MAT200: Logic Language and Proof

Lecture 8 - March 1 2021

Recall:

Recently: induction/recursion

Today: Sets

HW3 Problem 3

Let P(n) denote 5q.

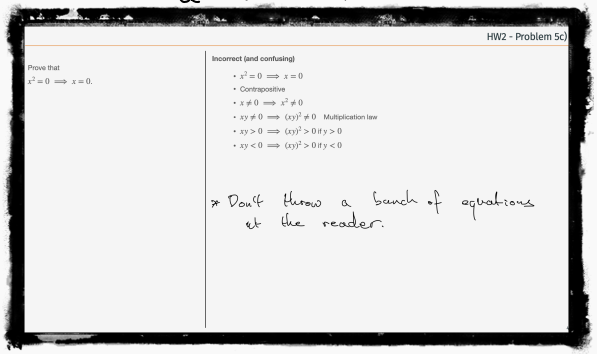
Let P(n) be the following statement:

P(n): "n is divisible by 5".

Prove that $P(n) \implies P(n+5)$

1) You shouldn't need to use induction to prove this.

2) You can't treat P(n) as a number.



3) Clarity.

Bad "proof"

$P(n) = n = 5q, \quad n = 5q$, where q is integer

$P(q) = \frac{5q}{q}$

$P(1) = \frac{5(1)}{5} = 1$

$P(n) \implies P(n+5)$

$\frac{n+5}{5} = P(n+5)$

$\frac{5q+5}{5} = P(n+5)$ distributivity

$\frac{5(q+1)}{5} = P(n+5)$

$q+1 = P(n+5)$ True

$P(n+5)$ is shown above and it's true

Still confusing.

1) P(n) is already defined.

2)

Meaningless

P(n) = 5q

P(n): statement. 5q: number.

P(n) = { }: set

WRONG.

Let n = 5q.

Better: Let q satisfy n = 5q.

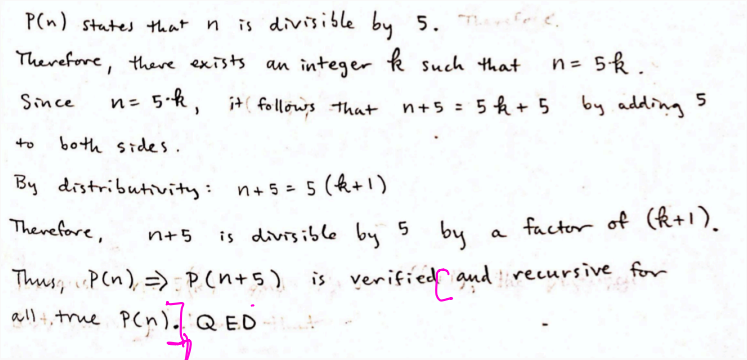
HW3 Problem 3

Let P(n) be the following statement:

P(n): “n is divisible by 5”.

Prove that $P(n) \implies P(n+1)$

Good proof:



1) You shouldn't need to use induction to prove this.

HW3 Problem 3

Let P(n) be the following statement:

P(n): “n is divisible by 5”.

Prove that $P(n) \implies P(n+1)$

Chains of equalities are ok,
if each step is very small, or you explain each step.

Problem 1 (10 points)

Prove that for all positive integers n,

$$\sum_{i=1}^{n} i^2 = \frac{1}{6}n(n+1)(2n+1).$$

Base case: For $n=1$, $\sum_{i=1}^{n} i^2 = 1$ and $\frac{1}{6}n(n+1)(2n+1) = \frac{1}{6}\times 2\times 3 = 1$
and therefore $\sum_{i=1}^{n} i^2 = \frac{1}{6}n(n+1)(2n+1)$.

Inductive step: Suppose now our inductive hypothesis that when $n=k$,
$\sum_{i=1}^{k} i^2 = \frac{1}{6}k(k+1)(2k+1)$ for some postive integer k.

Then when $n=k+1$,

$$\sum_{i=1}^{k+1} i^2 = \sum_{i=1}^{k} i^2 + (k+1)^2 \quad \text{(by definition)}$$
$$= \frac{1}{6}k(k+1)(2k+1) + (k+1)^2 \quad \text{(by inductive hypothesis)}$$
$$= \frac{k(k+1)(2k+1) + 6(k+1)^2}{6}$$
$$= \frac{(k+1)(2k^2+k+6k+6)}{6} \quad \text{(by distributivity)}$$
$$= \frac{(k+1)(k+2)(2k+3)}{6}$$
$$= \frac{(k+1)[(k+1)+1][2(k+1)+1]}{6} \quad \text{(by distributivity and associativity)}$$
$$= \frac{1}{6}(k+1)[(k+1)+1][2(k+1)+1]$$

and so we prove $\sum_{i=1}^{k+1} i^2 = \frac{1}{6}(k+1)[(k+1)+1][2(k+1)+1]$.

