

Lecture 29

Proof by induction

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

Well-ordering principle

Each 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

such that

$$(1) 0 \in X.$$

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

Then $X = \mathbb{N}$.

Proof Suppose that $\mathbb{N} \neq X$. Then

$\mathbb{N} \setminus X \neq \emptyset$. By the well ordering principle it has a smallest element ($\neq 0$) m .

But then $m-1 \in X$ which implies $m \in X$, giving a contradiction. It follows that $X = \mathbb{N}$, as claimed. $\square$

Application We want to prove infinitely many statements

$S_0, S_1, S_2, \dots$

Let $X \subseteq \mathbb{N}$ be def'd as follows:

$i \in X \Leftrightarrow S_i$ 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 $S_0, S_1, S_2, \dots$
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. Then prove that S_{n+1} is true.

We now give some examples of proof by
induction that help sharpen your use of the results.

By means of the same arguments,
the induction principle can be extended:

$$\text{def } \mathbb{N}^{\geq m} = \{m, m+1, \dots\}$$

Then if $X \subseteq \mathbb{N}^{\geq m}$ and

$$(1) m \in X \quad \text{and} \quad (2) n \in X \Rightarrow n+1 \in X$$

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

De Moivre's theorem

$$(\cos \theta + i \sin \theta)^n = \cos n\theta + i \sin n\theta \quad (n \in \mathbb{Z})$$

Proof when $n \geq 1$ clearly true.

Assume result holds for n we prove it holds for $n+1$.

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

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

by assumption.

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

properties of
complex multiplication

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

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

Proof clearly true when degree $= 1$.

same result holds for poly of degree n

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

If $f(x)$ has no roots then result is clearly true.

Else $f(x)$ has a root a_1 .

$$\text{Then } f(x) = (x - a_1) g(x)$$

where $g(x)$ is a poly of degree n .

So by assumption, $g(x)$ has at most n roots

It follows that $f(x)$ has at most $n+1$ roots. $\square$