ch. 4 : Direct Proof

To Prove $P \Rightarrow Q$

- Assume P is true
- show as a consequence that Q is also true

  use: - laws of logic
  - previously proved facts
  - definitions
  - axioms
- conclude that $P \Rightarrow Q$ is true.

Defn

let $a, b \in \mathbb{Z}$. we say that a divides b iff there exists $k \in \mathbb{Z}$ such that

$$b = ak$$

notation: $a \mid b$ "a divides b"

Also say: "a is a divisor of b"

"b is a multiple of a"

"a is a factor of b"

Rmk: we did not define $a|b$ to mean

$$\frac{b}{a} \in \mathbb{Z}$$

even though this is equivalent.

Theorem

For all $a, b, c \in \mathbb{Z}$, if $a \mid b$ and $b \mid c$, then $a \mid c$.

Proof:

Let $a, b, c \in \mathbb{Z}$. Assume $a \mid b$ and $b \mid c$. Then

$$a \mid b \Rightarrow b = k_1 a \quad \text{for some } k_1 \in \mathbb{Z}$$

and

$$b \mid c \Rightarrow c = k_2 b \quad \text{'' \quad ''} \quad k_2 \in \mathbb{Z}.$$

Therefore $c = k_2 b = k_2(k_1 a) = (k_2 k_1) a$.

Since $k_2 k_1 \in \mathbb{Z}$, we have that

$$a \mid c.$$

$\blacksquare$

Note:

we used some facts from algebra

- equals can be substituted for equals
- associative law for $\mathbb{Z}$: $k_1(k_2a) = (k_1k_2)a$
- closure of $\mathbb{Z}$ under multiplication:

$$k_1, k_2 \in \mathbb{Z} \Rightarrow k_1k_2 \in \mathbb{Z}.$$

Recall: (Axiom)

well ordering Property of $\mathbb{N} = \{0, 1, \dots\}$:

Every non-empty subset of $\mathbb{N}$ contains a least element.

Theorem (division algorithm)

for any $a, b \in \mathbb{Z}$ with $b > 0$, there exist unique $q, r \in \mathbb{Z}$ such that

$$a = qb + r \quad \text{and} \quad 0 \le r < b$$

we used W.O.P. to prove

(1) existence of $q, r \in \mathbb{Z}$.

left as exercise

(2) uniqueness of $q, r \in \mathbb{Z}$.

<u>Proof of (2) uniqueness:</u>

Assume

$$a = q_1 b + r_1 \quad \text{and} \quad 0 \le r_1 < b$$

and

$$a = q_2 b + r_2 \quad \text{and} \quad 0 \le r_2 < b$$

we must show that

$$r_1 = r_2$$

and $$q_1 = q_2.$$

these two equations imply

$$q_1 b + r_1 = q_2 b + r_2$$

$$\therefore \quad (q_1 - q_2) b = (r_2 - r_1)$$

If $r_1 < r_2$, then $0 \leq r_1 < r_2 < b$, hence

$$0 < (r_2 - r_1) < b$$

$$\therefore \quad 0 < (q_1 - q_2) b < b$$

i.e. $(q_1 - q_2) b$ is a positive multiple of b less than b, which is impossible.

$\therefore$ $r_1 \not< r_2$ $\therefore$ $r_1 \geq r_2$.

A similar argument shows $r_2 \geq r_1$, whence $r_1 = r_2$.

$\therefore \quad (q_1 - q_2) b = r_2 - r_1 = 0$

$\therefore \quad q_1 - q_2 = 0 \quad$ (since $b > 0$)

$\therefore \quad q_1 = q_2$

$\blacksquare$

<u>Ex.</u>

for any $n \in \mathbb{Z}$, there exist unique k and r such that

$$n = 2k + r \quad \text{and} \quad 0 \leq r < 2 .$$

Thus $r = 0$ or $r = 1$. Thus every integer is of one of the two forms:

- $n = 2k$ (called <u>even</u>)

or

- $n = 2k + 1$ (called <u>odd</u>)

<u>note</u>: uniqueness says no integer is <u>both</u> even and odd.

let

$$E = \{2k \mid k \in \mathbb{Z}\}$$

$$O = \{2k+1 \mid k \in \mathbb{Z}\}.$$

we have $E \cap O = \emptyset$ (uniqueness)

and $E \cup O = \mathbb{Z}$ (existence).

$\therefore$ E, O form a partition of $\mathbb{Z}$.

<u>Ex</u> take $b = 3$ in division algorithm. we get a Partition of $\mathbb{Z}$ into 3 sets

$$\{3k \mid k \in \mathbb{Z}\} = [0]_3$$

$$\{3k+1 \mid k \in \mathbb{Z}\} = [1]_3$$

$$\{3k+2 \mid k \in \mathbb{Z}\} = [2]_3$$

<u>Rmk</u> we can replace 2, 3 by any positive integer m.

<u>Defn</u>

Two integers a, b are said to have <u>same parity</u> iff they have same remainder on div. by 2.

We can define an arithmetic on the parities {Even, Odd}

a	b	+	×
E	E	E	E
E	O	O	E
O	E	O	E
O	O	E	O

Exercise

show this arithmetic is consistent

For instance, suppose $a \in O$ and $b \in E$. Then

$$a = 2k_1 + 1 \quad \text{and} \quad b = 2k_2$$

for some $k_1, k_2 \in \mathbb{Z}$. Thus

$$a + b = (2k_1 + 1) + 2k_2 = 2(k_1 + k_2) + 1 \in O$$
$$a \cdot b = (2k_1 + 1) \cdot 2k_2 = 2\left(k_2 \cdot (2k_1 + 1)\right) \in E$$

since $k_1 + k_2 \in \mathbb{Z}$ and $k_2(2k_1 + 1) \in \mathbb{Z}$.

note: all of this follows from uniqueness of Div. Alg.

Special Case:

<u>Theorem</u>

For any $n \in \mathbb{Z}$:

(1) if n is even, then n^2 is even

and

(2) if n is odd, then n^2 is odd.

Actually the converses are also true.

<u>Recall</u> an implication is equivalent to its contrapositive:

$$(P \Rightarrow Q) = (\sim Q \Rightarrow \sim P).$$