Proofs

Introduction To Math Proofs

Qinghao Hu

September 12, 2025

Contents

1 What is a Proof

Example. Let's proof that $\sqrt{2}$ is irrational

To start, we need to know what is the definition of irrational number

Definition: An irrational real number cannot be expressed in the form $\frac{m}{n}$, where n and m are integers

Proof. Assume, $\sqrt{2}$ is rational

$$\sqrt{2} = \frac{m}{n} \quad \text{(m and n are integers and } \frac{m}{n} \text{ is a reduced fraction)} \tag{1}$$

We can square both side using the principle of Algebra

$$2 = \frac{m^2}{n^2} \tag{2}$$

$$2n^2 = m^2 \tag{3}$$

$$\because \quad \text{Definition: A real number } N \text{ is even if it can be written as } N = 2k\text{, where } k \text{ is an integer} \tag{4}$$

$$\therefore m^2 \quad \textit{is even} \tag{5}$$

$$\therefore m \quad \textit{is even} \tag{6}$$

According to the definition, assume $m = 2k$, where $k \in \mathbb{I}$

Sub $m = 2k$ into equation (3)

$$2n^2 = (2k)^2 \tag{7}$$

$$n^2 = 2k^2 \tag{8}$$

$$n \text{ is even} \tag{9}$$

$$\because \text{According to (9) and (6), } n \text{ and } m \text{ are both even} \tag{10}$$

$$\therefore m \text{ and } n \text{ have a common factor of 2} \tag{11}$$

$$\therefore \frac{m}{n} \text{ is not an reduced fraction} \tag{12}$$

$$\text{This violate our original assumpution in (1)} \tag{13}$$

Therefore, $\sqrt{2}$ is not rational, $\sqrt{2}$ must be irrational □

2 Logical Rules

2.1 Modus Ponens

Definition: If p is ture and p implies q, then q is ture

Logical notation: $p, p \to q \therefore q$

Example: p = "It is raining", q = "The ground is wet"

Given: "it is raining" and "It is raining implies the ground is wet"

Conclusion: "The ground is wet"

2.2 Modus Tollens

Definition: If not q is ture and p implies q, then not p is true
Logical notation: $-q, p \rightarrow q \therefore -q$
Example: $p =$ "It is raining", $q =$ "The ground is wet"
Given: "it is raining" and "It is raining implies the ground is wet"
Conclusion: "It is not raining"

2.3 Hypothetical Syllogism

Definition: If p implies q and q implies r, then p implies r.
Logical notation: $(p \rightarrow q), (q \rightarrow r) \therefore (p \rightarrow r)$
Example: $p =$ "It is raining", $q =$ "The ground is wet", $r =$ "People use umbrellas"
Given: "It is raining implies the ground is wet" and "The ground is wet implies people use umbrellas"
Conclusion: "It is not raining implies people use umbrellas"

2.4 Disjunctive Syllogism

Definition: If not p is true and p or q is true, then q is true.
Logical notation: $-p, (p \vee q) \therefore q$
Example: $p =$ "It is raining", $q =$ "I will stay indoors"
Given: "It is not raining" and "It is raining or I will stay indoors"
Conclusion: "I will stay indoors"

2.5 Additon

Definition: If p is true, then p or q is true
Logical notation: $p \therefore (p \wedge q)$
Example: $p =$ "It is raining", $q =$ "I will go for a run"
Given: "It is raining"
Conclusion: "It is raining or I will go for a run"

2.6 Simplification

Definition: If p and q are true, then p is true
Logical notation: $(p \wedge q) \therefore p$
Example: $p =$ "It is raining", $q =$ "The ground is wet"
Given: "It is raining and The ground is wet"
Conclusion: "It is raining"

2.7 Conjunction

Definition: If p is true and q is true, then p and q are true.
Logical notation: $p, q \therefore (p \wedge q)$
Example: $p =$ "It is raining", $q =$ "The ground is wet"
Given: "It is raining", "The ground is wet"
Conclusion: "It is raining and The ground is wet"

3 Mathematical Sets

(Collection of Objects)

$\{\}$

$\{$All Triangles$\}$

$\{3, 6, 11, 117\}$, $\{$Real Numbers$\}$

$\{$What's in the set — The condition to be in the set$\}$

Example: $\{x$ — x is even and $x > 0\}$

3.1 Important Sets

$\mathbb{N}$ - The Natural Numbers(Counting Numbers): $\{1, 2, 3, \cdots\}$

$\mathbb{W}$ - The Whole Numbers: $\{0, 1, 2, 3, \cdots\}$

$\mathbb{Z}$ - The Integers: $\{\cdots, -3, -2, -1, 0, 1, 2, 3, \cdots\}$

$\mathbb{Q}$ - The Rational Numbers: $\{\frac{p}{q}|p, q \in \mathbb{Z}, q \neq 0\}$

$\mathbb{I}$ - The Irrational Numbers: $\{x|x \notin \mathbb{Q}, x \in \mathbb{R}\}$

$\mathbb{R}$ - The Real Numbers: $\{x\} = \{x|x \in \mathbb{Q}$ or $x \in \mathbb{I}\}$

$\mathbb{C}$ - The Complex (Imaginary) Numbers: $\{a + bi|a, b \in \mathbb{R}, i = \sqrt{-1}\}$

$\emptyset$ - Empty Set: $\{\}$

Sets do not care about orders, or duplicates.

3.2 Relationship of sets

Set A and B are equal ($A = B$).

$A \subseteq B$, $B \subseteq A$.

A is a subset of B if every element of A is also an element of B:

$(a \in A \to a \in B)$.

The Power Set of A, $P(A)$, is the set of all possible subsets of A.

The Complement, A^C or A', of a set A is the set of all elements in the universal set that are NOT elements of A.