Conclusion: hence, by introduction, $\sum_{i=1}^{n} i^2 = \frac{1}{6}n(n+1)(2n+1)$ for all postive integers n.

QED

HW3 Problem 6

Consider the following statement, P.

All people have the same surname.

Or, more formally,

if X is any finite set of people then each person in X has the same surname as every person in X.

The result is clearly false. So the proof must be flawed. What is the flaw?

Proof: We use induction on n, the number of people in X.
Base Case: Clearly, in any group of one people, all people have the same surname. Thus $P(1)$ is true.
Inductive Step: Suppose that $P(k)$ is true for some integer k, that is, in any group of k people, all people have the same surname (inductive hypothesis). We have to prove that $P(k+1)$ is true. To do this, consider a group of $k+1$ people.

First, exclude the last person and consider only the first k people. Then all these people have the same surname, by the induction hypothesis. Likewise, exclude the first person and consider only the last k people. Then these too must have the same surname. Therefore, the first person in the group is of the same surname as the people in the middle, who in turn are of the same surname as the last person. Hence everyone in the group is of the same surname.

This shows that $P(k+1)$ is true.

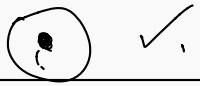
Conclusion: Therefore, by the induction principle, $P(n)$ is true for all integers $n \geq 1$. In other words, in any group of n people, all people have the same surname.

no middle for $k=1$.

$P(n)$: "For every set X of n people, all the people in X have the same surname".

Base Case

$P(1)$: "For every set X of 1 people, all the people in X have the same surname".



✓

Inductive Step: $P(k) \Rightarrow P(k+1)$.

Suppose $P(k)$ is true.

"For every set X of k people, all the people in X have the same surname".

The proof of $P(k) \Rightarrow P(k+1)$ is correct when $k \geq 2$.

But it is incorrect for $k=1$.

$P(1) \not\Rightarrow P(2)$.

Summary

- $P(1)$ is true
- The proof of $P(k) \Rightarrow P(k+1)$ is correct when $k \geq 2$.
- $P(1) \not\Rightarrow P(2)$.

HW3 Problem 6

Consider the following statement, P.

All people have the same surname.

Or, more formally,

if X is any finite set of people then each person in X has the same surname as every person in X.

The result is clearly false. So the proof must be flawed. What is the flaw?

Proof: We use induction on n, the number of people in X.
Base Case: Clearly, in any group of one people, all people have the same surname. Thus $P(1)$ is true.
Inductive Step: Suppose that $P(k)$ is true for some integer k, that is, in any group of k people, all people have the same surname (inductive hypothesis). We have to prove that $P(k+1)$ is true. To do this, consider a group of $k+1$ people.

First, exclude the last person and consider only the first k people. Then all these people have the same surname, by the induction hypothesis. Likewise, exclude the first person and consider only the last k people. Then these too must have the same surname. Therefore, the first person in the group is of the same surname as the people in the middle, who in turn are of the same surname as the last person. Hence everyone in the group is of the same surname.

This shows that $P(k+1)$ is true.

Conclusion: Therefore, by the induction principle, $P(n)$ is true for all integers $n \geq 1$. In other words, in any group of n people, all people have the same surname.

$\in$ $\subset$

"in" ↑ subset.

- $A \cup B = \{x : x \in A \text{ or } x \in B\}$
- $A \cap B = \{x : x \in A \text{ and } x \in B\}$
- $\emptyset = \{\}$ Empty set
- $\mathcal{P}(A) = \{X : X \subset A\}$ Power set
- $A \times B = \{(a, b) : a \in A \text{ and } b \in B\}$ Product.
- $A - B = \{x : x \in A \text{ and } x \notin B\}$ Difference
- $A^c = U - A$ Complement.

↑ "Everything not in A".

E.g. $A = \{1, 2, 3\}$.
$A^c = \{\$, 4, \pi, \text{Jupiter}, \text{MAT2001}, \ldots\}$.

E.g. $\mathcal{P}(\{0,1\}) = \{\emptyset, \{1\}, \{0\}, \{0,1\}\}$

Warning: $0 \notin \mathcal{P}(\{0,1\})$

Because 0 is not a subset of $\{0,1\}$.

i.e. "$0 \subset \{0,1\}$" is meaningless.

(number, set)

(But "$0 \in \{0,1\}$" works,

(number, set)

$\emptyset \subset \{0,1\}$.

Proof:

$x \in \emptyset \Rightarrow x \in \{0,1\}$

F

$A = \{1, 0\}$ $B = \{2, 3, 0\}$.

