Bi-implication

Some theorems can be written in the form

\[ P \text{ is equivalent to } Q \]

or, in other words,

\[ P \text{ implies } Q, \text{ and vice versa} \]

or

\[ Q \text{ implies } P, \text{ and vice versa} \]

or

\[ P \text{ if, and only if, } Q \]

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 \( Q \implies P \).
Divisibility and congruence

Definition 12  Let $d$ and $n$ be integers. We say that $d$ divides $n$, and write $d \mid n$, whenever there is an integer $k$ such that $n = k \cdot d$.

Example 13  The statement $2 \mid 4$ is true, while $4 \mid 2$ is not.

Definition 14  Fix a positive integer $m$. For integers $a$ and $b$, we say that $a$ is congruent to $b$ modulo $m$, and write $a \equiv b \pmod{m}$, whenever $m \mid (a - b)$.

Example 15

1. $18 \equiv 2 \pmod{4}$

2. $2 \equiv -2 \pmod{4}$

3. $18 \equiv -2 \pmod{4}$
Proposition 16  For every integer \( n \),

1. \( n \) is even if, and only if, \( n \equiv 0 \pmod{2} \), and

2. \( n \) is odd if, and only if, \( n \equiv 1 \pmod{2} \).

**Proof:** Let \( n \) be an integer.

(\( \Rightarrow \)) \( n \) is even \( \Rightarrow n \equiv 0 \pmod{2} \)

Assume \( n \) is even; that is, \( n = 2i \) for an integer \( i \).

RTP: \( n - 0 \) is a multiple of 2 which is the case because \( n = 0 + n \).

(\( \Leftarrow \)) \( n \equiv 0 \pmod{2} \Rightarrow n \) is even.

Assume \( n \equiv 0 \pmod{2} \) and show \( n \) is even.
Congruence modulo m

\[ a-m \rightarrow a \rightarrow a+m \rightarrow a+2m \rightarrow \ldots \]
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 quantifications

- 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,

\[
\forall x. P(x) \iff \forall y. P(y)
\]
Example 17

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

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.

   **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

\begin{align*}
\text{Assumptions} & \quad \text{Goal} \\
\forall x. P(x) & \\
\vdots &
\end{align*}

After using the strategy

\begin{align*}
\text{Assumptions} & \quad \text{Goal} \\
P(x) & \quad \text{(for a new (or fresh) } x) \\
\vdots &
\end{align*}
Example:

Assumptions

\[ n > 0 \]

Goal

for all integers \( n \), \( n \geq 1 \)

unprovable

\( \text{RIP: } n \geq 1 \)

Then from ① and ② we have \( n \geq 1 \). \( \times \)
Example:

Assumptions

\[ n > 0 \]

Goal

for all integers \( n, n \geq 1 \)

unprovable

\[ \equiv \text{for all int. } k, k \geq 1 \]

Let \( k \) be an integer (with \( k \) fresh/new in the proof).

RTP: \( k \geq 1 \)

which is not provable.
How to use universal statements

Assumptions

\[ \forall x. x^2 \geq 0 \]

\[ \pi^2 \geq 0 \]

\[ e^2 \geq 0 \]

\[ 0^2 \geq 0 \]
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 18  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.

$(\Rightarrow)$ Assume $a \equiv b \pmod{m} \iff a - b = im$ for some integer $i$.

RTE: $A$ positive integer $n$. $n \cdot a \equiv n \cdot b \pmod{n \cdot m}$

Let $n$ be an arbitrary positive integer.

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

That is, $n a - n b = k \cdot n m$ for an integer $k$.

By (1), $n(a - b) = n \cdot i \cdot m$ and so $n a - n b = n(a - b)$ is a multiple of $n \cdot m$. 

— 72 —
\( \leq \) Assume \( \forall \) pos. int. \( n \), \( na \equiv nb \pmod{nm} \)

RTP. \( a \equiv b \pmod{m} \)

Then from 0 by instantiation of \( n \) to 1

we have \( 1 \cdot a \equiv 1 \cdot b \pmod{1 \cdot m} \)

as required.
Equality in proofs

Examples:

- If $a = b$ and $b = c$ then $a = c$.

- If $a = b$ and $x = y$ then $a + x = b + x = b + y$. 
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.
Conjunctions

- How to *prove* them as goals.
- How to *use* them as assumptions.
Conjunction

Conjunctive statements are of the form

$P \text{ and } Q$

or, in other words,

both $P$ and also $Q$ hold

or, in symbols,

$P \land Q$ or $P \& Q$
The proof strategy for conjunction:

To prove a goal of the form

\[ P \land Q \]

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

\[ P \land Q \]

::

After using the strategy

Assumptions  Goal  Assumptions  Goal

\[ P \]

\[ Q \]

::  ::
The use of conjunctions:

To use an assumption of the form $P \land Q$, treat it as two separate assumptions: $P$ and $Q$. 
Theorem 19  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. Let $n = 6k$ for an integer $k$.

($\Rightarrow$) Assume $6 \mid n \iff n = 6k$ for an integer $k$.

- **RTP:** $2 \mid n \land 3 \mid n$
  - **RTP:** $2 \mid n$
    - $n = 2i$ for an integer $i$.
    - **RTP:** $3 \mid n$

---

— 84 —
Since by (1), \( n = 6k \). Then \( n = 2(3k) \) and so \( 2 \mid n \).

\[ \text{Lemma: } (a | b \land b | c) \Rightarrow (a | c). \quad \text{Exercise.} \]

\[ \iff \text{ RDP: } (2 \mid n \land 3 \mid n) \Rightarrow 6 \mid n \]

\[ \text{Assume: } 2 \mid n \land 3 \mid n \]

\[ \text{So } 2 \mid n \iff ^{(1)} n = 2i \text{ for int } i. \]

\[ \text{and } 3 \mid n \iff ^{(2)} n = 3j \text{ for int } j. \]

\[ \text{RDP: } 6 \mid n \iff n = 6k \text{ for an int } k. \]

From (1) and (2), \( 2i = 3j \). \text{Exercise.}

From (1), \( 3n = 6i \). From (2), \( 2n = 6j \). \text{Exercise.}


\[ \forall n \quad (2 \mid n \land 3 \mid n \land 5 \mid n) \iff (30 \mid n) \]

\[ \forall a, b, \quad (a \mid n \land b \mid n) \iff (a \cdot b) \mid n \quad ? \]