Simple and composite statements

A statement is *simple* (or *atomic*) when it cannot be broken into other statements, and it is *composite* when it is built by using several (simple or composite statements) connected by *logical* expressions (e.g., if…then…; …implies …; …if and only if …; …and…; either …or …; it is not the case that …; for all …; there exists …; etc.)

Examples:

'2 is a prime number'

'for all integers m and n, if $m \cdot n$ is even then either n or m are even'

* Typo in printed notes

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.

The main proof strategy for implication:

To prove a goal of the form

$$P \implies Q$$

assume that P is true and prove Q.

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

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

1. Write: $\mathrm{Assume\ P}$.
2. Show that Q logically follows.

Scratch work:

Before using the strategy

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

After using the strategy

Assumptions	Goal
	Q
$\vdots$	
P	

Proposition 8 *If* m *and* n *are odd integers, then so is* $m \cdot n$.

PROOF:

compound implication

(m and n odd integers $\Longrightarrow$ $m \cdot n$ odd)

Assume m and n are odd integers. We will show that $m \cdot n$ is odd. By assumption, m is of the form $2k+1$ for some integer k and n is of the form $2l+1$ for some integer l. Thus,

$$m \cdot n = (2k+1) \cdot (2l+1) = \ldots$$

$\square$

An alternative proof strategy for implication:

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

Def

the *contrapositive* of ‘P implies Q’ is ‘not Q implies not P’

In symbols, $P \Rightarrow Q$ is equivalent to

$$\neg Q \Rightarrow \neg P$$

An alternative proof strategy for implication:

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

Since

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

we obtain the following:

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.*

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. ~~Assume x is irrational; That is x is not of the form m/n for integers m and n~~. We will prove the contrapositive; That is, $\sqrt{x}$ rational implies x rational. Assume $\sqrt{x}$ is rational.

...

$\square$

Logical Deduction — Modus Ponens —

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,

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

The use of implications:

To use an assumption of the form $\mathrm{P} \implies \mathrm{Q}$, 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:

Assumptions

(1) P_1, P_2, P_3 statements

(2) $P_1 \Rightarrow P_2$

(3) $P_2 \Rightarrow P_3$

(4) P_1

Goal

P_3

(4) & (2), by MP, we have

(5) P_2

(5) & (3), by MP, we have

P_3.

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: Assume n is an integer.

($\Longrightarrow$) We prove: n even $\Rightarrow$ n^2 even. So further assume n is even; That is, $n = 2k$ for some integer k. Then, $n^2 = (2k)^2 = 2(2k^2)$ which is of the form 2ℓ (for $\ell = 2k^2$) and so even.

($\Longleftarrow$) We prove: n^2 even $\Rightarrow$ n even. ~~Assume n^2 even; That is, $n^2 = 2k$ for some integer k.~~ by establishing the contrapositive; That is

n odd $\Rightarrow n^2$ odd.

But this holds as a corollary of

m and n odd $\Rightarrow m \cdot n$ odd

which we have already shown $\square$

Divisibility

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* $m \mid (a - b)$*.*

if ... (unravel) ...

a is congruent to b modulo m

Example 16

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