Module 7

Methods of Proof: Direct General

Rule of Universal Specification

If an open statement is true for all possible replacements in the designated universe, then that open statement is true for each specific individual member in that universe.

If ∀x p(x) is true, then we know that p(a) is true, for each a in the universe for x.

$\forall x, p(x)$ is true
a in the universe of x, $P(a)$ is true

Rule of Universal Generalization

Universal generalization is the rule of inference that states that ∀xP(x) is true, given the premise that P(c) is true for all elements c in the domain. Universal generalization is used when we show that ∀xP(x) is true by taking an arbitrary element c from the domain and showing that P(c) is true. The element c that we select must be an arbitrary, and not a specific, element of the domain.

Direct Proof (General)

If Proof is of the form : P : "if p then q"
then direct general proof is appropriate.

$a \in \mathbb{Z}$

even integer : $2a$
odd integer : $2a+1$ or $2a-1$

$\mathbb{Z} = \{\ldots, -4, -3, -2, -1, 0, 1, 2, 3 \ldots\}$

$\mathbb{Z}_o = \{\ldots, -5, -3, -1, 1, 3, 5, \ldots\}$

odd

$\mathbb{Z}_E = \{\ldots, -4, -2, 0, 2, 4, \ldots\}$

$a \in \mathbb{Z}$ (a is an arbitrary element)

Ex 1: Prove the Theorem: Every odd integer is the difference of two perfect squares.

If there exists an odd integer, then its equal to difference of two perfect squares.

Ex: $9 = 25-16 = 5^2-4^2$

$-5 = 4-9 = 2^2-5^2$

$-5 = 2a+1$ $\quad a = \frac{-5-1}{2}$

$a = -3$ $\quad a^2 = 9$

$(a+1)^2 = (-3+1)^2 = 4$

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

$\mathbb{P}$: $\forall n \in \mathbb{Z}$, If $n \in \mathbb{Z}_o$ then $\exists s,t \in \mathbb{Z}$, such that $n = s^2 - t^2$

$$\forall n \in \mathbb{Z}, n \in \mathbb{Z}_o \longrightarrow \exists s,t \in \mathbb{Z}, \text{ such that } n = s^2 - t^2$$

Proof:

(i) Let $a \in \mathbb{Z}$ $\qquad$ defination

(ii) Let $n = 2a+1$ $\qquad$ defination of odd

(iii) $n = \underline{a^2+2a+1} - a^2$ $\qquad$ algebra (factoring)

(iv) $n = (a+1)^2 - a^2$ $\qquad$ $s = a+1 \quad t = a$

(v) $n = s^2 - a^2$

$\boxed{\therefore \text{ steps i–v show that } \mathbb{P} \text{ is valid/true}}$

<u>Ex 2</u>: $\mathbb{P}$: $\forall \mathbf{m}, \mathbf{n} \in \mathbb{Z}_o$, $m + n \in \mathbb{Z}_E$

$-1 + 9 = 8$

$5 + 3 = 8$

$17 + 1 = 18$

Proof:

(i) Let $a, b \in \mathbb{Z}$ — defination

(ii) Let $m = 2a+1$ — defination of odd.

(iii) Let $n = 2b+1$ — defn of odd.

(iv) $m+n = 2a+1+2b+1$ — algebra

(v) $m+n = 2a+2b+2$ — algebra

(vi) $m+n = 2(a+b+1)$ — defination of even

$\therefore$ Steps (i)-(vi) show that $\mathbb{P}$ is true.

"a divides b"

Definition: Divisibility

$a \mid b$ iff $b/a \in \mathbb{Z}$

$a \nmid b$ iff $b/a \notin \mathbb{Z}$

Ex: $6/3 = 2 \in \mathbb{Z}$ $\Rightarrow c \in \mathbb{Z}$, $b = ca$.

$5/5 = 1 \in \mathbb{Z}$

$5/2 = 2.5 \notin \mathbb{Z}$ $\Rightarrow c \notin \mathbb{Z}$, $b = ca$.

$10/3 = 3.3 \notin \mathbb{Z}$

Ex 3: $\mathbb{P}$: $\forall a, b \in \mathbb{Z}$ **and** $a \neq \pm 1$, $a|b \rightarrow a \nmid b+1$

Proof:

(i) $a \mid b$ — given / premise

(ii) Let $c \in \mathbb{Z}$ — define

(iii) $b = ca$ — defination of $a \mid b$

(iv) $b+1 = ca+1$ — algebra

(v) $b+1 = a(c + 1/a)$ — algebra / factoring.

(vi) $c + 1/a \notin \mathbb{Z}$, $a \nmid b$ — defination of $a \nmid b$

$\therefore$ Steps (i)-(vi) proove $\mathbb{P}$ is valid.

Ex 4: $\mathbb{P}$: $\forall \mathbf{m} \in \mathbb{Z}$, $\mathbf{4|m \rightarrow 2|m}$

$\circledast$

Proof:

(i) $4 | m$ — Premise | given

(ii) Let $c \in \mathbb{Z}$ — define

(iii) $m = 4c$ — defination of $a|b$

(iv) $m = 2(2c)$ — factoring.

(v) $2c \in \mathbb{Z}$, so $2|m$ — defination of $a|b$

$\boxed{\therefore \text{ Steps (i) - (v) Show } \mathbb{P} \text{ is true.}}$

(For Fun)

Ex 5: (Extra Problem) $\mathbb{P}$: $2 = 1$ $\not\ast$ False

what is a? what is x?

(i) Let $a = x$

explanations?

(ii) $a + a = x + a$

(iii) $2a = x + a$

(iv) $2a - 2x = x + a - 2x$

(v) $2(a - x) = a - x$

dividing by zero??

(vi) $2 = 1$???