cse 16 7-30-20

continue proof ...

Proof of (ii)

Suppose $e|a$ and $e|b$. By a previous lemma e divides any integer comb. of a and b. Thus

$$e \mid (an+bm) = d$$

$$\therefore e \le d,$$

Proving (ii) ∎

chapter 10 : Mathematical Induction

Ex. observe

$$1 = 1^2$$
$$1+3 = 2^2$$
$$1+3+5 = 3^2$$
$$1+3+5+7 = 4^2$$
$$\vdots$$

evidently

$$1+3+5+\cdots+(2n-1) = n^2$$

or

$$\sum_{k=1}^{n} (2k-1) = n^2$$

Any case can be verified. How to Prove all cases.

$$\forall n \in \mathbb{N} : \sum_{k=1}^{n} (2k-1) = n^2$$

Let $P(n)$ be a propositional function with universe $\mathbb{N}$. Suppose we wish to prove

$$(*) \qquad \forall n \in \mathbb{N} : P(n)$$

or

$$\forall n \geq 1 : P(n)$$

i.e. show $P(n)$ is true for all $n \in \mathbb{N}$.

A proof of $*$ by mathematical induction proceed in 2 steps.

I. Base.
Prove $P(1)$ is true.

II. Induction
Prove: $\forall n \geq 1 : P(n) \Rightarrow P(n+1)$
let $n \geq 1$ be an arbitrary positive integer, Assume $P(n)$ is true, then show as a consequence that $P(n+1)$ is also true.

Once steps I and II are complete, conclude (*) is true.

The ~~start~~ sentence $P(n)$ is called the <u>induction hypothesis</u>, since it's assumed true on induction step.

<u>Rmk</u>

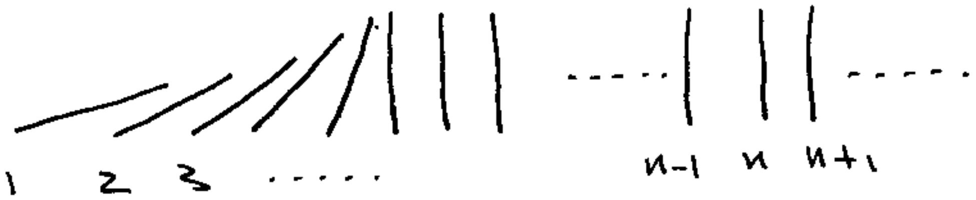
- Some persons believe Assuming $P(n)$ is true is <u>circular reasoning</u> (i.e. assuming within a proof, the conclusion you wish to prove, which is invalid.) In fact we don't assume (*). Instead we assume $P(n)$ for just <u>one</u> n.

- Imagine a "Proof" as follows

	<u>why?</u>
$P(1)$	I.
$P(1) \Rightarrow P(2)$	II. in case $n=1$
$P(2)$	Modus Ponens
$P(2) \Rightarrow P(3)$	II. $n=2$
$P(3)$	M.P.
$P(3) \Rightarrow P(4)$	II. $n=3$
$P(4)$	M.P.
$\vdots$	

But a proof is supposed to be finite.

- Domino Analogy



$P(n) =$ "the n^{th} domino falls"

Goal: Prove

$$\forall n \geq 1 : P(n)$$

i.e. "all dominos fall"

To prove this we do

I. $P(1)$ = "the 1st domino falls"

II. $\forall n \geq 1 : P(n) \Rightarrow P(n+1)$

= "if any domino falls, then the next domino falls"

The validity of this method is based on the following

<u>Theorem</u> (Principle of mathematical induction) For any propositional function $P(n)$ with universe $\mathbb{N}$, the following is true

$$\left[P(1) \wedge \forall n \left(P(n) \Rightarrow P(n+1)\right)\right] \Rightarrow \forall n : P(n)$$

This follows by W.O.P. of $\mathbb{N}$. Proof later.

Ex. $\forall n \geq 1$ $\boxed{\sum_{k=1}^{n} (2k-1) = n^2} \leftarrow P(n)$

Proof.

I. $P(1)$ is $\sum_{k=1}^{1} (2k-1) = 1^2$, i.e. $2 \cdot 1 - 1 = 1 \cdot 1$

i.e. $1 = 1$, which is true.