$A \times B = \{(1,2), (1,3), (1,0), (0,2), (0,3), (0,0)\}$

$\emptyset \in \{1,2\}$. F

$\emptyset \in \{\emptyset, 1, 2\}$. T

However $\emptyset \in \mathcal{P}(\{1,2\})$ T.

$\emptyset \subset \{1,2\}$ T

- $A \cup B = \{x : x \in A \text{ or } x \in B\}$
- $A \cap B = \{x : x \in A \text{ and } x \in B\}$
- $\varnothing = \{\}$
- $\mathscr{P}(A) = \{X : X \subset A\}$
- $A \times B = \{(a, b) : a \in A \text{ and } b \in B\}$
- $A - B = \{x : x \in A \text{ and } x \notin B\}$
- $A^c = U - A$

- $A \cup B = \{x : x \in A \text{ or } x \in B\}$
- $A \cap B = \{x : x \in A \text{ and } x \in B\}$
- $\emptyset = \{\}$
- $\mathcal{P}(A) = \{X : X \subset A\}$
- $A \times B = \{(a, b) : a \in A \text{ and } b \in B\}$
- $A - B = \{x : x \in A \text{ and } x \notin B\}$
- $A^c = U - A$

* Let $P(n)$ = "n is divis by 5"

$P(n)$ = 5q.

statement number

* "$0 \subset \{0,1\}$"

number set

* $\{1,2,3\} \times 5$

set number.

* $5 \in 5$

number number.

$\phi = \{\}$ T

But

$\{\} \neq \{\phi\}$. F

$\{\phi\} = \{\{\}\}$. T

$\{\phi\}$ has 1 element. T

1) Find relevant defs.

Theorem: $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

Proof:

We have:

$$
\begin{aligned}
A \cap (B \cup C) &= \{x : x \in A \text{ and } x \in (B \cup C)\} && \text{by definition of } \cap \\
&= \{x : x \in A \text{ and } (x \in B \text{ or } x \in C)\} && \text{by def'n of } \cup \\
&= \{x : (x \in A \text{ and } x \in B) \text{ or } (x \in A \text{ and } x \in C)\} && \text{because. } P \text{ and } (Q \text{ or } R) \equiv (P \text{ and } Q) \text{ or } (P \text{ and } R) \\
&= \{x : (x \in A \cap B) \text{ or } (x \in A \cap C)\} && \text{by definition of } \cap \\
&= (A \cap B) \cup (A \cap C). && \text{by definition of } \cup.
\end{aligned}
$$

distributativity of logical statements.

No venn diagrams.
No truth tables.

- $A \cup B = \{x : x \in A \text{ or } x \in B\}$
- $A \cap B = \{x : x \in A \text{ and } x \in B\}$
- $\varnothing = \{\}$
- $\mathcal{P}(A) = \{X : X \subset A\}$
- $A \times B = \{(a, b) : a \in A \text{ and } b \in B\}$
- $A - B = \{x : x \in A \text{ and } x \notin B\}$
- $A^c = U - A$

Theorem: $(A \subset B) \iff (A \cup B = B)$

Proof:

($\Rightarrow$) Suppose $A \subset B$

Then $x \in A \Rightarrow x \in B$. (*)

We want to show $A \cup B = B$,

i.e. $(x \in A$ or $x \in B) \iff x \in B$.

i.e. $\begin{cases} (x \in A \text{ or } x \in B) \Rightarrow x \in B & (1) \\ \text{and} \\ x \in B \Rightarrow (x \in A \text{ or } x \in B) & (2) \end{cases}$

For (1),

if $x \in A$ then $x \in B$ by assumption (*)

if $x \in B$ then $x \in B$ trivially.

(2) is true tautologically.

Thus we have shown $A \cup B = B$

So $A \subset B \Rightarrow A \cup B = B$.

Rough work:

Given	Want
$A \subset B$.	$A \cup B = B$
$(x \in A \Rightarrow x \in B.)$	$x \in A \cup B \iff x \in B.$
	$x \in A$ or $x \in B \iff x \in B$
	$\begin{cases} x \in A \text{ or } x \in B \Rightarrow x \in B \\ \text{and} \\ x \in B \Rightarrow x \in A \text{ or } x \in B \end{cases}$
	Trivial.

Which definitions?

- $A = B$ means $x \in A \iff x \in B$
- $A \subset B$ means $x \in A \implies x \in B$
- $A \cup B = \{x : x \in A \text{ or } x \in B\}$
- $A \cap B = \{x : x \in A \text{ and } x \in B\}$
- $\emptyset = \{\}$
- $\mathcal{P}(A) = \{X : X \subset A\}$
- $A \times B = \{(a, b) : a \in A \text{ and } b \in B\}$
- $A - B = \{x : x \in A \text{ and } x \notin B\}$
- $A^c = U - A$

(Still have to do $\Leftarrow$).