Lecture 29

Proof by induction

Useful proof technique, but given undue prominence in school Maths because it is fairly routine.

Well ordering principle

Every non-empty subset of $\mathbb{N}$ has a smallest element.

We use this principle to prove the following:

Induction principle Let $X \subseteq \mathbb{N}$ be s.t.

(1) $0 \in X$.

(2) $n \in X \Rightarrow n+1 \in X$.

Then $X = \mathbb{N}$.

<u>Proof</u> Suppose that $\mathbb{N} \neq X$.

Then $\mathbb{N} \setminus X \neq \emptyset$.

By the well ordering principle, this set has a smallest element, we call it m.

Observe $m \neq 0$ since by (1) $0 \in X$.

It follows that $m-1 \in X$.

But then by (2), $m \in X$. Contradiction.

It follows that $\mathbb{N} \setminus X = \emptyset$ and so $\mathbb{N} = X$

$\blacksquare$

Application We want to prove

that infinitely many statements

$S_0, S_1, S_2, \ldots$

are all true.

Let $X \subseteq \mathbb{N}$ be defined as follows:

$i \in X \iff S_i$ is true.

If X satisfies the induction principle then $X = \mathbb{N}$ and so S_i is true for all $i \geq 0$.

The proof that $S_0, S_1, S_2, \ldots$

are all true is organized as follows:

(1) Base case. Prove that S_0 is true

(2) IH (Induction hypothesis). Assume that S_n is true.

On this assumption, prove that S_{n+1} is true.

By means of ~~the same~~ similar arguments, the induction principle can be extended.

Define $\mathbb{N}^{\geq m} = \{m, m+1, m+2, \ldots\}$

Then if $X \subseteq \mathbb{N}^{\geq m}$ is s.t.

(1) $m \in X$

(2) $n \in X \Rightarrow n+1 \in X$

Then $X = \mathbb{N}^{\geq m}$.

Examples

When $n \geq 1$ we have De Moivre's theorem

$$(\cos\theta + i\sin\theta)^n = \cos n\theta + i\sin n\theta$$

Proof When $n=1$ result is clearly true.

Assume result holds for n.

We prove that it must hold for $n+1$.

$$(\cos\theta + i\sin\theta)^{n+1} =$$

$$(\cos\theta + i\sin\theta)(\cos\theta + i\sin\theta)^n$$

IH

$$= (\cos\theta + i\sin\theta)(\cos n\theta + i\sin n\theta)$$

$$= \cos(\theta + n\theta) + i\sin(\theta + n\theta) \quad \text{by properties of mult. in } \mathbb{C}.$$

$$= \cos(n+1)\theta + i\sin(n+1)\theta \quad \blacksquare$$

A non-constant polynomial of degree n has at most n roots.

<u>Proof.</u> Clearly true when $n = 1$

Suppose result is true for all polys of degree n

Let $f(x)$ be a poly of degree $n+1$

If $f(x)$ has no roots we are done.

If $f(x)$ has a root a then

$$f(x) = (x-a)\, g(x)$$

where $\deg g(x) = n$.

By (IH) $g(x)$ has at most n roots.

Thus $f(x)$ has at most $n+1$ roots ∎

$$\overline{z_1 + \dots + z_n} = \overline{z_1} + \dots + \overline{z_n}$$

<u>Proof</u> <u>when $n=2$</u>

$$\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$$

Put $z_1 = a_1 + b_1 i$ $\quad z_2 = a_2 + b_2 i$

Then $z_1 + z_2 = (a_1 + a_2) + (b_1 + b_2) i$

$\therefore \overline{z_1 + z_2} = (a_1 + a_2) - (b_1 + b_2) i$

$\overline{z_1} + \overline{z_2} = (a_1 - b_1 i) + (a_2 - b_2 i)$

$= (a_1 + a_2) - (b_1 + b_2) i$

using the result for $n=2$

$\therefore \overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}.$

IH. Assume result true for n. Prove for $n+1$

$$\overline{(z_1 + \dots + z_n + z_{n+1})} = \overline{(z_1 + \dots + z_n) + z_{n+1}}$$

$$= \overline{(z_1 + \dots + z_n)} + \overline{z_{n+1}}$$

IH used here.

$$= (\overline{z}_1 + \dots + \overline{z}_n) + \overline{z}_{n+1} \qquad \boxed{P}$$

$$\overline{(z_1 \dots z_n)} = \overline{z}_1 \dots \overline{z}_n$$

is proved in a similar way.

You can find out more about proof by induction in Section 3.8 of my book.