A theorem is a mathematical statement that is always true. The most common form of a theorem is the following:

If $P$ then $Q$.

where $P$ is a list of conditions (or more technically hypotheses) and $Q$ is the conclusion.

Consider the following example. We know that a spider usually has eight legs. Stating this in the form of a theorem, we might write:

If $x$ is a normal healthy spider then $x$ has 8 legs.

The converse of the theorem, If $P$ then $Q$, is

If $Q$ then $P$.

(a similar looking statement but with the $P$ and the $Q$ interchanged). The converse of our “theorem” about spiders is:

If $x$ has 8 legs then $x$ is a normal healthy spider.

This statement is not always true – $x$ could be a crab, say. So it is not a theorem, and we would say in such a case that the converse (of the original “theorem” about spiders) is false.

The statement, If $P$ then $Q$, may also be stated in each of the following ways:

- $P$ only if $Q$.
- $P \implies Q$. (the ‘ $\implies$ ’ symbol is read implies)
- $Q$ if $P$.

Sometimes a statement ‘If $P$ then $Q$’ and its converse ‘If $Q$ then $P$’ are both always true. These two statements can be merged into one in each of the following ways:

- $P$ if and only if $Q$.
- $P \iff Q$.

(You will have to read the dangerous bend above for the language to make English sense.)

Proofs

One way to prove a statement of form ‘If $P$ then $Q$’ is according to the following structure:

Assume $P$.

Sequence of statements that each follow from earlier statements.

Deduce $Q$.

Conclude: “if $P$ then $Q$”.

\[\square\]
To prove an identity of form $LHS = RHS$, start with one side and reduce it to the other lining up all the $=$ signs, e.g.

\[
LHS = \ldots
\]
\[
\vdots
\]
\[
= RHS
\]

We may prove inequalities such as $LHS < RHS$ in an analogous way, except that the relational symbols we line up may be any of $<, \leq$ or $=$.

The following demonstrates both the directionality of a proof and why one should never manipulate both sides at once in proving an identity.

\[
0 = 1
\]
\[
0 \cdot 0 = 1 \cdot 0
\]
\[
0 = 0
\]

From which we can deduce (the rather vacuous statement)

\[
\text{if } 0 = 1 \text{ then } 0 = 0.
\]

Observe that while the final statement $0 = 0$ is true the first statement $0 = 1$ is false. We can deduce nothing whatever about an earlier statement from the truth of a later statement. Truth flows down not up.

**Mathematical Induction**

Suppose you need to find a general formula for the sum of the first $n$ natural numbers. Ignoring that we could use the theory of arithmetic progressions, you might start by looking for a pattern:

\[
1 = 1
\]
\[
1 + 2 = 3
\]
\[
1 + 2 + 3 = 6
\]
\[
\vdots
\]

and if you are lucky you might guess that:

\[1 + 2 + \cdots + n = \frac{n(n + 1)}{2},\]

but how might you show that this is true, for any natural number $n$?

One way is to use the **Principle of Mathematical Induction (PMI)**. The idea is that you start with some statement that depends on a natural number $n$. (A statement is something that can be either true or false.) Call this statement $P(n)$. Then the PMI states:

If we can show that both

- $P(1)$ is true; and
- for a general natural number $k$, if $P(k)$ is true then $P(k + 1)$ is also true;

then we can conclude that $P(n)$ is true for all natural numbers $n$. 

This is exactly like proving that we can climb a ladder, in the following way.

- First we show we can get on the first (bottom) rung.
- Then we show we can get from any one rung (i.e. the kth rung) to the next rung (i.e. the (k + 1)st rung).

It should be clear that we could then get to any rung of the ladder we like (given enough time).

Let us prove our simple example above by induction.

**Example 1.** First we define \( P(n) : 1 + 2 + \cdots + n = \frac{n(n+1)}{2} \).

Notice, a ‘:’ was used here to indicate that \( P(n) \) is short-hand for everything that follows the ‘:’. Use of a symbol like ‘\( = \)’ instead of ‘::’ would have been too confusing!