The Union of two sets, $A \cup B$, is the set containing all the elements from either A or B.

Theorem: if $A \subseteq B, B \subseteq C$, then $A \subseteq C$

4 Quantifiers

4.1 Universal Quantify

"For all"

$\forall$

Example: $\forall y \in \mathbb{R}, y^2 \geqslant 0$

4.2 Essential Quantify

"There Exists"

$\exists$

Example: $\exists x$ such that $x + 3 = 5$

4.3 Negations

$$\neg$$

This is a dog

This is not a dog

Examples:

$$\neg(A \text{ or } B) = \neg A \text{ and } \neg B$$
$$\neg(A \text{ and } B) = \neg A \text{ or } \neg B$$
$$\neg(A \Rightarrow B) = A \text{ and } \neg B$$
$$\neg(\forall x,\ y) = \exists x \text{ such that } \neg y$$

5 Direct Proofs

$$\begin{gathered} \text{Assumption} \\ \Rightarrow \text{something} \\ \Rightarrow \cdots \\ \Rightarrow \text{conclusion} \end{gathered}$$

Example. Prove: The sum of two Even integers equals an even integer

Proof.

$$\text{Let } x, y \in \mathbb{Z} \quad \text{Assume } x \text{ and } y \text{ are both even.} \tag{14}$$
$$\Rightarrow x = 2a, y = 2b, (a, b \in \mathbb{Z}) \tag{15}$$
$$\Rightarrow x + y = 2a + 2b \tag{16}$$
$$\Rightarrow x + y = 2(a + b) \tag{17}$$
$$\text{Given that each Even number N can be present in this form } N = 2k \tag{18}$$
$$\Rightarrow \therefore \text{The sum of two Even integers equals an even integer} \tag{19}$$

□

6 Contrapositive proof

$$p \to q \equiv \neg q \to \neg p$$

Example. Theorem: if x is an irrational number, then $\frac{1}{x}$ is also an irrational number.
we want to show: $\neg(\frac{1}{x}$ is not irrational$) \Rightarrow \neg(x$ is irrational$)$

$$x \in \mathbb{R} \setminus \mathbb{Q} \Rightarrow x \neq \frac{p}{q}, (p, q \in \mathbb{Z}) \tag{20}$$
$$\text{Assume } \frac{1}{x} \text{ is Not Irrational} \tag{21}$$
$$\Rightarrow \frac{1}{x} \text{ is rational, } (\frac{1}{x} \in \mathbb{Q}) \tag{22}$$
$$\Rightarrow \frac{1}{x} = \frac{m}{n}, (m, n \in \mathbb{Z}) \tag{23}$$
$$\Rightarrow x = \frac{n}{m} \tag{24}$$
$$\Rightarrow \text{x is rational} \tag{25}$$

7 Two Way Proof

Also known as (Two way Proof)

Example. Theorem: A whole number is divisible by 9 iff the sum of its digits is divisible by 9.

Proof.

$$x \in \mathbb{W} = \{0, 1, 2, 3, \cdots\} \tag{26}$$
$$x \text{ has digits } , a_n, a_{n-1}, \cdots, a_2, a_1, a_0 \tag{27}$$
$$x = 10^n a_n + 10^{n-1} a_{n-1} + \cdots + 100 a_2 + 10 a_1 + a_0 \tag{28}$$
$$\text{Assume } x \text{ is divisible by 9.} \tag{29}$$
$$10^n a_n + 10^{n-1} a_{n-1} + \cdots + 100 a_2 + 10 a_1 + a_0 \text{(divisible by 9)} \tag{30}$$
$$-(999 \ldots 99 a_n + \cdots + 99 a_2 + 9 a_1)\text{(is divisible by 9)} \tag{31}$$
$$= a_n + a_{n-1} + \cdots + a_2 + a_1 + a_0 \text{ (is divisible by 9)} \tag{32}$$
$$\tag{33}$$
$$\text{Assume } a_n + a_{n-1} + a_{n-2} + \cdots + a_2 + a_1 + a_0 \text{ is divisible by 9} \tag{34}$$
$$x = a_n + a_{n-1} + a_{n-2} + \cdots + a_2 + a_1 + a_0 \tag{35}$$
$$+((999 \ldots 99) a_n + \cdots + 99 a_2 + 9 a_1) \text{ (is divisible by 9)} \tag{36}$$
$$\Rightarrow x \text{ is divisible by 9} \tag{37}$$

□

8 Proof by Contradiction

Assume the opposite of what we want to prove, then show a contradiction.

Example. Theorem: $\sqrt{3}$ is irrational.

Proof.

$$\text{Assume } \sqrt{3} \in \mathbb{Q} \tag{38}$$

$$\Rightarrow \sqrt{3} = \frac{m}{n} \text{ is a reduced fraction,} (n, m \in \mathbb{Z} \text{ and } n \neq 0) \tag{39}$$

$$\Rightarrow 3 = \frac{m^2}{n^2} \tag{40}$$

$$\Rightarrow 3 * n^2 = m^2 \tag{41}$$

$$\Rightarrow m^2 \text{ is a multiple of 3 and } m \text{ is a multiple of 3} \tag{42}$$

$$\Rightarrow m = 3k, (k \in \mathbb{Z}) \tag{43}$$

$$\Rightarrow 3n^2 = (3k)^2 \tag{44}$$

$$\Rightarrow 3n^2 = 9k^2 \tag{45}$$

$$\Rightarrow 3n^2 = 3k^2 \tag{46}$$

$$\Rightarrow n^2 \text{ is a multiple of 3 and } n \text{ is a multiple of 3} \tag{47}$$

$$\Rightarrow \frac{m}{n} \text{ is NOT in lowest terms} \tag{48}$$

□