leq \sin(2x) \leq 1$

So $-2 \leq \cos(2x) + \sin(2x) \leq 2$

Thus $\cos(2x) + \sin(2x) \neq 3$ since $3 \notin [-2, 2]$

$\forall x \in \mathbb{R}, \cos(2x) + \sin(2x) \neq 3$ i.e. $\neg, (\exists x \in \mathbb{R}, \cos(2x) + \sin(2x) = 3)$

Prove/Disprove Nested Quantified Statement

Consider examples

1. $\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, x^3 - y^3 = 1$
2. $\exists x \in \mathbb{R}, \forall y \in \mathbb{R}, x^3 - y^3 = 1$

1. True

   Let $x \in \mathbb{R}$ and set $y = \sqrt[3]{x^3 - 1}$

   Then $x^3 - y^3 = x^3 - \left(\sqrt[3]{x^3 - 1}\right)^3 = x^3 - (x^3 - 1) = 1$

   $\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, x^3 - y^3 = 1$

2. False

   The negation is $\forall x \in \mathbb{R}, \exists y \in \mathbb{R}$ with $x^3 - y^3 \neq 1$

   Let $x \in \mathbb{R}$ and choose $y = x$

   Then $x^3 - y^3 = x^3 - x^3 = 0 \neq 1$

   $\neg(\exists x \in \mathbb{R}, \forall y \in \mathbb{R}, x^3 - y^3 = 1)$

Prove/Disprove Implication

IMPORTANT

1. To prove the implication $A \Rightarrow B$, assume that the hypothesis A is true, and use this assumption to show that the conclusion B is true. The hypothesis A is what you start with. The conclusion B is where you must end up.
2. To prove the universally quantified implication $\forall x \in S, P(x) \Rightarrow Q(x)$:

Let x be an arbitrary element of S, assume that the hypothesis $P(x)$ is true, and use this assumption to show that the conclusion Q(x) is true.

Example:
Prove that $\forall$ integers K, if K^5 is a perfect square, then $9K^{19}$ is a perfect square.

Proof

Let $K \in \mathbb{Z}$.
Assume that K^5 is a perfect square.
Then $\exists l \in \mathbb{Z}$ such that $K^5 = l^2$.
Now, $9K^{19} = 9(K^5)^3 K^4 = 9(l^2)^3 K^4 = 3^2 (l^3)^2 (K^2)^2 = (3l^3 K^2)^2$

Since 3, l, and K are integers, we have $3l^3K^2 \in \mathbb{Z}$ so $(3l^3K^2)^2$ is a perfect square, that is, $9K^{19}$ is a perfect square.

$\therefore K \in \mathbb{Z}$, if K^5 is a perfect square, then $(9K^{19})$ is a perfect square.

Divisibility of Integers

IMPORTANT

An integer m **divides** an integer n, and we write $m \mid n$, if there exists an integer k so that $n = k \cdot m$

If $m \mid n$ then we say that m is a **divisor** of n, n is the multiple of m

Examples
$7 \mid 56$ since $56 = 7 \cdot 8$
$7 \mid -56$ since $-56 = 7 \cdot . - 8$
$56 \nmid 7$ we need to write $7 = 56k, k \in \mathbb{R}$
$a \mid 0$ where $a \in \mathbb{Z}$ since $0 = a \cdot 0, \forall z \in \mathbb{Z}$ $0 \nmid a \forall a \in \mathbb{Z}$ except $a = 0$, we can write $0 = 0 \cdot 0$

Prove $\forall m \in \mathbb{Z}$, if $14 \mid m$, then $7 \mid m$
Assume $14 \mid n$, Then (by definition), $\exists k \in \mathbb{Z}, n = 14k$
Then $m = 7 \cdot 2 \cdot k = 7 \cdot 2k$
Since $k \in \mathbb{Z}$, so is $2k \in \mathbb{Z}$
$\therefore 7 \mid m$

1. Transivity of Divisibility (TD)

IMPORTANT

Proposition: $\forall a, b, c, \in \mathbb{Z}$**, if** $a \mid b$ **and** $b \mid c$**, then** $a \mid c$

