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* $\Longrightarrow$ some *conclusion*

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

PROOFS

Assumptions

The main proof strategy for implication:

To prove a goal of the form

$$P \implies Q$$

assume that P is true and prove Q.

Goal.

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: $\text{Assume } P$.
2. Show that Q logically follows.

Scratch work:

composite statement

Before using the strategy

Assumptions	Goal
$A \Rightarrow B$	$P \implies Q$
$\boxed{?}$ How: do we use it?	
$\vdots$	

After using the strategy

Assumptions	Goal
	Q
$\vdots$	
P	

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

$$\mathrm{P} \implies \mathrm{Q}$$

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
	$P \implies Q$
$\vdots$	

After using the strategy

Assumptions	Goal
	not P
$\vdots$	
not Q	

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.*

$0, 1, 2, \ldots$

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 $\boxed{x \text{ is irrational}}$; 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 $\mathrm{P} \implies \mathrm{Q}$, the statement Q follows.

or, in other words,

> If P and $\mathrm{P} \implies \mathrm{Q}$ hold then so does Q.

or, in symbols,

$$\frac{\mathrm{P} \qquad \mathrm{P} \implies \mathrm{Q}}{\mathrm{Q}}$$

Assumptions

$$\frac{P \qquad P \Rightarrow Q}{Q}$$

Goal

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* $P_1 \implies P_2$ *and* $P_2 \implies P_3$ *then* $P_1 \implies P_3$.

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

So assume

assumptions.

Goal

① $P_1 \Rightarrow P_2$

② $P_2 \Rightarrow P_3$

Show $P_1 \Rightarrow P_3$. For which assume ③ $\boxed{P_1}$ to show P_3

From ① and ③ by MP we have $\boxed{P_2 \text{ holds}}$ ④

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

Bi-implication

Some theorems can be written in the form

$$\boxed{\mathrm{P} \text{ is equivalent to } \mathrm{Q}}$$

or, in other words,

$$\boxed{\mathrm{P} \text{ implies } \mathrm{Q}\text{, and vice versa}}$$

or

$$\boxed{\mathrm{Q} \text{ implies } \mathrm{P}\text{, and vice versa}}$$

or

$$\boxed{\mathrm{P} \text{ if, and only if, } \mathrm{Q}} \qquad \boxed{\mathrm{P} \text{ iff } \mathrm{Q}}$$

or, in symbols,

$$\boxed{\mathrm{P} \iff \mathrm{Q}}$$

Proof pattern:

In order to prove that

$$P \iff Q$$

1. Write: $(\Longrightarrow)$ and give a proof of $P \implies Q$.
2. Write: $(\Longleftarrow)$ 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 $\boxed{n \text{ even}}$ (1); that is, $n = 2k$ for an integer k.

Show n^2 even; that is, $n^2 = 2\ell$ 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 $n^2 = (2k+1)^2 = \cdots = 2(\,..\,)+1$. $\square$

WARNING

$Q \Rightarrow P$ and its contrapositive is not $P \Rightarrow$ not Q!

$$P \Leftrightarrow Q$$

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

($\Leftarrow$) We show by the contrapositive not $Q \Rightarrow$ 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 $m \mid (a - b)$.*

$0 \mid 0$ is true

$n \mid 0 \iff \ldots n \ldots ?$

$0 \mid m \iff \ldots m \ldots ?$

n is a multiple of d

Example 16

1. $18 \equiv 2 \pmod{4}$
2. $2 \equiv -2 \pmod{4}$
3. $18 \equiv -2 \pmod{4}$

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

$n = 2k$

$2 \mid n - 0 = n$

So $n = 2\ell$

Proposition 17 *For every integer* n,

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:

$n = 2k+1$

$2 \mid n-1$ so $n - 1 = 2\ell$

hence $n = 2\ell + 1$

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 $Q \implies P$.