Proofs

Rules of inference

(1) Modus ponens

p T

$p \to q$ T

$\therefore \; q$

p

(T) "Today is Tuesday"

(T) "If today is Tuesday, Bob is working"

p q

"Bob is working" must be true.

p	q	$p \to q$
T	T	T
T	F	F
F	T	T
F	F	T

So, in mathematics:

if p holds (i.e., is true), and $p \to q$ holds, then q must hold.

---

(2) Modens tollens

$\neg q$

$p \to q$

$\therefore \; \neg p$

"not (Bob is working)"

"if today is Tuesday, Bob is working"

"not (today is Tuesday)"

p	q	$\neg q$	$p \to q$
T	T	F	T
T	F	T	F
F	T	F	T
F	F	T	T

Modus tollens via contraposition

reminder:

p	q	$p \to q$	$\neg p$	$\neg q$	$\neg q \to \neg p$
T	T	T	F	F	T
T	F	F	F	T	F
F	T	T	T	F	T
F	F	T	T	T	T

contraposition: $p \to q \equiv \neg q \to \neg p$

1. $p \to q$ is given
2. $\neg q$ is given
3. $p \to q \equiv \neg q \to \neg p$ using the contrapision

$$\begin{array}{l} \neg q \\ \neg q \to \neg p \\ \hline \therefore \neg p \end{array}$$

Example using modus ponens

"for every integer x, if x is odd, then $x+1$ is even."

"x is odd" p

"$x+1$ is even" q

"if x is odd, then $x+1$ is even" $p \to q$

assume "x is odd" is true $1, 3, 5, \dots$

"being odd" means $x = 2 \cdot y + 1$

$2 \cdot 0 + 1 = 1$

$2 \cdot 1 + 1 = 3$

"$\underbrace{\text{Let } x \text{ be an integer}}_{\text{"any"}}$, such that $\underbrace{x = 2y+1}_{\text{"odd"}}$."

<u>NOW</u>: we need to show that $x+1$ is even.

"being even" means $\boxed{w = 2 \cdot v}$

$\Rightarrow \quad x = 2y+1$ we add $+1$ to both sides

$$x+1 = 2y+1+1$$
$$x+1 = 2y+2$$
$$x+1 = 2(\underbrace{y+1}_{=v})$$
$$x+1 = 2 \cdot v$$

even number

Theorem = statement, which has been proven on previously proven statements and axioms.

Axiom = generally accepted statements

→ "every natural number n has exactly one successor $n+1$."

"$1+1=2$"

Proof = a clear and concise explanation that <u>convinces</u> another mathematician that a statement is true.

Example

$(\forall x \in \mathbb{Z})(\forall y \in \mathbb{Z})$ if x is odd and if y is odd then $\underbrace{x \cdot y}_{\text{product}}$ is odd.

$x = 2a+1$
$y = 2b+1$

$x \cdot y = (2a+1)(2b+1) =$
$= 4ab + 2a + 2b + 1 =$
$= 2\underbrace{(2ab + a + b)}_{m} + 1$
$= 2m+1$

by def. is an odd integer $\square$

$p \leftrightarrow q = (p \xrightarrow{a)} q) \wedge (q \xrightarrow{b)} p)$

"$\underbrace{x \text{ is even}}_{p}$ if and only if $\underbrace{x+1 \text{ is odd}}_{q}$."

a) if (x is even) then ($x+1$ is odd).
b) if ($x+1$ is odd) then (x is even).

(a) $x = \underbrace{2 \cdot v}_{\text{even}} \Rightarrow x+1 = \underbrace{2v+1}_{\text{odd}}$ ✓

(b) $x+1 = 2v+1 \Rightarrow x+1 = 2v+1 \quad / -1$
$x = 2v$
by def. even.

number

How to handle logical statements:

Statement — **Ways to prove it**

(*) p
- prove that p is true
- assume p is false, and derive a contradiction

$p \wedge q$
- prove p and q (*)

$p \vee q$
- prove p
- prove q
- assume $\neg p$ and deduce q is true
- assume $\neg q$ and deduce p is true

$p \to q$
- assume p is true and deduce that q is true.
- assume $\neg q$ and deduce $\neg p$.

p	q	$p \to q$
T	T	T
T	F	F
F	T	T
F	F	T

$p \longleftrightarrow q$
- prove $(p \to q)$ and $(q \to p)$
- prove p and q
- prove $\neg p$ and $\neg q$

p	q	$p \leftrightarrow q$
T	T	T
T	F	F

F	T	F
F	F	T

$(\exists x \in S)\, P(x)$ – find an x in S such that $P(x)$

$(\forall x \in S)\, P(x)$ – prove that $P(x)$ holds for all x in S.

Example: for every integer x, if $\underbrace{x \text{ is even}}_{A}$, then $\underbrace{x^2 \text{ is even}}_{B}$.

let x be any integer so that $x = 2y$.

Show: x^2 is even ; $x^2 = 2t$

$$\rightarrow \quad x = 2y \;\Big|^2$$

$$x^2 = 4y^2 = (2y)^2$$

$$= 2(\underbrace{2y^2}_{=t})$$

$x^2 = 2 \cdot t$ by definition is even.

Direct proof for statements $p: A \rightarrow B$.
assume A and deduce B.

– shown a few times.

we assume A is true and then, using aksioms, definitions and previously proven theorems to deduce that B must be true.

Example: Prove that if m, n are perfect squares, then $m \cdot n$ is also a perfect square.

A number x is a perfect square if $x = y^2$

$9 = 3^2$

$16 = 4^2$

$25 = 5^2$

$3^2 \cdot 4^2 = 144$
$= 12^2$

$m = a^2$, $n = b^2$

$\underline{m \cdot n} = a^2 \cdot b^2 = (a \cdot b)^2$ $\square$

therefore, $m \cdot n$ is also a perfect square.

Proof by contradiction: $p: A \to B$

reminder: $\neg(p \to q) \equiv p \wedge \neg q$

We assume A and $\neg B$ and derive a contradiction

Example: if x is rational ($\frac{1}{2}$) and y is irrational ($\sqrt{5}$), then $x+y$ is irrational.

x is rational : $x = \frac{p}{q}$, $q \neq 0$

Assume the negation:
- x is rational : $x = \frac{p}{q}$
- y is irrational
- $x+y$ is not irrational $x+y = \frac{p'}{q'}$, $q' \neq 0$

$$\frac{p}{q} + y = \frac{p'}{q'} \quad \Big| -\frac{p}{q}$$

$$y = \frac{p'}{q'} - \frac{p}{q}$$

$$y = \frac{\overbrace{p' \cdot q - p \cdot q'}^{m}}{\underbrace{q' \cdot q}_{n}}$$

* m, n are also $\in \mathbb{Z}$, as they are the result of operations between $p, q, p', q' \in \mathbb{Z}$

$y = \frac{m}{n}$ by definition is a rational number!

contradicts our assumption

therefore the opposite must hold

Example: Prove that $\sqrt{2}$ is irrational.

Let's assume that $\sqrt{2}$ is rational.

$\sqrt{2} = \frac{a}{b}$, $b \neq 0$ $a, b \in \mathbb{Z}$ $\{1, 2, 3, \ldots\}$

- in addition, we demand $b > 0$

! $a > 0$ also because the same se $\mathbb{Z}$

- now, we choose a, b such that they are the smallest number in our set from which we take b.

$\frac{2}{1}$

$\frac{10}{20} = \frac{1}{2}$

$- \quad a \quad |^2$

$$\sqrt{2} = \frac{\quad}{b} \quad |$$

$$2 = \frac{a^2}{b^2} \quad | \cdot b^2$$

$$\underbrace{2b^2}_{\text{def. of an even number}} = a^2$$

def. of an even number, so a itself is even (remember proof from before)

$$a = \underbrace{2 \cdot k}$$

$$2b^2 = (2k)^2$$

$$2b^2 = 4k^2 \quad / :2$$

$$b^2 = \underbrace{2k^2}$$

def. of an even number, so b itself is even

$$b = 2 \cdot m$$

So, there must be another number m, which in turn must be smaller than b to fulfill the previous constraint.

- But, earlier we required that b is already the smallest number from our set.

So, we cannot $\sqrt{2}$ as $\frac{a}{b}$.

And, therefore, $\sqrt{2}$ cannot be rational, but must be irrational. $\square$

Example: Prove: if $3n+2$ is odd, then n is odd.

$$p: \quad A \rightarrow B$$

$$\neg p: \quad \neg(A \rightarrow B) \equiv A \land \neg B$$

A: $3n+2$ is odd

B: n is odd

Proof by contradiction: $A \land \neg B$

A: $3n+2$ is odd

B: n is not odd = n is even.

$$n = 2k$$

$\underbrace{3n+2 \text{ is odd}}$; use $n=2k$:

$$3(2k)+2 = 6k+2 = 2(\underbrace{3k+1})$$

$$\underbrace{=2m'}_{\text{definition of an even number}}$$ ↯

$\Rightarrow$ A is not odd as we have demanded $\square$

Mathematical induction

Def 46: To prove that $P(n)$ is true for all positive integers n, where $P(n)$ is a propositional function, we complete three steps:

1. we verify $P(1)$ is true "basic step"
2. we assume $P(k)$ "inductive step"
3. we show that the implication $P(k) \to P(k+1)$ is true for all positive integers k.

Example: Prove that for every positive integer n:

$$1+2+3+\ldots+n = \frac{n(n+1)}{2}$$

("Gaussian Sum formula")

$$P(1): \quad 1 = \frac{1\cdot(1+1)}{2} = \frac{1\cdot 2}{2} = 1 \checkmark$$

$$P(k) \quad \boxed{1+2+3+\ldots+k} = \boxed{\frac{k(k+1)}{2}}$$

inductive hypothesis must be used in the argument.

Let's take the next element to be added

k+1 must be added to the sequence

$$\boxed{1+2+3+\ldots+k}+(k+1) =$$

use the IH (inductive hypothesis)

$$= \frac{k(k+1)}{2} + (k+1) = \frac{k(k+1)}{2} + \frac{2(k+1)}{2} =$$

$$= \frac{k(k+1)+2(k+1)}{2} = \frac{(k+1)(k+2)}{2}$$

in turn is: $\frac{n(n+1)}{2}$ when

$$\frac{(k+1)((k+1)+1)}{2}$$

$n = (k+1)$

So, we showed:

$P(1)$ which is the "basic step"

$P(k) \rightarrow P(k+1)$ using $P(k)$ "inductive hypothesis"

and we correctly concluded $P(k+1)$.

So $\forall n (P(n))$. $\square$

Question: Can we use mathematical induction to prove properties about negative integers also (e.g. is there a situation where we have $P(k) \rightarrow P(k-1)$)?

Short answer: Yes, induction can be used for any set of objects which can be represented as a sequence.

E.g. you can use the induction twice:

- once to prove it for all positive integers
- once for all negative integers.

But, note that not all properties can be proven for negative integers.

Want more? see the link on math.stackexchange.com