Some similar proposition
$\forall a, b, c \in \mathbb{Z}$, if $a \mid b$ or $a \mid c$, then $a \mid bc$

Proof

Let $a, b, c, \in \mathbb{Z}$
Suppose $a \mid b, b \mid c$
Then,
$\exists n \in \mathbb{Z}, b = a \cdot n$
$\exists n \in \mathbb{Z}, b = c \cdot m$
Now, $c = b \cdot m = a \cdot n \cdot m = a(nm)$ Since $n, m \in \mathbb{Z}$ then $n \cdot m \in \mathbb{Z}$, and so $a \mid c$

2. Divisibility of Integer Combination (DIC)

IMPORTANT

Proposition: $\forall a, b, c \in \mathbb{Z}$**, if** $a \mid b$ **and** $a \mid c$**, then for all integers** x **and** y**,** $a \mid (bx + cy)$

Proof

Let $a, b, c \in \mathbb{Z}$
Assume $a \mid b$ and $a \mid c$.
Then $\exists k, l \in \mathbb{Z}, b = ka$ and $c = la$ Let $x, y \in \mathbb{Z}$
Then $bx + cy = kax + lay = a(kx + ly)$ Since $k, x, l, y \in \mathbb{Z}$, we have $kx + ly \in \mathbb{Z}$. By definition, it means $a \mid (bx + cy)$
Q.E.D.

Prove of Contrapositive

Example: $\forall x \in \mathbb{Z}$ if $x^2 + 4x - 2$ is odd, then x is odd

Proof

Let $x \in \mathbb{Z}$, we prove the implication by proving the contrapositive.
Assume x is even.
Then $k \in \mathbb{Z}, x = 2k$
$x^2 + 4x - 2 = (2k)^2 + 4(2k) + 2 = 2(2k^2 + 4k - 1)$
Since $k \in \mathbb{Z}$, $2(2k^2 + 4k - 1) \in \mathbb{Z}$, so the contrapositive is true.
Therefore the original statement is also true

$\square$

IMPORTANT

$A \Rightarrow (B \vee C) \equiv ((A \wedge \neg(B)) \Rightarrow C)$

Example:

$\forall x \in \mathbb{R}$, if $x^2 - 7x + 12 \geq 0$, then $x \leq 3$ or $x > 4$

Proof

Proof 1:
Let $x \in \mathbb{R}$.
Assume $x^2 - 7x + 12 \geq 0 \wedge x > 3$.
Notice $x^2 - 7x + 12(x-3)(x-4)$, so the inequality can be rewritten as $(x-3)(x-4) \geq 0$.
Since $x \geq 3$, then $x - 3 > 0$, so $(x-3)(x-4) \geq 0$, we must have $x - 4 \geq 0$. Thus $x \geq 4$. We have shown $\forall x n \mathbb{R}$, if $x^2 - 7x + 12 \geq 0$ and $x > 3$ then $x \geq 4$, which is logically equivalent to the original statement.

$\square$

Proof

Proof 2:
The contrapostive is $\forall x \in \mathbb{R}, ((x > 3) \wedge (x < 4)) \Rightarrow x^2 - 7x + 12 < 0$ The inequality becomes $(x-3)(x-4) < 0$. The solution set is $(3, 4)$. The contrapositive is true, thus the original statement is true.

$\square$

Proof by Contradiction

Let A be a statement, Note that either A or $\neg A$ must be false, so the compound statement $A \wedge (\neg A)$ is always false. The statement $A \wedge (\neg A)$ is true is called a contradiction.

Example:
Proof that there is no largest integer

Proof

In order to obtain a contradiction, let us assume that there is a largest integer. Call this integer N. Then, $\forall n \in \mathbb{Z}, N \geq n$. *
Now let $n = N + 1$, since $N, i \in \mathbb{Z}$, we have $N + 1 \in \mathbb{Z}$, so by *, $N \geq N + 1$, this implies $0 \geq 1$. This is an contradiction. So the assumption that there is a largest integer must be false.
$\therefore$ There is no largest integer.

