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.

Scratch work:

Before using the strategy

Assumptions	Goal
	$P \implies Q$
$\vdots$	

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

$$P \implies Q$$

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
	$P \implies Q$
$\vdots$	

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.*

$$\{0, 1, 2, \ldots, n, \ldots\} = \mathbb{N}$$

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

PROOF: Assume x is a positive real number.

x irrational $\Longrightarrow$ $\sqrt{x}$ irrational

Assume x is irrational. ~ That is, x is not of the form p/q for p and q integers

RTP: $\sqrt{x}$ is irrational

{ That is, $\sqrt{x}$ is not of the form m/n for m and n integers.

We are stuck and need to restart.

PROOF: We prove the statement by contrapositive.

That is, $\sqrt{x}$ not irrational $\Rightarrow$ x not irrational

equivalently $\sqrt{x}$ is rational $\Rightarrow$ x rational

Assume $\sqrt{x}$ is rational, that is, of the form p/q for p and q integers.

RTP: x is of the form m/n for some integers m and n

$\sqrt{x} = p/q$ So $(\sqrt{x})^2 = p^2/q^2$ Hence $x = p^2/q^2$

and we are done. $\boxtimes$

Logical Deduction
— Modus Ponens —

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,

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

PROOF

Assumptions Goal

$P \Rightarrow Q$

P

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.

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: Assume P_1, P_2, P_3 are statements.

$$(P_1 \Rightarrow P_2 \text{ and } P_2 \Rightarrow P_3) \implies (P_1 \Rightarrow P_3)$$

Assume : (1) $\boxed{P_1 \Rightarrow P_2}$ and (2) $\boxed{P_2 \Rightarrow P_3.}$

RTP : $P_1 \Rightarrow P_3$

(3) Assume: $\boxed{P_1}$

RTP : P_3

By MP from (1) and (3), we have (4) $\boxed{P_2}$

By MP from (2) and (4), we have P_3

as required. ☒

Bi-implication

Some theorems can be written in the form

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

or, in other words,

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

or

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

or

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

or, in symbols,

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

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: Let n is an integer.

(n is of the form 2k for an integer k) $\Longleftrightarrow$ (n^2 is of the form 2 l for some integer l)

($\Rightarrow$) Assume n = 2k for k an integer

Show $n^2 = 2l$ for l an integer.

Then $n^2 = (2k)^2 = 2.(2k^2)$

and so of the form 2 . l (for l the integer $2k^2$)

and we are done.

($\Leftarrow$) ($n^2 = 2l$ for l integer) $\Longrightarrow$ ($n = 2k$ for k integer)

~~Assume $n^2 = 2l$ for l integer~~

~~Show $n = 2k$ for k integer~~

We prove the contrapositive:

($n = 2k+1$ for k integer) $\Longrightarrow$ ($n^2 = 2l+1$ for l integer)

Assume $n = 2k+1$ (k integer)

Then $n^2 = (2k+1)^2 = 2(2k^2+2k)+1$

and hence of the form $2l+1$ (for $l = 2k^2+2k$).

$\boxtimes$

Divisibility and congruence

Definition 13 *Let* d *and* n *be integers. We say that* d *divides* n*, and write* $\boxed{d \mid n}$*, 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* $\boxed{a \equiv b \pmod{m}}$*, whenever* $m \mid (a - b)$*.*

Recall: Predicate is a statement that is true or false depending on the values of its variables.

Example 16

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

$$\Big(a \equiv b \pmod{m} \text{ and } b \equiv c \pmod{m} \Big)$$

$$\Rightarrow \Big(a \equiv c \pmod{m} \Big) \quad ?$$

Exercise.

Proposition 17 *For every integer* n,

congruence modulo 2 is nothing but being even or odd

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: