1 Theorems

In our first session we were introduced to the idea that a theorem is a mathematical statement that is always true, and that the most basic form a theorem takes is the following:

If \( P \) then \( Q \).

and that this statement can equivalently be expressed in any of the following ways:

- \( P \) only if \( Q \).
- \( P \implies Q \).
- \( P \implies Q \). (This is how the form on the previous line is read.)
- \( Q \) if \( P \).

In last week’s session, we explored different strategies for proving statements of form “\( P \implies Q \)”, with the two main strategies being:

Direct Proof.
Proof by Contradiction.

Often a component of a proof will involve the proof of an identity, a statement of form \( \text{LHS} = \text{RHS} \), that is always true. Essentially, we use the transitivity property of ‘=’:

\[
\text{If } a = b \text{ and } a = c \text{ then } a = c.
\]

Using this property, we organise a proof of an identity, to be a reduction of one side to the other, lining up all the = signs, in the following way:

\[
\text{LHS} = \ldots \\
: \\
= \text{RHS}
\]

We may prove inequalities such as \( \text{LHS} < \text{RHS} \) 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.*
2 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:

\[
\begin{align*}
1 &= 1 \\
1 + 2 &= 3 \\
1 + 2 + 3 &= 6 \\
& \vdots
\end{align*}
\]

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 \( k \)th 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). More formally, we use the Principle of Mathematical Induction when we want to prove an infinite set of statements \( P(1), P(2), P(3), \ldots \), or equivalently when we want to prove,

\[
\forall n \in \mathbb{N}, \ P(n) \text{ is true.}
\]

We prove this in two steps:

(i) We show that \( P(1) \) is true.

(ii) We show that \( \forall k \in \mathbb{N}, \ P(k) \implies P(k + 1). \)

Step (ii) proves an infinite number of statements: \( P(1) \implies P(2), P(2) \implies P(3), \ldots \). In the first place we have:

\[
\begin{align*}
P(1) &\implies P(2). \\
P(1) \text{ holds by (i).} \\
\therefore P(2)
\end{align*}
\]

Now that we have \( P(2) \), and so with \( P(2) \implies P(3) \), we deduce \( P(3) \). In this way, we see that the statements (i) and (ii) are sufficient to deduce \( P(n) \) for all \( n \in \mathbb{N} \).

Let us prove our simple example above by induction.
Example 1. First we define \[ P(n) : \quad 1 + 2 + \cdots + n = \frac{n(n + 1)}{2}. \]

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.

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

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:

\[ \text{If hypothesis then conclusion} \]

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 \( n \).

\[ \square \]

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 \( P(n) \): “\( f(n) = x^n + \frac{1}{x^n} \) is an integer”.

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

\[
\begin{align*}
f(1) &= x^1 + \frac{1}{x^1} = x + \frac{1}{x} \\
\text{So . . . } f(1) &= x^1 + \frac{1}{x^1} \text{ is an integer, i.e. } P(1) \text{ is true.}
\end{align*}
\]

\[
\begin{align*}
f(2) &= x^2 + \frac{1}{x^2} = (x + \frac{1}{x})^2 - 2x \cdot \frac{1}{x} \\
&= N^2 - 2 \\
\text{So . . . } f(2) \text{ is an integer, i.e. } P(2) \text{ is true.}
\end{align*}
\]

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

\[
\begin{align*}
f(k + 1) &= x^{k+1} + \frac{1}{x^{k+1}} \\
&= (x^k + \frac{1}{x^k})(x + \frac{1}{x}) - x^k \cdot \frac{1}{x} - \frac{1}{x^k} \cdot x \\
&= (x^k + \frac{1}{x^k})(x + \frac{1}{x}) - (x^{k-1} + \frac{1}{x^{k-1}}) \\
&= f(k).N + f(k - 1).
\end{align*}
\]

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 \( n \). 

\[ \square \]
The variation of induction above is known as secondary induction. By imagining what conditions make it possible to climb a ladder we can come up with other variations, e.g.

If at the inductive step we can only prove: \( P(k) \implies P(k + 3) \).

Then at the base step we must prove say \( P(1), P(2) \) and \( P(3) \).

Also, sometimes a proposition \( P(n) \) doesn’t start to be true at \( n = 1 \). With:

(i) \( P(n_0) \) holds, and

(ii) \( P(k) \implies P(k + 1) \) for general \( k \),

we deduce \( P(n) \) holds for all integers \( n \geq n_0 \).

And, nearly finally, with the Principle of Complete Induction, the steps are:

(i) Show that \( P(1) \) holds.

(ii) Show that \( P(1), P(2), \ldots, P(k) \implies P(k + 1) \), for general \( k \).

**Example 3.** Show that \( 1 < n \in \mathbb{N} \implies n \) has a prime factor.

**Proof.** In this case \( P(n) \) is the statement “\( n \) has a prime factor”. We start at \( n = 2 \) since \( P(1) \) is false.

(i) \( P(2) \) is true.

For (ii) we suppose \( P(2), P(3), \ldots, P(k) \) are all true. Consider \( P(k + 1) \). If \( k + 1 \) has no factors except itself and 1 then it’s prime and so \( P(k + 1) \) is true. Otherwise, \( k + 1 = ab \) where \( 1 < a < k + 1 \). Since we have assumed \( P(a) \) is true, there is a prime \( p \) which divides \( a \), i.e.

\[
\exists m \in \mathbb{N} \text{ such that } a = pm \\
\implies n + 1 = pm \times b \\
\implies p \mid k + 1 \\
\implies k + 1 \text{ has a prime factor.}
\]

Thus \( P(k + 1) \) follows from \( P(2), P(3), \ldots, P(n) \).

So from (i) and (ii) together, the statement has been proven by PCI, for all integers \( n \geq 2 \). \( \square \)

**Exercises.**

1. Prove for any natural number \( n \) that

   (i) \( 1 + 3 + 5 + \cdots + 2n - 1 = n^2 \);
   (ii) \( 1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{1}{6}n(n + 1)(2n + 1) \);
   (iii) \( 1^3 + 2^3 + 3^3 + \cdots + n^3 = \frac{1}{4}n^2(n + 1)^2 \);
   (iv) \( 1^2 + 4^2 + 7^2 + \cdots + (3n - 2)^2 = \frac{1}{2}n(6n^2 - 3n - 1) \);
   (v) \( 2^2 + 5^2 + 8^2 + \cdots + (3n - 1)^2 = \frac{1}{2}n(6n^2 + 3n - 1) \).
2. Prove that for any natural number \( n \),
\[
2(\sqrt{n+1} - 1) < 1 + \frac{1}{\sqrt{2}} + \cdots + \frac{1}{\sqrt{n}} < 2\sqrt{n}.
\]

3. Prove \( 3^n > 2^n \) for all natural numbers \( n \).

4. Prove Bernoulli’s Inequality which states:
If \( x \geq -1 \) then \((1 + x)^n \geq 1 + nx \) for all natural numbers \( n \).

5. Prove that for any natural number \( n \geq 2 \),
\[
\left(1 - \frac{1}{\sqrt{2}}\right)\left(1 - \frac{1}{\sqrt{3}}\right)\cdots\left(1 - \frac{1}{\sqrt{n}}\right) < \frac{2}{n^2}.
\]

6. Prove that for any natural number \( n \),
\[
\frac{1}{2} \cdot \frac{3}{4} \cdot \frac{5}{6} \cdots \frac{2n-1}{2n} \leq \frac{1}{\sqrt{3n+1}}.
\]

7. Prove that \( 7^{2n} - 48n - 1 \) is divisible by 2304 for every natural number \( n \).

8. For every natural number \( n \), show that
\[
u_n = \frac{(1 + \sqrt{5})^n - (1 - \sqrt{5})^n}{2^n \cdot \sqrt{5}}
\]
is a natural number.
In fact, \( u_n \) is the \( n \)th Fibonacci number.

9. Consider all the possible subsets of the set \( \{1, 2, \ldots, n\} \) which do not contain any consecutive numbers.
Prove that the sum of squares of the products of the numbers in these sets is \((n+1)! - 1\).

10. Prove that for all \( n \in \mathbb{N} \) and \( x \in \mathbb{Z} \setminus \{1\} \), \( x^n - 1 \) is divisible by \( x - 1 \).

11. Given that \( a_1 = -2 \), \( a_2 = -16 \) and \( a_{n+2} = 8a_{n+1} - 15a_n \), prove that \( a_n = 3^n - 5^n \) for all \( n \in \mathbb{N} \).

12. Use Mathematical Induction to prove the following propositions, for \( n \in \mathbb{N} \) (unless further restricted).

   (i) \( 2^1 + 2^2 + \cdots + 2^n = 2^{n+1} - 2 \).

   (ii) \( \frac{n^3}{3} + \frac{n^5}{5} + \frac{7n}{15} \) is an integer.

   (iii) For all \( n > 2 \), the sum of the interior angles of a convex polygon of \( n \) sides is \( 180(n-2)^\circ \).

   (iv) If a set \( A \) contains \( n \) elements then the power set of \( A \) contains \( 2^n \) elements.

   (v) The Fibonacci numbers are defined by:
   \[
   F_1 = F_2 = 1, \text{ and } F_{n+2} = F_n + F_{n+1}, n \geq 1.
   \]
   Show that
   \[
   F_1 + F_2 + \cdots + F_n = F_{n+2} - 1.
   \]