# Intro to proofs: the statement $P \Rightarrow Q$.

Let $P, Q$ be any statements, like: "it's raining," "$n$ is a perfect square," "$A \subseteq B$," "39 is even."

The following all mean the same thing:

- $P$ implies $Q$,
- $P \Rightarrow Q$,
- If $P$ then $Q$,
- Whenever $P$ is true, $Q$ follows.
- Under the condition $P$, the conclusion $Q$ holds.

Example: if $P$ is "it's Saturday" and $Q$ is "it's the weekend," then $P \Rightarrow Q$. However, $Q \not\Rightarrow P$.

To prove a $P \Rightarrow Q$ statement, assume $P$, then do whatever works to conclude $Q$.

$P \Rightarrow Q$ proof TEMPLATE:

**Theorem.** $P \Rightarrow Q$.

**Proof.** Assume $P$. [Then do what you have to, to get to:] Therefore, $Q$.

So $P \Rightarrow Q$. □

Notes.

1) The last line, "So $P \Rightarrow Q$," is optional.

2) The "□" is to clearly indicate end of proof.

## EXAMPLES.

**Theorem 1.**
If $n$ is an even integer, then $n+1$ is an odd integer.

**Proof.**
Assume $n$ is an even integer. Then $n = 2k$ for some $k \in \mathbb{Z}$. So $n+1 = 2k+1$ for some $k \in \mathbb{Z}$. Therefore, $n+1$ is odd.

$\underbrace{\text{So } n \text{ is even} \Rightarrow n+1 \text{ is odd.}}_{\text{optional statement}}$ □

**Definition:** if $a, b \in \mathbb{Z}$, we say "$a$ divides $b$," written $a | b$, if $b = an$ for some $n \in \mathbb{Z}$.
E.g. $3|6$ $(6 = 3 \cdot 2)$, $7|(-273)$ $(-273 = 7 \cdot (-39))$, $7 \nmid 15$, $7|0$ $(0 = 7 \cdot 0)$, $0|0$, $0 \nmid 7$.

**Proposition 1.** *
Let $b \in \mathbb{Z}$. If $10|b$, then $5|b$.

**Proof.**
Assume $b \in \mathbb{Z}$ and $10|b$. Then $b = 10n$ for some $n \in \mathbb{Z}$. But $10 = 5 \cdot 2$, so
$b = (5 \cdot 2)n = 5 \cdot 2n$. Therefore, $5|b$.

So $b \in \mathbb{Z}$ and $10|b \Rightarrow 5|b$. □

* A proposition is like a theorem, only less significant. (Significance is subjective.)

[ Question: is the converse to Proposition 1 true? That is: does $5 \mid b \Rightarrow 10 \mid b$, for $b \in \mathbb{Z}$?

Answer: no. For example, $5 \mid 25$, but $10 \nmid 25$. ]

**Theorem 2.**

If $n \in \mathbb{Z}$, then $n^2 + 5n + 4$ is even.

**Proof.**

** Assume $n \in \mathbb{Z}$. We consider two cases:

(a) Suppose $n$ is even. Then $n = 2k$ for some $k \in \mathbb{Z}$. So

$$\begin{aligned} n^2 + 5n + 4 &= (2k)^2 + 5(2k) + 4 \\ &= 4k^2 + 10k + 4 \\ &= 2(2k^2 + 5k + 2) \\ &= 2m, \end{aligned}$$

where $m = 2k^2 + 5k + 2 \in \mathbb{Z}$. So $n^2 + 5n + 4$ is even.

(b) Suppose $n$ is odd. Then $n = 2k+1$ for some $k \in \mathbb{Z}$. So

$$\begin{aligned} n^2 + 5n + 4 &= (2k+1)^2 + 5(2k+1) + 4 \\ &= 4k^2 + 4k + 1 + 10k + 5 + 4 \\ &= 4k^2 + 14k + 10 \\ &= 2(2k^2 + 7k + 5) \\ &= 2\ell, \end{aligned}$$

where $\ell = 2k^2 + 7k + 5 \in \mathbb{Z}$. So $n^2 + 5n + 4$ is even.

Now $n$ must be even or odd, and in either case, $n^2 + 5n + 4$ is even.
So $n \in \mathbb{Z} \Rightarrow n^2 + 5n + 4$ is even. $\square$

** This method is called <u>proof by cases</u>.

<u>Theorem 3.</u>
Let $a,b,c \in \mathbb{Z}$. If $a|b$ and $b|c$, then $a|c$.

<u>Proof.</u>
Assume $a,b,c \in \mathbb{Z}$, and $a|b$ and $b|c$.

Then $b = an$ for some $n \in \mathbb{Z}$, and $c = bm$ for some $m \in \mathbb{Z}$. So

$$c = bm = (an)m = a \cdot (mn).$$

That is, $c = ak$, where $k = mn \in \mathbb{Z}$. Therefore, $a|c$.

So $a,b,c \in \mathbb{Z}$, $a|b$, $b|c \Rightarrow a|c$. $\square$