

Proof Writing & Mathematical Notation

★ Basics of Mathematical Reasoning

⊙ **P** → a proposition / hypothesis, i.e. any statement that can be true or false.

T / 1 → universal truth / tautology.

F / 0 → universal falsehood / falsity / falsum

{ we will use plain symbols w/o boldfaces for the sake of convenience. }

⊙ Logical Operators

we will use these symbols.

$\wedge$	/	$\cdot$	/	$\&$	and
$\vee$	/	$+$	/	$\parallel$	or
$\neg$	/	$\sim$	/	$!$	not

$\Rightarrow$

implies

$\Leftarrow$

is implied by

$\Leftrightarrow$ / $\equiv$

equivalence

NOTE:

$\neg T \equiv F$

and, $\neg F \equiv T$

$\forall P, P \oplus \neg P \equiv T$

xor

{ Read more on Wikipedia: "List of Logic Symbols" }

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

$$B \Leftarrow A \equiv A \Rightarrow B$$

$$A \Leftrightarrow B \equiv (A \Rightarrow B) \wedge (B \Rightarrow A)$$

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

Quantifiers and Qualifiers

{ You need to know the basics of Set Theory }
 { to understand this:

$$\forall x \in A \quad P(x)$$

Proposition P holds for every x in the set A .

$$\exists x \in A \quad \text{such that } P(x)$$

There exists at least one x in A for which the proposition P holds.

$$\exists! x \in A \mid P(x)$$

There exists exactly one x in A for which the proposition P holds.

NOTE: " $\in A$ " may be ~~omitted~~ or rewritten in a way that doesn't change its meaning, or omitted entirely where the set in question is obvious.

$$\text{eg: } \exists \varepsilon > 0 \mid \dots$$

$$\Downarrow \exists \varepsilon \in \{x \mid x > 0, x \in \mathbb{R}\}$$

{ Again, read up further on Wikipedia if you }
 { want to, this is the bare minimum. }

⊛ Proofs

⊙ What is a proof?

- When asked to "prove" something, your essential task is to show, (say P)

$$\boxed{T \Rightarrow P}$$

i.e., start with something you know to be true, and use logical arguments to show that P must follow from that.

↳ a "direct" proof.

• However...

$$\boxed{T \Rightarrow P}$$

 $\Leftrightarrow$

$$\boxed{T \Leftrightarrow P}$$

proof by equivalence

$$\boxed{T \Rightarrow P}$$

 $\equiv$

$$\boxed{F \Leftarrow \neg P}$$

proof by contradiction

We can play with the statements to make things more convenient for ourselves.

⊙ Common Proving Techniques

• "Direct" Proofs

Start with something true and use logic to show that P must also be true. One of the most conventional approaches.

Looks something like: "Given: blah-blah

$\Rightarrow$ ---

$\Rightarrow$ ---

$\Rightarrow P$

• Proof by Equivalence

Construct a proposition Q | $P \Leftrightarrow Q$
(on atleast, $P \Leftarrow Q$).

Then prove Q .

This usually looks something like this:

• To show that: P

But we know, for P to hold, Q must hold.

P holds iff Q holds.

iff = if and only if.

(then proceed to prove Q , somehow)

• Proof by Contradiction

To show P , assume that P does not hold,
i.e. $\neg P$ holds,
then show that this leads to a contradiction.

Essentially prove $\neg P \Rightarrow F$

$$\equiv P \Leftarrow T$$

• Proof by Induction

This is a specialised technique used for proving a proposition for $\mathbb{N}$ (or $\{n \mid n \in \mathbb{N}, n \geq k\}$).

The idea is to...

- i) Prove the base case ($n=k$); ie. Prove P_k
- ii) Prove that $[P_e \Rightarrow P_{e+1} \quad \forall e \geq k], e \in \mathbb{N}$.

Then, $\vdash P_k \Rightarrow P_{k+1} \Rightarrow P_{k+2} \Rightarrow \dots$ (to infinity and beyond)

$\Rightarrow P_n$ (holds) $\forall n \in \mathbb{N}, n \geq k$.

$\hookrightarrow$ writing "holds" is extraneous, only for the sake of clarity.

- These techniques may be applied together, inside one another, etc., in order to prove a certain result.

① Disproving

There are generally 2 ways to disprove P .

- i) Find a counterexample.
- ii) Prove $\neg P$.

Often, the 2 methods essentially mean the same thing.

② Equivalences

- Equivalences are one of the ~~strongest~~ tools in your arsenal. Think of them as bidirectional highways, getting to even one side of it automatically gives you the other.

- However, this also makes them more difficult to prove.

- Typically, equivalences are written like this:

" P iff (if and only if) Q ."

This actually contains 2 statements.

" P if Q " , i.e. $P \Leftarrow Q$.

" P only if Q " , i.e. $P \Rightarrow Q$.

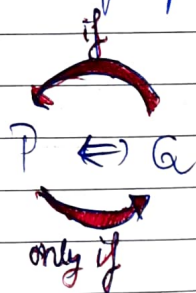
- So, while proving, you actually need to do 2 proofs:

i) ~~Ass~~ (If part or $\Leftarrow$)

Assume Q is true and prove P .

ii) (Only if part or $\Rightarrow$)

Assume P is true and prove Q .



- ~~At~~ Alternatively, use a chain of equivalences---

$$P \Leftrightarrow A \Leftrightarrow B \Leftrightarrow C \Leftrightarrow Q$$

...

① Necessary & Sufficient Conditions

If $P \Rightarrow Q$, Q is said to be necessary for P .

If $P \Leftarrow Q$, Q is said to be sufficient for P .

If $P \Leftrightarrow Q$, Q is said to be necessary and sufficient for P .

{ A lot of Mathematics at the higher level is about finding necessary & sufficient conditions, that can be easily tested for. }

② Converse:

The converse of $\boxed{P \Rightarrow Q}$ is $\boxed{P \Leftarrow Q}$.

Note: $P \Rightarrow Q \equiv \neg P \Leftarrow \neg Q$

But, $P \Rightarrow Q \neq P \Leftarrow Q$,
i.e. converses may not always hold.