Subgroup

26 August 2020 09:16

$a * b = ab$

$\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$

$U(n) = \{a \mid 0 < a < n, \ gcd(a, n) = 1\}$

$\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$

$U(15) = \{1, 2, 4, 7, 8, 11, 13, 14\}$

$U(12) = \{1, 5, 7, 11\}$

GL

$GL(2, R) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix}, a, b, c, d \in R \mid ad - bc \neq 0 \right\}$

$Identity = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I_2$

$SL(2, R) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix}, a, b, c, d \in R \mid ad - bc = 1 \right\}$

$\mathbb{Z}_p^* = \{1, 2, 3, 4, \ldots, p-1\}$

$\{\mathbb{Z}_n, +_n\}$ group

$a +_n b = (a + b) \bmod n$

$\{Z_{11}, +_{11}\}$ group

$6 +_{11} 10 = 16 \pmod{11}$

$= 5$

$6 +_{11} 5 = 11 \pmod{11} = 0$.

$Z_{11} = \{0, 1, 2, 3, \ldots, 10\}$

$$a +_n b = \begin{cases} a+b, & \text{if } a+b \le n \\ a+b-n, & \text{if } a+b \ge n \end{cases}$$

Z

$\{Z_4, +_4\}$ is a group

$Z_4 = \{0, 1, 2, 3\}$

① Binary operation

$a +_4 b \in Z_4$ for all $a, b \in Z_4$

$0 +_4 0 = 0$, $0 +_4 1 = 1$,

$1 +_4 0 = 1$, $1 +_4 1 = 2$, $1 +_4 2 = 3$

$1 +_4 3 = 4 = 0 \in Z_4$.

$2 +_4 3 = 5 \pmod{4} = 1 \in Z_4$

② Associative

$(a +_4 b) +_4 c = a +_4 (b +_4 c)$

(3) Identity

.0.

④ Inverse

Inverse of $0 = 0 \in \mathbb{Z}_4$

Inverse of $1 = 3 \in \mathbb{Z}_4$

Inverse of $2 = 2 \in \mathbb{Z}_4$

Inverse of $3 = 1 \in \mathbb{Z}_4$

$\{\mathbb{Z}_4, +_4\}$ is a group.

$\{\mathbb{Z}_n, +_n\}$ is a group $\forall n$.

$\{\mathbb{Z}_p^*, \cdot_p\}$ is a group

$$a \cdot_p b = \begin{cases} ab, & \text{if } ab < p \\ ab - p, & \text{if } ab > p \end{cases}.$$

$a \cdot_p b = ab \pmod p$

p is a prime.

$\{\mathbb{Z}_5^*, \cdot_p\}$ is a group

① Binary operation $\mathbb{Z}_p^* = \{1, 2, 3, 4\}$

$2 \cdot_5 4 = 8 \pmod 5 = 3$

$4 \cdot_5 4 = 16 \pmod 5 = 1$

$3 \cdot_5 3 = 1$

$2 \cdot_5 3 = 1$ $\quad 4 \cdot 5\, 4 = 16 \pmod 5 = 1$

$4 \cdot_5 3 = 2.$ $\quad a \cdot_p b = ab \pmod p =$ remainder when ab divided by p.

② Associative

③ Identity $= 1$

④ Inverse

$b = a^{-1}$

$(1)^{-1} = 1, \ (2)^{-1} = 3$

$(3)^{-1} = 2, \ (4)^{-1} = 1. \in \mathbb{Z}_5^*$

$\therefore (\mathbb{Z}_5^*, \cdot_p)$ is a group.

Commutative group (or abelian group)

$(G, *)$ is an abelian group if G is a group and G is commutative under operation $*$.

or $*$ is commutative in G.

Examples -

① $(\mathbb{Z}, +)$ is an abelian group

② $(R^*, \cdot)$ is an abelian group

③ $(\mathbb{Z}_n, +_n)$ is an abelian group

④ $(\mathbb{Z}_p^*, \cdot_p)$ is an abelian group.

⑤ $GL(2, R) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid ad - bc \neq 0, \; a, b, c, d \in R \right\}$

is not an abelian group.

⑥ $SL(2, R)$ is not an abelian group.

$SL(2, R) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid ad - bc = 1, \; a, b, c, d \in R \right\}$