Lecture 28 | 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 $X = \mathbb{N}$.

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

<u>Application</u> We want to prove infinitely many statements

$$S_0, S_1, S_2, \ldots\ldots$$

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

$$i \in X \iff S_i \text{ is true.}$$

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) <u>Base case</u> Prove that S_0 is true.

(2) <u>IH (induction hypothesis)</u> 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 up the use of our [illegible].

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

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

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

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

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

De Moivre's theorem

$$(\cos\theta + i\sin\theta)^n = \cos n\theta + i\sin n\theta \qquad (n \geq 1)$$

Proof When $n = 1$ clearly true.

Suppose 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

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

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

Proof Clearly true when degree $= 1$.

Suppose result holds for polys 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.

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. ∎

Other results in the course can be proved in the same way

$$\sqrt{2} \notin \mathbb{Q} \quad (\therefore \sqrt{2} \in \mathbb{R} \setminus \mathbb{Q})$$

That is, $\sqrt{2}$ is irrational.

To prove this result, we need the following lemma.

A iff B means '$A \Rightarrow B$' and '$B \Rightarrow A$'

<u>Lemma</u> Let $x \in \mathbb{N}$. Then

(i) x is even if and only if x^2 is even.

(ii) x is odd if and only if x^2 is odd.

<u>Even</u> means that $2 | x$ ('2 divides x')

<u>odd</u> means that $x = 2m+1$ for some $m \in \mathbb{N}$.

The proof of this lemma is straightforward.

See Chapter 2 of my book.

7 号 事

__Application__ $\mathbb{R} \setminus \mathbb{Q} \neq \emptyset$.

We prove, concretely, that $\sqrt{2} \in \mathbb{R} \setminus \mathbb{Q}$.

We use a technique called __proof by contradiction__.

If $a \in \mathbb{Q}$ then a is called __rational__

If $a \in \mathbb{R} \setminus \mathbb{Q}$ then a is called irrational = in-rational

= not-rational.

Either a is rational or a is irrational.

We show that a is rational is impossible.

This demonstrates that a is irrational.

Suppose that $\sqrt{2}$ is rational.

Then $\sqrt{2} = \frac{a}{b}$ where $a, b \in \mathbb{N}$.

Can ensure that a and b have no common divisor (why?) (*)

squaring both sides of above equation and rearranging

we get $2b^2 = a^2$.

Thus a^2 is even.

So, a is even. We can therefore write $a = 2x$

for some x. Thus $2b^2 = (2x)^2$ so

$b^2 = 2x^2$. Thus b^2 is even and so b is even.

It follows that a and b are both even contradicting (*)