MA4070 - Elements of Groups and Rings

A binary operation $(\cdot)$ on a set S is a function

$\cdot : S \times S \to S$

Example

(i) $+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ (ii) $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$

Denote it by $(S, \cdot)$ to mean $\cdot$ is a binary operation on set S

(iii) $(M_{m \times n}(\mathbb{R}), +)$

Also, matrix multiplication is a binary operation

(iv) $M_n(\mathbb{R}) = M_{n \times n}(\mathbb{R})$

$(M_n(\mathbb{R}), +)$, $(M_n(\mathbb{R}), \cdot)$

(v)

$T = \text{Maps}(S, S) \to \{f : S \to S\}$

$T \times T \to T$

$(f, g) \mapsto g \circ f$

identity
$Id : S \to S$
$Id(s) = s, \forall s \in S$

Let S be a set and $\cdot : S \times S \to S$ be a binary operation on S

(i) It is associative if $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ $\forall$ $a, b, c \in S$

(Non - Example) : $(\mathbb{R}, -)$

(ii) It is commutative if $a \cdot b = b \cdot a$ $\forall$ $a, b \in S$

(iii) An element $e \in S$ is an identity element of the set S with respect to the binary operation $\cdot$ if $a \cdot e = e \cdot a = a$ $\forall$ $a \in S$

An element $a \in S$ is said to be invertible if $\exists$ $b \in S$ such that $ab = ba = e$

Proposition

If $\cdot$ is an associative binary operation on S, and $a, b \in S$ then

(i) $(ab)^{-1} = b^{-1}a^{-1}$

(ii) $(a^{-1})^{-1} = a$

Proof

(i) Consider $(ab)(b^{-1}a^{-1})$, because $(ab)(ab)^{-1} = e$ by definition

By associative property,

$(ab)(b^{-1}a^{-1}) = a(b(b^{-1}a^{-1}))$

Apply the property again

$a((b\,b^{-1})a^{-1}) = a(e\,a^{-1})$

$= a(a^{-1}) = e$

$\Rightarrow \quad (ab)^{-1}(ab)(b^{-1}a^{-1}) = (ab)^{-1}e$

$= (b^{-1}a^{-1}) = (ab)^{-1}$.

(ii) By definition of e

- If the binary operation is written as $(+)$ then for any positive integer n, we write

$a^n = \underbrace{a \cdots a}_{n \text{ times}}$ $\qquad na = \underbrace{a + \cdots + a}_{n \text{ times}}$

Groups

Definition : A non-empty set G with a binary operation $\cdot$ is said to be a group if

(i) $\cdot$ is associative
(ii) $\cdot$ is with identity
(iii) every element of G is invertible

Examples :

(i) $(\mathbb{Z}, +)$ ✓ (ii) $(\mathbb{N}, +)$ ×
(iii) $(\mathbb{R}, +)$ ✓ (iv) $(\mathbb{Q}, +)$ ✓
(v) $(\mathbb{R}, \cdot)$ × (vi) $(\mathbb{R}\setminus\{0\}, \cdot)$ ✓
(vi) $(M_{m\times n}(\mathbb{R}), +)$ ✓ (vii) $(M_n(\mathbb{R}), \cdot)$ ×
(viii) $(\mathrm{Maps}(S,S), \cdot)$ × (ix) $(GL_n(\mathbb{R}), \cdot)$ ✓

Proposition

If G is a group, then the equations $ax = b$ and $ya = b$ have unique solutions

Proof :

$$ax = b$$
$$a^{-1}(ax) = a^{-1}b$$
$$(a^{-1}a)x = a^{-1}b$$
$$ex = a^{-1}b$$
$$x = a^{-1}b$$

$$ya = b$$
$$(ya)a^{-1} = ba^{-1}$$
$$y(aa^{-1}) = ba^{-1}$$
$$ye = ba^{-1}$$
$$y = ba^{-1}$$

$a^{-1}b$ is the solution for $ax = b$
ba^{-1} is the solution for $ya = b$

Cancellation Law

- $ab = ac \Rightarrow b = c$
- $ba = ca \Rightarrow b = c$

Proof :

$$a^{-1}(ab) = a^{-1}(ac)$$
$$(a^{-1}a)b = (a^{-1}a)c$$
$$b = c$$

$$(ba)a^{-1} = (ca)a^{-1}$$
$$b(aa^{-1}) = c(aa^{-1})$$
$$b = c$$