Conjunction

Conjunctive statements are of the form

$$\boxed{P \textbf{ and } Q}$$

or, in other words,

$$\boxed{\text{both } P \text{ and also } Q \text{ hold}}$$

or, in symbols,

$$\boxed{P \wedge Q} \qquad \text{or} \qquad \boxed{P \,\&\, Q}$$

The proof strategy for conjunction:

To prove a goal of the form

$$P \wedge Q$$

first prove P and subsequently prove Q (or vice versa).

Proof pattern:

In order to prove

$$P \wedge Q$$

1. Write: Firstly, we prove P. and provide a proof of P.
2. Write: Secondly, we prove Q. and provide a proof of Q.

Scratch work:

Before using the strategy

Assumptions	Goal
	$P \wedge Q$
$\vdots$	

After using the strategy

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

Assumptions Goal

$A \wedge B$ Q

A B

The use of conjunctions:

To use an assumption of the form $P \wedge Q$,
treat it as two separate assumptions: P and Q.

Theorem 20 *For every integer* n*, we have that* $6 \mid n$ *iff* $2 \mid n$ *and* $3 \mid n$.

PROOF: Let n be an arbitrary integer.

($\Rightarrow$) $6 \mid n$ Then ($2 \mid n$ and $3 \mid n$)

Assume $6 \mid n$; that is $n = 6k$ for int. k

RTP: $2 \mid n$ and $3 \mid n$

RTP$_1$: $2 \mid n$

$n = 2(3k)$

So $2 \mid n$

RTP$_2$: $3 \mid n$

$n = 3(2k)$

So $3 \mid n$.

$(\Leftarrow)$ ($2|n$ and $3|n$) then $6|n$

<u>Assume</u>: $2|n$ and $3|n$

So $2|n$ i.e. $n=2i$ (int i)

So $3|n$ i.e. $n=3j$ (int j)

<u>RTP</u>: $6|n$

i.e. $n=6k$ for some int k

equivalently $n=2.3.k$ for some int. k

So $3n=3.2.i=6i$

also $2n=2.3.j=6j$

Therefore $n=3n-2n=6i-6j=6(i-j)$.

and we are done. $\boxtimes$

$6 \mid n \iff (2 \mid n \;\&\; 3 \mid n)$

$30 \mid n \iff (2 \mid n \;\&\; 3 \mid n \;\&\; 5 \mid n)$?

and other generalisations?

$12 \mid n \iff$ --- ?

Existential quantification

Existential statements are of the form

> **there exists** an individual x in the universe of discourse for which the property $P(x)$ holds

or, in other words,

> **for some** individual x in the universe of discourse, the property $P(x)$ holds