- Show \( P(1) \) is true;

  **Proof.** \( P(1) \) is of the form LHS = RHS. To show it is true we start with one side and reduce it to the other side. Now the LHS of \( P(1) \) is just 1 and the RHS of \( P(1) \) is \( \frac{1 \cdot 2}{2} \), i.e.

  \[
  \text{LHS of } P(1) = 1 \quad = \frac{1 \cdot 2}{2} = \text{RHS of } P(1)
  \]

  So \( P(1) \) is true. \( \square \)

- Show, for a general natural number \( k \): if \( P(k) \) is true then \( P(k + 1) \) is also true;

  **Proof.** To prove a statement of form:

  If hypothesis then conclusion

  we assume the hypothesis and deduce from it, the conclusion. Hence, we assume \( P(k) \) is true, i.e. we assume

  \[
  \text{LHS of } P(k) = \text{RHS of } P(k).
  \]

  Now we wish to deduce that \( P(k + 1) \) is true. Now \( P(k + 1) \) is of the form LHS = RHS. So to show it is true we start with one side and reduce it to the other side. (Somewhere along the way we expect to use our assumption that \( P(k) \) is true – incidentally, this assumption is called the inductive assumption). Thus, starting with one side . . .

  \[
  \text{LHS of } P(k + 1) = 1 + 2 + \cdots + k + k + 1
  \]

  \[
  = \text{(LHS of } P(k)) + k + 1
  \]

  \[
  = \text{(RHS of } P(k)) + k + 1, \quad (\text{using the inductive assumption})
  \]

  \[
  = \frac{k(k + 1)}{2} + k + 1
  \]

  \[
  = \frac{k(k + 1) + 2(k + 1)}{2}
  \]

  \[
  = \frac{(k + 1)(k + 2)}{2}
  \]

  \[
  = \frac{(k + 1)((k + 1) + 1)}{2}
  \]

  \[
  = \text{RHS of } P(k + 1)
  \]

  So, if \( P(k) \) is true then \( P(k + 1) \) is true. \( \square \)

Thus we may now deduce that, by the PMI, \( P(n) \) is true for all natural numbers \( n \).
Example 2. Prove that:

If \( x + \frac{1}{x} \) is an integer then \( x^n + \frac{1}{x^n} \) is an integer for all positive integers \( n \).

You will notice differences between the structures of our proof below and that of our elementary example above, but you will notice also great similarities. One of the differences is that the “can get onto the next rung” step of the proof requires two previous rungs, which means that the “can get onto the first rung” step of the proof must be replaced with a proof that one “can get onto the first two rungs” – think of the ladder.

**Proof.** Assume \( x + \frac{1}{x} \) is some integer \( N \).

We show that \( x^n + \frac{1}{x^n} \) is an integer for all positive integers \( n \), by induction.

Let \( P(n): \text{"} f(n) = x^n + \frac{1}{x^n} \text{ is an integer"} \).

Firstly, we prove \( P(1) \) and \( P(2) \).

\[
f(1) = x^1 + \frac{1}{x^1} = x + \frac{1}{x}
\]

So \( \ldots f(1) = x^1 + \frac{1}{x^1} \) is an integer, i.e. \( P(1) \) is true.

\[
f(2) = x^2 + \frac{1}{x^2} = (x + \frac{1}{x})^2 - 2x \cdot \frac{1}{x} = N^2 - 2
\]

So \( \ldots f(2) \) is an integer, i.e. \( P(2) \) is true.

Now we prove: “if \( P(k - 1) \) and \( P(k) \) are true then \( P(k + 1) \) is true”, for \( k \geq 2 \).

Assume \( P(k - 1) \) and \( P(k) \) are true, i.e. that \( f(k - 1) \) and \( f(k) \) are integers. Then

\[
f(k + 1) = x^{k+1} + \frac{1}{x^{k+1}}
\]

\[
= (x^k + \frac{1}{x^k})(x + \frac{1}{x}) - x^k \cdot \frac{1}{x} - \frac{1}{x^k} \cdot x
\]

\[
= (x^k + \frac{1}{x^k})(x + \frac{1}{x}) - (x^{k-1} + \frac{1}{x^{k-1}})
\]

\[
= f(k).N + f(k - 1).
\]

So \( f(k+1) \) is an integer, if \( f(k - 1) \) and \( f(k) \) are, i.e. for \( k \geq 2 \), if \( P(k - 1) \) and \( P(k) \) are true then \( P(k + 1) \) is true.

Thus, by induction, \( P(n) \) is true for all positive integers \( n \).

Hence, we have shown that, if \( x + \frac{1}{x} \) is an integer then \( x^n + \frac{1}{x^n} \) is an integer for all positive integers \( n \). \( \Box \)