

Implication

Theorems can usually be written in the form

if a collection of *assumptions* holds,
then so does some *conclusion*

or, in other words,

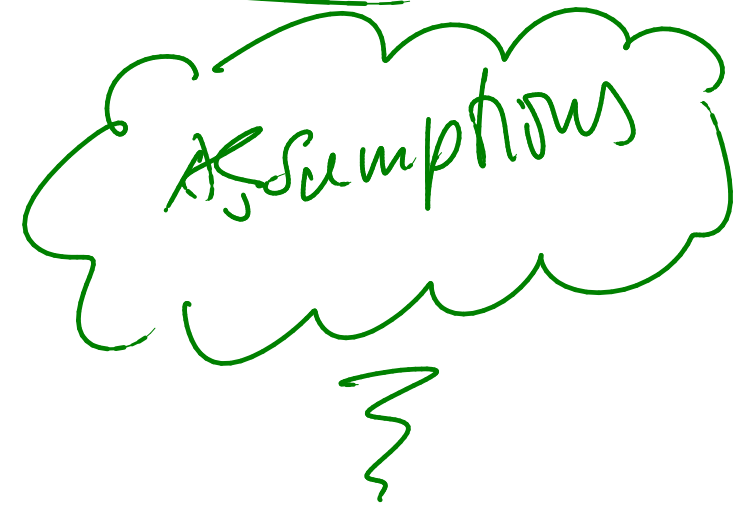
a collection of *assumptions* **implies** some *conclusion*

or, in symbols,

a collection of *hypotheses* \implies some *conclusion*

NB Identifying precisely what the assumptions and conclusions are is the first goal in dealing with a theorem.

PROOFS



The main proof strategy for implication:

To prove a goal of the form

$$P \implies Q$$

assume that P is true and prove Q .

God.

NB *Assuming* is not *asserting*! Assuming a statement amounts to the same thing as adding it to your list of hypotheses.

Proof pattern:

In order to prove that

$$P \implies Q$$

1. **Write:** Assume P .
2. Show that Q logically follows.

Scratch work:

Before using the strategy

Assumptions

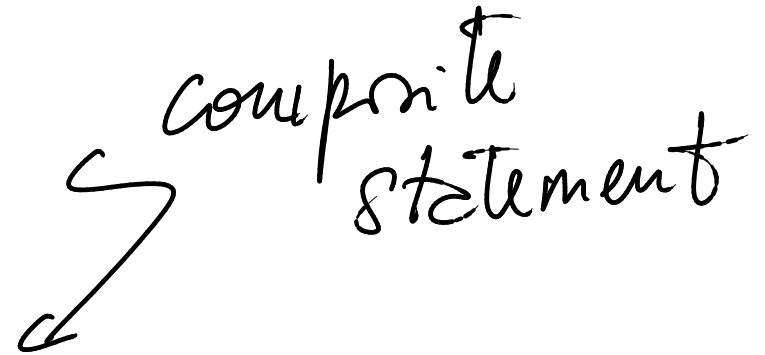
$$A \Rightarrow B$$

↳ [?] How: do we use it?

Goal

$$P \Rightarrow Q$$

composite statement



After using the strategy

Assumptions

⋮

P

Goal

Q

An alternative proof strategy for implication:

To prove an implication, prove instead the equivalent statement given by its **contrapositive**.

Definition:

the contrapositive of 'P implies Q' is 'not Q implies not P'

Proof pattern:

In order to prove that

$$P \implies Q$$

1. **Write:** We prove the contrapositive; that is, ... **and state the contrapositive.**
2. **Write:** Assume ‘the negation of Q ’.
3. Show that ‘the negation of P ’ logically follows.

Scratch work:

Before using the strategy

Assumptions

⋮

Goal

$P \implies Q$

After using the strategy

Assumptions

⋮

not Q

Goal

not P

Definition 9 *A real number is:*

- ▶ rational if it is of the form m/n for a pair of integers m and n ; otherwise it is irrational.
- ▶ positive if it is greater than 0, and negative if it is smaller than 0.
- ▶ nonnegative if it is greater than or equal 0, and nonpositive if it is smaller than or equal 0.
- ▶ natural if it is a nonnegative integer.

