

Bi-implication

Some theorems can be written in the form

P is equivalent to Q

or, in other words,

P implies Q, and vice versa

or

Q implies P, and vice versa

or

P if, and only if, Q

P iff Q

or, in symbols,

$P \iff Q$

Proof pattern:

In order to prove that

$$P \iff Q$$

1. Write: (\implies) and give a proof of $P \implies Q$.
2. Write: (\impliedby) 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,

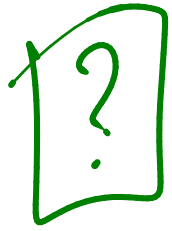
NB: The same by $P(y)$,
 $\forall z, P(z), \dots$

$\forall x. P(x)$

\rightarrow $P(x)$ 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 .



Assumptions

$\forall y. P(y)$ God
"
 $\forall x. P(x)$

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

$\sim x$

Let x be arbitrary

$P(x)$

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

$\forall x. P(x)$

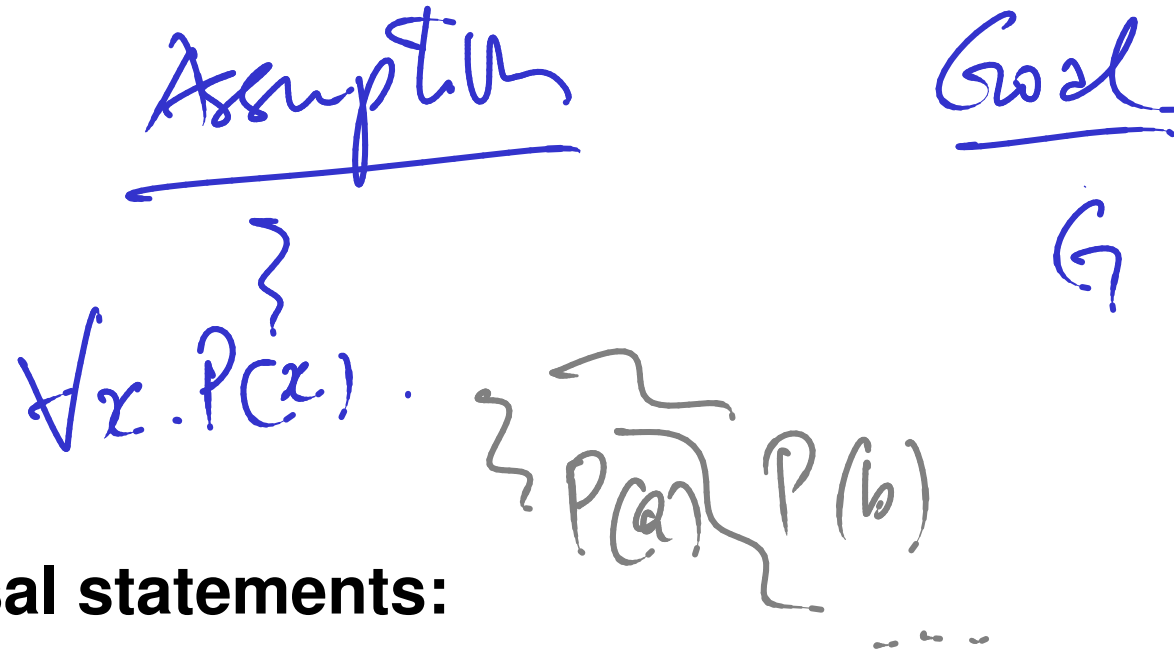
After using the strategy

Assumptions

⋮

Goal

$P(x)$ (for a new (or fresh) x)



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.

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

Let a, b be arbitrary integers.

(\Rightarrow) Assume $a \equiv b \pmod{m}$ 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, $(na - nb) = k \cdot n \cdot m$ for int k

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

So $na - nb = l(nm)$ and we are done \square

Assume

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

RTP: $a \equiv b \pmod{m}$

From (*) by instantiation (taking $n=1$) we

have $1 \cdot a \equiv 1 \cdot b \pmod{1 \cdot m}$

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

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.

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

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

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

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

P and Q

or, in other words,

both P and also Q hold

or, in symbols,

$P \wedge Q$

or

$P \& Q$

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

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

$P \wedge Q$

After using the strategy

Assumptions

⋮

Goal

P

Assumptions

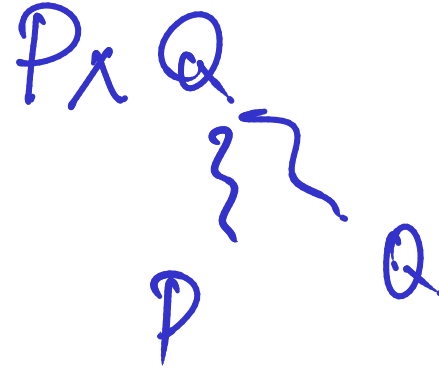
⋮

Goal

Q

Assumption

Goal



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

(\implies) Assume $6 \mid n$; that is, $n = 6k$ for int k (*)

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

Lemma

$a \mid b \wedge b \mid c \implies a \mid c$

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

RTP: $6|n$

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

proof idea:

$3|i$; i int.

and $n = 2i$ for some i int

$n = 3j$ for some j int

$$3n = 3 \cdot 2 \cdot i = 6i$$

$$2 \cdot n = 2 \cdot 3 \cdot j = 6j$$

$$n = 3n - 2n = 6i - 6j \\ = 6(i - j)$$