$(\mathbb{Z}, +)$ "additive" group - properties

a) closure $\forall x, y \mid (x \in \mathbb{Z}) \land (y \in \mathbb{Z}) \rightarrow (x + y \in \mathbb{Z})$ Operations in a set, stay in that set

b) associativity $\forall x, y, z \in \mathbb{Z} \mid (x+y) + z = x + (y+z)$

c) neutral There is an integer $0 \mid \forall x \in \mathbb{Z} \mid x + 0 = 0 + x = x$

d) invertibility $\forall x, y \in \mathbb{Z} \mid y = -x \rightarrow x + y = y + x = 0$

e) commutativity $\forall x, y \in \mathbb{Z} \mid x + y = y + x$

Theorem: Any operation has an <u>existing</u> and <u>unique</u> solution

$a + z = b$ has unique solution $z = b - a = (-a) + b$

proof:

a) "Existence": $a + \underbrace{((-a) + b)}_{z} = a - a + b = b$

b) "Uniqueness": given z_1 and z_2 from $\mathbb{Z}$,

assume: $a + z_1 = b$ & $a + z_2 = b$ $\Big\} z_1 = z_2 = b$
$-a$ $-a$

$(R^+, \times)$ "multiplicative" group

a) closure $\forall x, y \in R^+ \rightarrow x \cdot y \in R^+$

b) associativity $\forall x, y, z \in R^+ \mid (x \cdot y) \cdot z = x \cdot (y \cdot z)$

c) neutral There is a neutral 1, such that $\forall x \in R^+ \mid x \cdot 1 = 1 \cdot x = x$

d) invertibility $\forall x, y \in R^+ \mid y = x^{-1} \rightarrow x \cdot y = y \cdot x = 1$

e) commutativity $\forall x, y \in R^+ \mid x \cdot y = y \cdot x$

Theorem:

$\forall a, b \in R^+ \mid a \cdot z = b$ has unique solution $z = a^{-1} \cdot b$

proof:

a) Existence

b) Uniqueness there is a problem → many combination can lead to same result.