II. $\forall n \geq 1 : P(n) \Rightarrow P(n+1)$

Let $n \geq 1$ be chosen arbitrarily. Assume for this n that

$$\sum_{k=1}^{n} (2k-1) = n^2 .$$ (induction hypothesis)

we must show that

$$\sum_{k=1}^{n+1} (2k-1) = (n+1)^2 .$$ (induction conclusion)

> 0

$$\sum_{k=1}^{n+1}(2k-1) = \left(\sum_{k=1}^{n}(2k-1)\right) + \left(2(n+1)-1\right)$$

$$= n^2 + (2n+1) \quad \left\{\begin{array}{l}\text{by the}\\ \text{induction hypothesis}\end{array}\right.$$

$$= (n^2+2n+1)$$

$$= (n+1)^2,$$

as required.

By the P.M.I., we conclude

$$\forall n \geq 1 : \sum_{k=1}^{n}(2k-1) = n^2 . \qquad \blacksquare$$

Ex. let $x \in \mathbb{R}$, $x \neq 1$. show

$$\forall n \geq 1 : \boxed{\sum_{k=0}^{n-1} x^k = \frac{x^n - 1}{x - 1}} \leftarrow P(n)$$

Proof.

I. $P(1)$ says $\sum_{k=0}^{1-1} x^k = \frac{x^1 - 1}{x - 1}$, i.e.

$x^0 = \frac{x-1}{x-1}$, i.e. $1 = 1$, which is true.

II. $\forall n \geq 1 : P(n) \Rightarrow P(n+1)$

Let $n \geq 1$ be arbitrary. Assume

$$\sum_{k=0}^{n-1} x^k = \frac{x^n - 1}{x - 1} \quad \text{(ind. hyp.)}$$

we must show

$$\sum_{k=0}^{n} x^k = \frac{x^{n+1} - 1}{x - 1} \quad \text{(ind. concl.)}$$

observe

$$\sum_{k=0}^{n} x^k = \left(\sum_{k=0}^{n-1} x^k\right) + x^n$$

$$= \left(\frac{x^n - 1}{x-1}\right) + x^n \quad \left\{ \text{by the ind. hyp.} \right.$$

$$= \frac{x^n - 1}{x-1} + \frac{x^n(x-1)}{x-1}$$

$$= \frac{\cancel{x^n} - 1 + x^{n+1} - \cancel{x^n}}{x-1}$$

$$= \frac{x^{n+1} - 1}{x-1},$$

as required.

Result follows by P.M.I. ∎

Remarks

- always state ind. hyp. explicitely, i.e. don't write "assume P(n)"
- always state ind. conclusion ('must show') explicitely
- always state the point(s) in the proof where the ind. hyp. is used.

Ex. $\forall n \geq 1 : \boxed{\sum_{k=1}^{n} k = \frac{n(n+1)}{2}} \leftarrow P(n)$

Proof.

I. $P(1)$ is $\sum_{k=1}^{1} k = \frac{1(1+1)}{2}$, i.e. $1 = \frac{1 \cdot 2}{2}$,

i.e. $1 = 1$, which is true.

II. $\forall n \geq 1 : P(n) \Rightarrow P(n+1)$

Let $n \geq 1$. Assume

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2}. \qquad \text{(ind. hyp.)}$$

we must show

$$\sum_{k=1}^{n+1} k = \frac{(n+1)(n+2)}{2} \qquad \text{(ind. concl.)}$$

so

$$\begin{aligned}
\sum_{k=1}^{n+1} k &= \left(\sum_{k=1}^{n} k\right) + (n+1) \\
&= \frac{n(n+1)}{2} + (n+1) \qquad \left\{ \begin{array}{l} \text{by the} \\ \text{ind. hyp.} \end{array} \right. \\
&= \frac{n(n+1) + 2(n+1)}{2} \\
&= \frac{(n+1)(n+2)}{2},
\end{aligned}$$

as required.

Result follows by P.M.I. ∎

Exercises

- $\forall n \geq 1 : \displaystyle\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$

- $\forall n \geq 1 : \displaystyle\sum_{k=1}^{n} k^3 = \left(\frac{n(n+1)}{2}\right)^2$