$\mathbb{L} \quad 0, 1, 2, \dots$

Proposition 10 Let x be a positive real number. If x is irrational then so is \sqrt{x} .

PROOF: We show

$$x \text{ irrational} \Rightarrow \sqrt{x} \text{ irrational.}$$

Assume x is irrational; that is, it is not of the form m/n for integers m and n .

Need to show \sqrt{x} is irrational; that is, it is not of the form k/l for integers k and l .

We are stuck, so we start again.

Proposition 10 Let x be a positive real number. If x is irrational then so is \sqrt{x} .

PROOF: We prove the contrapositive; that is,
 \sqrt{x} rational $\Rightarrow x$ rational

So we assume \sqrt{x} is rational; that is, of the form m/n for integers m and n .

Need show x is rational; that is, of the form k/l for integers k and l .

$\sqrt{x} = m/n$ hence $x = (\sqrt{x})^2 = m^2/n^2$ and since m^2

and n^2 are integers x is a rational. \square

Logical Deduction — Modus Ponens —

How we use assumptions of implication type!

A main rule of *logical deduction* is that of *Modus Ponens*:

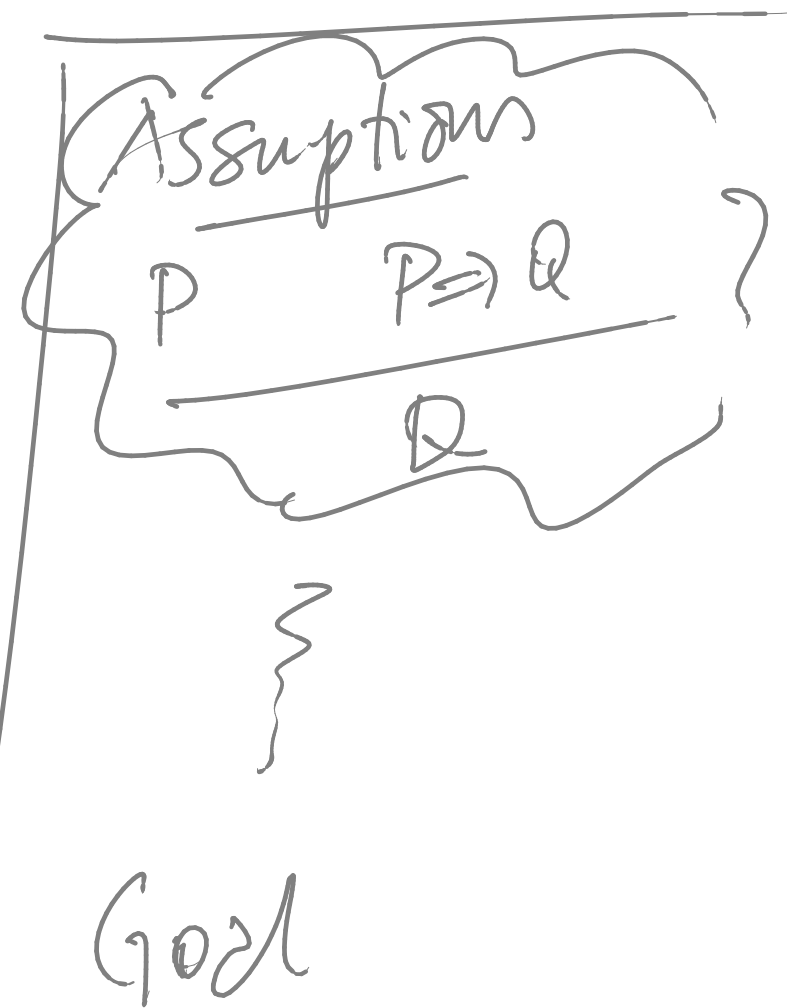
From the statements P and $P \implies Q$,
the statement Q follows.

or, in other words,

If P and $P \implies Q$ hold then so does Q .

or, in symbols,

$$\frac{P \quad P \implies Q}{Q}$$



The use of implications:

To use an assumption of the form $P \implies Q$,
aim at establishing P .