$\square$

Proof that $\sqrt{2}$ is irrational:

Proof

Assume, for the sake of contradiction, that $\sqrt{2}$ is rational, we have $\sqrt{2} \in \mathbb{Q}$ and $\sqrt{2} = \frac{a}{b}$ where $a, b \in \mathbb{Z}$ and $b \neq 0$. We also can assume $\sqrt{2}$ is positive. It also safe to say that a and b cannot be both even. [Proof of a is always even and b is always even is omitted] Contradiction. Thus $\sqrt{2}$ must be irrational

Proving Uniqueness

There is a unique element $x \in S$ s.t. $P(x)$ is true.

Prove that there is at least one element $x \in S$ s.t. $P(x)$ is true.

1. Assume that $P(x)$ and $P(y)$ are true for $x, y \in S$ and prove that this assumption leads to the conclusion $x = y$
2. Assume that are true for distinct $x, y \in S$ and prove this assumption leads to a contradiciton

Example:

$\forall a, b \in \mathbb{Z}$, if $a \neq 0$ and $a \mid b$, then there is a unique integer k s.t. $b = ka$

Proof

Let $a, b \in \mathbb{Z}$, and assume $a \neq 0$ and $a \mid b$.
By defintion, $\exists y \in \mathbb{Z}, b = ka$. Now, to prove uniqueness, assume $\exists, k, l \in \mathbb{Z}, b = ka$ and $b = la$
Then $a(k - l) = 0$, given $a \neq 0$, then $k - l = 0 \Rightarrow k = l$. $\therefore$ k is unique.

$\square$

Prove If and Only If Statements

To prove the an if and only if statment, we have this logical equivalence. Proving two implication will result the proof of the if and only if statement.

$$(A \Longleftrightarrow B) \equiv ((A \Longrightarrow B) \land (B \Longrightarrow A))$$

Example:
Prove $\forall x, \in \mathbb{R}$, with $x, y \geq 0, x = y \Longleftrightarrow \frac{x+y}{2} = \sqrt{xy}$

Proof

Let x, y be arbitrary non-negative real numbers.

(i)($\Longrightarrow$) Assume $x = y$, then $\frac{x+y}{2} = \frac{2x}{2} = 2$, and $\sqrt{xy} = \sqrt{xx} = x$ as $x \geq 0$

Therefore $\frac{x+y}{2} = \sqrt{xy}$ we have shown the implication: if $x = y$ then $\frac{x+y}{2} = \sqrt{xy}$

(ii)($\Longleftarrow$) Assume $\frac{x+y}{2} = \sqrt{xy}$
then $\frac{(x+y)^2}{4} = xy$
This implies $\frac{x^2+2xy+y^2}{4} = xy$
then $x^2 + 2xy = y^2 = 4xy$
$x^2 - 2xy + y^2 = 0$, means $(x - y)^2 = 0$, so, $x - y = 0$, implies $x = y$ We have proved if $\frac{x+y}{2} = \sqrt{xy}$ then $x = y$.

Therefore we have shown that $\forall x, \in \mathbb{R}$, with $x, y \geq 0, x = y \Longleftrightarrow \frac{x+y}{2} = \sqrt{xy}$

$\square$

Consider a triangle
In $\triangle\, ABC$, prove that $b = c \cos A \Longleftrightarrow \angle C = 90°$.

Proof

(i) ($\Longrightarrow$) Assume $b = \cos A$ then $\angle C = 90°$.
$a^2 = b^2 + c^2 - 2ab \cos C$
$a^2 = b^2 + c^2 - 2ab \Rightarrow a^2 - b^2 - c^2 c^2 - b^2$
$c^2 = a^2 + b^2$, implies the triangle is must be a right triagle
(ii) ($\Longleftarrow$) Assume $\angle C = 90°$ then $b = c \cos A$ Then $a^2 + b^2 = c^2, a^2 + c^2 \cos^2 A = c^2$