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

$$P \land Q$$

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
	$P \wedge Q$
⋮	

After using the strategy

Assumptions	Goal	Assumptions	Goal
	P		Q
⋮		⋮	

The use of conjunctions:

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

$\forall$ int n. $6 | n \iff 2 | n$ & $3 | n$

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 integer. RTP: $6 | n \iff 2 | n$ & $3 | n$.

($\Rightarrow$) Ass. $6 | n$, i.e. $n = k6$ for an int k.

$\therefore$ $n = k.2.3$. $\therefore$ $n = 2.(k.3)$ $\therefore$ $2 | n$.

$\therefore$ $n = 3.(k.2)$. $\therefore$ $3 | n$. $\therefore$ $2 | n$ & $3 | n$.

($\Leftarrow$) Ass. $2 | n$ and $3 | n$. I.e.

$n = 2.i$ and $n = 3.j$ for integers i, j.

$\therefore$ $3.n = 3.2.i = 6i$

$\therefore$ $2.n = 2.3.j = 6j$

$\therefore$ subtracting, $n = 3.n - 2n = 6i - 6j = 6.(i-j)$

$\therefore$ $6 | n$ ☒

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,

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

e.g.

$d \mid n \iff$

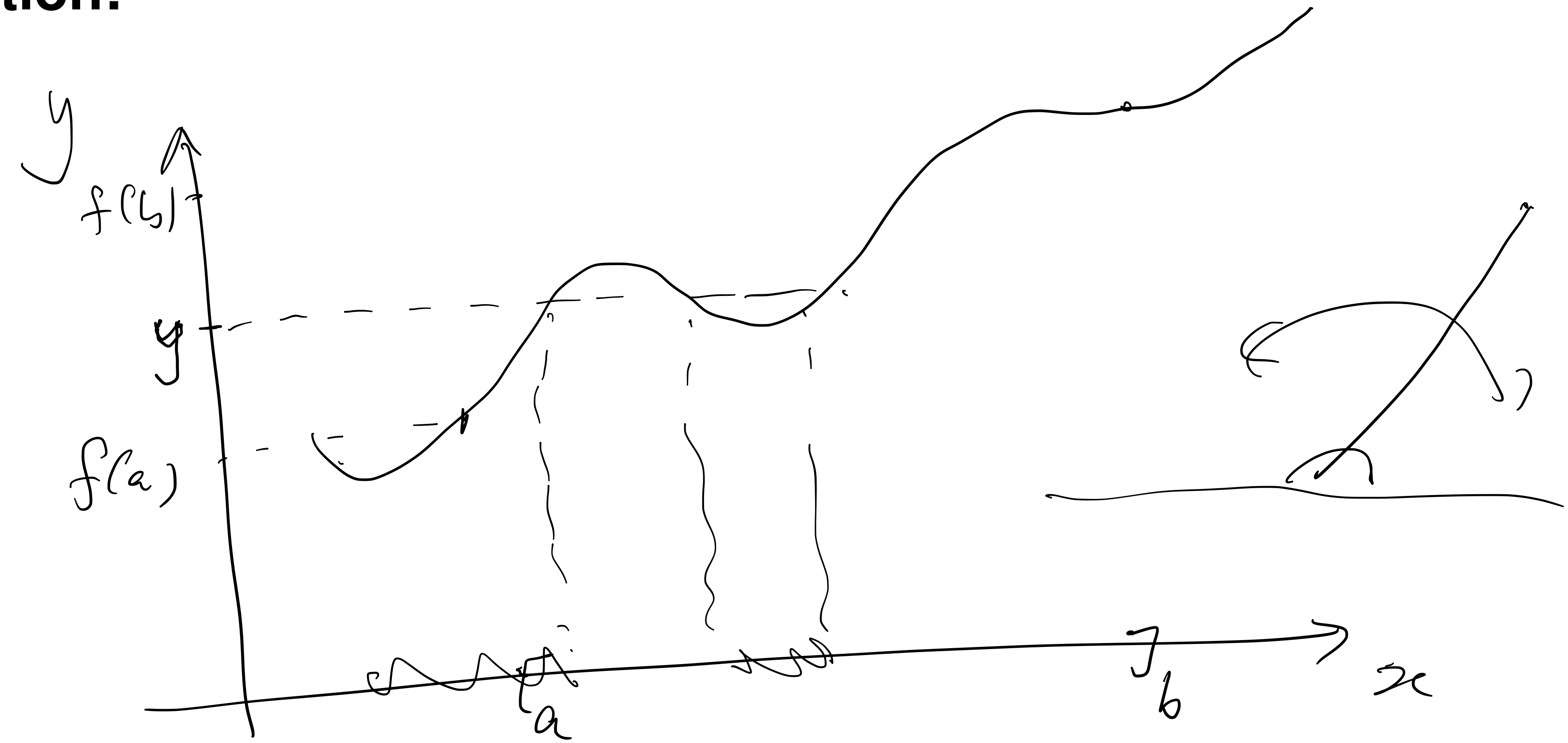
$\exists \text{nat } j.\ n = j \cdot d$

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.

eg. $\text{fn } x.\ x + 1$

$\text{fn } y.\ y + 1$

$\exists y.\ P(y)$

Proof pattern:

In order to prove

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

1. Write: 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)

$\forall$ pos. int. k $\exists$ nat. i, j. $4k = i^2 - j^2$.

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 a pos. int. RTP $\exists$ nat i, j. $4k = i^2 - j^2$.

Want integers i_0 and j_0, nat. nos. s.t.

$$4k = i_0^2 - j_0^2.$$

k		i_0 j_0
1	4	$2^2 - 0^2$
2	8	$3^2 - 1^2$

Take $i_0 = k+1$, $j_0 = k-1$.

Then $i_0^2 - j_0^2 = (k+1)^2 - (k-1)^2$

$= k^2 + 2k + 1 - k^2 + 2k - 1$

$= 4k$.

$\therefore \exists i, j$. — $\boxtimes$

The use of existential statements:

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.

$\forall$ int. l, m, n. $l \mid m \;\&\; m \mid n \Rightarrow l \mid n$

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

PROOF: Let l, m, n be integers. RTP $l \mid m \;\&\; m \mid n \Rightarrow l \mid n$.

Assume $l \mid m \;\&\; m \mid n$, i.e. $\exists i.\ m = i \cdot l$ and $\exists j.\ n = j \cdot m$.

So there are witnesses / hats i_0, j_0. $m = i_0 \cdot l$ and $n = j_0 \cdot m$

RTP. $\exists k.\ n = k \cdot l$. Want k_0 s.t. $n = k_0 \cdot l$

We have $n = j_0 \cdot m = j_0 \cdot i_0 \cdot l = (j_0 \cdot i_0) \cdot l$

So $k_0 = j_0 \cdot i_0$ is a witness for

$\exists k.\ n = k \cdot l$.

$\boxtimes$

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,

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

Disjunction

Disjunctive statements are of the form

$$\boxed{P \text{ or } Q}$$

or, in other words,

$$\boxed{\text{either } P,\ Q, \text{ or both hold}}$$

or, in symbols,

$$\boxed{P \vee Q}$$