

$\forall$  : for all

$\exists$  : there exist

$\nexists$  : not for all

$\nexists$  : there not exist

$\in$  : in

$\subset$  : subset

$\Rightarrow$  : then (법칙)

$\rightarrow$  : if then (조건)

$\nless, \nless, \Rightarrow \Leftarrow$ , C.T.D : contradiction

■, Q.E.D, E.T.S : 증명끝

WLOG : Without Loss Of Generality

iff : if and only if

L.H.S : Left Hand Side

R.H.S : Right Hand Side

$\mathbb{N}$  : 자연수

$\mathbb{C}$  : 복소수

$\mathbb{Z}^+$  : 양의 정수

$\mathbb{Z}$  : 정수

$\mathbb{R} \setminus \mathbb{Q}$  : 무리수

$\mathbb{Z}^-$  : 음의 정수

$\mathbb{Q}$  : 유리수

$\mathbb{P}$  : 소수

$\mathbb{Z}^\oplus$  : 음이 아닌 정수

$\mathbb{R}$  : 실수

$\mathbb{C} \setminus \mathbb{R}$  : 허수

$\mathbb{Z}^\ominus$  : 양이 아닌 정수

$$\mathbb{Z}_p := \{x \in \mathbb{Z}^\oplus \mid x < p\}$$

$$\mathbb{Z}_p^\times := \{x \in \mathbb{Z}^+ \mid x < p \wedge \gcd(x, p) = 1\}$$

$$\text{operator mod} \langle a, b \rangle := r \in \mathbb{Z}_b \text{ s.t. } \exists b \text{ s.t. } a = b_f + r$$

p.H.p : pigeon Hole principle (비둘기집 원리)

M.I. : Mathematical Induction (수학적 귀납법)

B.C : By Contrast (귀류법)

Trivial : 자명하다

Group binary operator

$\langle G, \cdot \rangle$  is group if

- set  $\rightarrow$
1.  $\forall a, b \in G \Rightarrow a \cdot b \in G$  : Closed under  $\cdot$  (= Closed on  $\cdot$ )
  1.  $\forall a, b, c \in G \Rightarrow (a \cdot b) \cdot c = a \cdot (b \cdot c)$  : Associativity
  2.  $\exists e \in G$  s.t.  $\forall a \in G \Rightarrow a \cdot e = e \cdot a = a$  : Identity
  3.  $\forall a \in G \Rightarrow \exists a^{-1} \in G$  s.t.  $a \cdot a^{-1} = a^{-1} \cdot a = e$  : Inverse

Field

$\langle F, +, \cdot \rangle$  is field if

0.  $\forall a, b \in F \Rightarrow a + b \in F \wedge a \cdot b \in F$
1.  $\forall a, b \in F \Rightarrow a + b = b + a \wedge a \cdot b = b \cdot a$
2.  $\forall a, b, c \in F \Rightarrow (a + b) + c = a + (b + c) \wedge (a \cdot b) \cdot c = a \cdot (b \cdot c)$
3.  $\exists 0 \in F$  s.t.  $\forall a \in F \Rightarrow a + 0 = a$  (0: + 에서의 항등원을 의미하는 기호)
4.  $\exists 1 \in F$  s.t.  $\forall a \in F \Rightarrow a \cdot 1 = a$  (1:  $\cdot$  에서의 항등원을 의미하는 기호)
5.  $\forall a \in F \Rightarrow \exists -a \in F$  s.t.  $a + (-a) = 0$
6.  $\forall a \in F \setminus \{0\} \Rightarrow \exists a^{-1} \in F$  s.t.  $a \cdot a^{-1} = 1$
7.  $\forall a, b, c \in F \Rightarrow a \cdot (b + c) = a \cdot b + a \cdot c$