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 $Q \implies P$.

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 $Q \implies P$.

Universal quantification

Universal statements are of the form

> **for all** individuals x of the universe of discourse,
> the property $P(x)$ holds

or, in other words,

> no matter what individual x in the universe of discourse
> one considers, the property $P(x)$ for it holds

or, in symbols,

NB: The same $\forall y. P(y)$, $\forall z. P(z)$, ...

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

P(x) predicate

that is a statement whose truth value depends on the values taken by the variable

Example 18

2. *For every positive real number x, if x is irrational then so is $\sqrt{x}$.*

3. *For every integer n, we have that n is even iff so is n^2.*

$\boxed{?}$

Assumptions $\forall y. P(y)$ Goal

⋮ $\forall x. P(x)$

what if you have already assumed things about x?

The main proof strategy for universal statements:

To prove a goal of the form

$$\forall x. P(x)$$

let x stand for an arbitrary individual and prove $P(x)$.

Assumptions ⋮ Goal

$\sim x \sim$ Let ~~x~~ y be arbitrary $P(\cancel{x}\,y)$

Proof pattern:

In order to prove that

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

1. Write: Let x be an arbitrary individual.

   Warning: Make sure that the variable x is new (also referred to as fresh) in the proof! If for some reason the variable x is already being used in the proof to stand for something else, then you must use an unused variable, say y, to stand for the arbitrary individual, and prove $P(y)$.

2. Show that $P(x)$ holds.

Scratch work:

Before using the strategy

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

After using the strategy

Assumptions	Goal
	$P(x)$ (for a new (or fresh) x)
$\vdots$	

Assumption   Goal

$\forall x. P(x)$ G

$P(a)$ $P(b)$ ...

The use of universal statements:

To use an assumption of the form $\forall x. P(x)$, you can plug in any value, say a, for x to conclude that $P(a)$ is true and so further assume it.

This rule is called *universal instantiation*.

Proposition 19 *Fix a positive integer* m. *For integers* a *and* b, *we have that* $a \equiv b \pmod{m}$ *if, and only if, for all positive integers* n, *we have that* $n \cdot a \equiv n \cdot b \pmod{n \cdot m}$.

PROOF: Let m be a positive integer.

$\forall a, b$ integers. $a \equiv b \pmod m \iff \left(\forall \text{ positive } n.\ na \equiv n \cdot b \pmod{n \cdot m} \right)$

Let a, b be arbitrary integers.

($\Rightarrow$) Assume $\boxed{a \equiv b \pmod m}$. that is, $a - b = l \cdot m$ for int l.

RTP: $\forall n.\ na \equiv nb \pmod{n \cdot m}$

Assume n is positive

RTP: $na \equiv nb \pmod{n \cdot m}$

That is, $\boxed{(na - nb) = k \cdot n \cdot m \text{ for int } k}$

Since $a-b = lm$ Then $n(a-b) = nlm$

So $na - nb = l(n.m)$ and we are done $\boxtimes$

Assume

$(\Leftarrow)$ $\forall$ positive n. $na \equiv nb \pmod{nm}$ $(*)$

<u>RTP:</u> $a \equiv b \pmod{m}$

From $(*)$ by instantiation (taking $n = 1$) we have $1 \cdot a \equiv 1 \cdot b \pmod{1 \cdot m}$

Hence $a \equiv b \pmod{m}$. $\boxtimes$

Equality axioms

Just for the record, here are the axioms for *equality*.

- Every individual is equal to itself.

$$\forall x.\ x = x$$

- For any pair of equal individuals, if a property holds for one of them then it also holds for the other one.

$$\forall x. \forall y.\ x = y \implies \big(P(x) \implies P(y)\big)$$

NB From these axioms one may deduce the usual intuitive properties of equality, such as

$$\forall x. \forall y.\ x = y \implies y = x$$

and

$$\forall x. \forall y. \forall z.\ x = y \implies (y = z \implies x = z) \quad .$$

However, in practice, you will not be required to formally do so; rather you may just use the properties of equality that you are already familiar with.

Conjunction

Conjunctive statements are of the form

$$\boxed{P \text{ **and** } Q}$$

or, in other words,

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

or, in symbols,

$$\boxed{P \land Q} \quad \text{or} \quad \boxed{P \ \& \ Q}$$

$\underline{NB}$: $(P \Leftrightarrow Q) =_{df} (P \Rightarrow Q) \wedge (Q \Rightarrow P)$

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
$\vdots$		‖	$\vdots$	

Assumption Goal

$P \wedge Q$ G

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.

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

PROOF: $\forall n$ integer. $6 \mid n \iff (2 \mid n \wedge 3 \mid n)$

Let n be an integer.

RTP: $6 \mid n \iff (2 \mid n \wedge 3 \mid n)$

$(\Longrightarrow)$ Assume $6 \mid n$; That is, $\boxed{n = 6k \text{ for int } k}$ (*)

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

Lemma

$a \mid b \wedge b \mid c \Rightarrow a \mid c$

RTP: $2 \mid n$, i.e. $n = 2p$ for int p

(*) So $n = 2p$ for $p = 3k$

RTP: $3 \mid n$, i.e. $n = 3q$ for int q

So by (*) $n = 3 \cdot q$ for $q = 2k$

RTP:

$(\Rightarrow)$ $(2|n \wedge 3|n) \Rightarrow 6|n$

Assume: $2|n \wedge 3|n$ ~ So $2|n$ and also $3|n$; i.e.

$\boxed{n = 2i \text{ for some } i \text{ int}}$

and

$\boxed{n = 3j \text{ for some } j \text{ int}}$

RTP: $6|n$

That is $n = 6k$ (k int)

proof idea:

$3n = 3.2.i = 6i$

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

$n = 3n - 2n = 6i - 6j$

$= 6(i - j)$