Once this is done, by Modus Ponens, one can
conclude Q and so further assume it.

Notation: $P_1 \Rightarrow P_2 \Rightarrow P_3$ then $P_1 \Rightarrow P_3$

Theorem 11 Let P_1 , P_2 , and P_3 be statements. If $P_1 \Rightarrow P_2$ and $P_2 \Rightarrow P_3$ then $P_1 \Rightarrow P_3$.

PROOF: Show $P_1 \Rightarrow P_2$ and $P_2 \Rightarrow P_3$ then $P_1 \Rightarrow P_3$

So assume

① $P_1 \Rightarrow P_2$

② $P_2 \Rightarrow P_3$

assumptions.

Goal

③

P_1

to show P_3

Show $P_1 \Rightarrow P_3$. For which assume P_1 to show P_3

From ① and ③ by MP we have

P_2 holds ④

From ② and ④ by MP we have P_3 ; that is, our goal \square

Bi-implication

Some theorems can be written in the form

P is equivalent to Q

or, in other words,

P implies Q, and vice versa

or

Q implies P, and vice versa

or

P if, and only if, Q

P iff Q

or, in symbols,

$P \iff Q$

Proof pattern:

In order to prove that

$$P \iff Q$$

1. Write: (\implies) and give a proof of $P \implies Q$.
2. Write: (\impliedby) and give a proof of $Q \implies P$.

Proposition 12 Suppose that n is an integer. Then, n is even iff n^2 is even.

PROOF: (\Rightarrow) Show n even $\Rightarrow n^2$ even.

Assume $\boxed{n \text{ even}}$; that is, $n = 2k$ for an integer k .

Show n^2 even; that is, $n^2 = 2l$ for an integer l .

From ①, $n = 2k$ so $n^2 = (2k)^2 = 2 \cdot \underbrace{(2k^2)}_{\text{integer}}$ and

thus even.

(\Leftarrow) Show n^2 even $\Rightarrow n$ even.

Assume $\boxed{n^2 \text{ even}}$; that is, $n^2 = 2p$ for an integer p

We are stuck ~ restart by showing the

contrapositive:

We show n odd $\Rightarrow n^2$ odd

Assume $n = 2k + 1$ for an integer k

Show $n^2 = (2k + 1)^2 = \dots = 2(\dots) + 1$. \square

WARNING

$Q \Rightarrow P$ and its contrapositive
is not $P \Rightarrow \text{not } Q$!

$$P \Leftrightarrow Q$$

(\Rightarrow) We show $P \Rightarrow Q$...

(\Leftarrow) We show by the contrapositive
 $\text{not } Q \Rightarrow \text{not } P$ } Wrong

predicate

Divisibility and congruence

predicate

Definition 13 Let d and n be integers. We say that d divides n , and write $d \mid n$, whenever there is an integer k such that $n = k \cdot d$.

Example 14 The statement $2 \mid 4$ is true, while $4 \mid 2$ is not.

Definition 15 Fix a positive integer m . For integers a and b , we say that a is congruent to b modulo m , and write $a \equiv b \pmod{m}$, whenever $m \mid (a - b)$.

Example 16

- $18 \equiv 2 \pmod{4}$
- $2 \equiv -2 \pmod{4}$
- $18 \equiv -2 \pmod{4}$

$0 \mid 0$ is true
$n \mid 0 \Leftrightarrow \dots n \dots ?$
$0 \mid m \Leftrightarrow \dots m \dots ?$

n is a multiple of d

$a \equiv b \pmod{m}$
 $b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m} ?$

$$n = 2k$$

Proposition 17 For every integer n ,

$$2 \mid n - 0 = n$$

$$\text{So } n = 2l$$

1. n is even if, and only if, $n \equiv 0 \pmod{2}$, and

2. n is odd if, and only if, $n \equiv 1 \pmod{2}$.

PROOF:

$$n = 2k + 1$$

$$2 \mid n - 1 \text{ so } n - 1 = 2l$$

$$\text{hence } n = 2l + 1$$

The use of bi-implications:

To use an assumption of the form $P \iff Q$, use it as two separate assumptions $P \implies Q$ and $Q \implies P$.