UNIVERSAL QUANTIFICATION

- How to prove them as goals.

&

- How to use them as assumptions.

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,

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

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*.*

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 $P(x)$.

Proof pattern:

In order to prove that

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

1. Write: Let x be an arbitrary individual.

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

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)
$\vdots$	

Unprovable

Assumptions	Goal
⋮	for all integers n, $n \geq 1$
(*) $n > 0$	
⋮	

Unprovable

Assumptions

⋮

(*) $n > 0$

⋮

Goal

for all integers n, $n \geq 1$

Assumptions

⋮

(*) $n > 0$

⋮

(**) n is an integer

Goal

$n \geq 1$

Unprovable

Assumptions

Goal

$\vdots$

(*) $n > 0$

$\vdots$

$\boxed{\text{for all integers } n,\ n \geq 1}$

for all integers x, $x \not\geq 1$

Unprovable

Assumptions

⋮

(*) $n > 0$

⋮

Goal

$\boxed{\text{for all integers } n,\ n \geq 1}$

for all integers x, $x \geq 1$

Assumptions

⋮

(*) $n > 0$

⋮

(**) x is an integer
[x new or fresh in the proof]

Goal

$x \geq 1$

How to use universal statements

Assumptions

$\vdots$

$\forall x . x^2 \geq 0$

$\vdots$

$\pi^2 \geq 0$

$e^2 \geq 0$

$0^2 \geq 0$

$\vdots$

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.

Let a and b be arbitrary integers.

<u>RTP</u>: $a \equiv b \pmod{m} \iff \forall$ pos. int. n $n \cdot a \equiv n \cdot b \pmod{n \cdot m}$

<u>RTP</u>:

(1) $a \equiv b \pmod{m} \Rightarrow \forall$ pos. int n. $n \cdot a \equiv n \cdot b \pmod{n \cdot m}$

and

(2) $(\forall$ pos. int. n, $n \cdot a \equiv n \cdot b \pmod{n \cdot m}) \Rightarrow a \equiv b \pmod{m}$

Let m be a positive integer.

Let a and b be arbitrary integers.

RTP

(2) $(\forall \text{ pos. int. } n,\ n\cdot a \equiv n\cdot b \pmod{n\cdot m}) \Rightarrow a \equiv b \pmod{m}$

Assume

$\forall$ pos. int. n, $n\cdot a \equiv n\cdot b \pmod{n\cdot m}$

Then, by instantiation, we have

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

that is

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

Let m be a positive integer.

Let a and b be arbitrary integers.

<u>RTP</u>:

(1) $a \equiv b \pmod{m} \Rightarrow \forall$ pos. int n.

$$n \cdot a \equiv n \cdot b \pmod{n \cdot m}$$

<u>Assume</u>

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

<u>RTP</u>: $\forall$ pos. int. n, $n \cdot a \equiv nb \pmod{nm}$.

Let n be a positive integer.

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

i.e. $(na - nb) = k(n \cdot m)$ for an int. k

From assumption

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

we have $a - b = i \cdot m$ for an int. i

Hence

$$n(a-b) = n \cdot i \cdot m$$

and so

$$na - nb = i\,(n \cdot m).$$

$\boxtimes$