or, in symbols,

equivalent to $\exists y. P(y)$

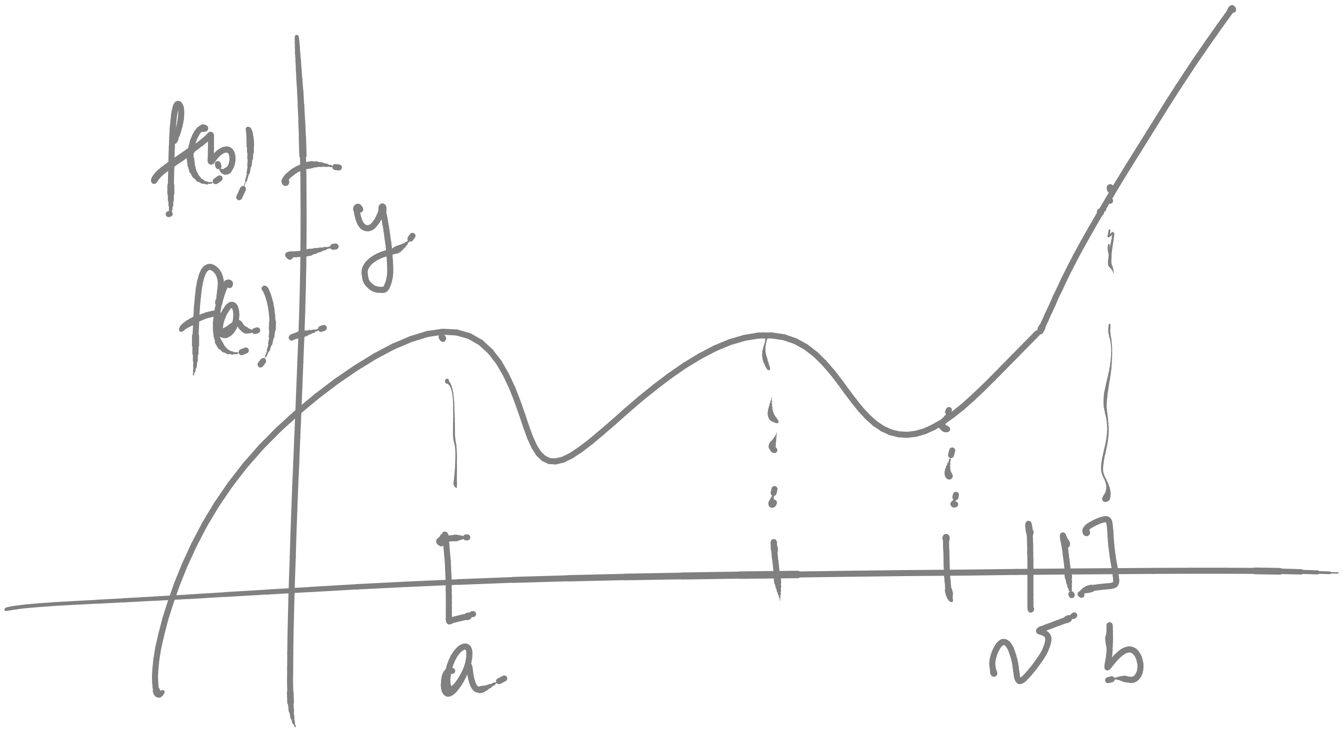
$$\boxed{\exists x. P(x)}$$

Example: The Pigeonhole Principle.

Let n be a positive integer. If $n + 1$ letters are put in n pigeonholes then there will be a pigeonhole with more than one letter.

Theorem 21 (Intermediate value theorem) *Let f be a real-valued continuous function on an interval $[a, b]$. For every y in between $f(a)$ and $f(b)$, there exists v in between a and b such that $f(v) = y$.*

Intuition:



The main proof strategy for existential statements:

To prove a goal of the form

$$\exists x.\, P(x)$$

find a ***witness*** for the existential statement; that is, a value of x, say w, for which you think $P(x)$ will be true, and show that indeed $P(w)$, i.e. the predicate $P(x)$ instantiated with the value w, holds.

Proof pattern:

In order to prove

$$\exists x.\, P(x)$$

1. Write: $\mathrm{Let}\ w = \ldots$ (the witness you decided on).
2. Provide a proof of $P(w)$.

Scratch work:

Before using the strategy

Assumptions	Goal
	$\exists x.\, P(x)$
$\vdots$	

After using the strategy

Assumptions	Goals
	$P(w)$
$\vdots$	

$w = \ldots$ (the witness you decided on)

Proposition 22 *For every positive integer* k*, there exist natural numbers* i *and* j *such that* $4 \cdot k = i^2 - j^2$.

PROOF: Let k be an arbitrary integer.

RTP: $\exists$ nat. numbers i and j. $4k = i^2 - j^2$.

Consider $i = k+1$

and $j = k-1$

Therefore $i^2 - j^2 = \dots \dots = 4k$. ?

k	i	j
1	2	0
2	3	1
3	4	~~3~~ 2
n	$n+1$	$n-1$

$\sim$ guess!

$$\| \quad (k+1)^2 - (k-1)^2 = \dots = 4k \qquad \boxtimes$$

Assumptions Goal

$\exists x. P(x)$ Q

Let x_0 be such $P(x_0)$ holds.

The use of existential statements:

(or fresh)

To use an assumption of the form $\exists x. P(x)$, introduce a new variable x_0 into the proof to stand for some individual for which the property $P(x)$ holds. This means that you can now assume $P(x_0)$ true.

Theorem 24 *For all integers* l, m, n, *if* $\mathrm{l} \mid \mathrm{m}$ *and* $\mathrm{m} \mid \mathrm{n}$ *then* $\mathrm{l} \mid \mathrm{n}$.

PROOF: Let l, m, n be integers.

Assume $l \mid m$; that is, $\exists i$ int. $l \cdot i = m$ ①

$m \mid n$; that is, $\exists j$ int. $m \cdot j = n$ ②

RTP: $l \mid n$; that is, $\exists k$ int. $l \cdot k = n$

Let i_0 int. such that $l \cdot i_0 = m$ (from ①)

Let j_0 int. such that $m \cdot j_0 = n$ (from ②)

Let $w = i_0 \cdot j_0$. Then $l \cdot w = l \cdot i_0 \cdot j_0 = m \cdot j_0 = n$

$\boxtimes$

Unique existence

The notation

$$\exists!\, x.\, P(x)$$

stands for

the *unique existence* of an x for which the property $P(x)$ holds .

That is,

$$\exists x.\, P(x) \;\wedge\; \Big(\forall y.\, \forall z.\, \big(P(y) \wedge P(z) \big) \implies y = z \Big)$$