Group Theory

PMATH 336

<u>e.g.</u> $\mathbb{Z}, +$

$a, b \in \mathbb{Z}$ $a+b \in \mathbb{Z}$ [Closure]

$0 \in \mathbb{Z}$ $a+0 = 0+a = a$ [Identity]

$5+(-5)=0$ $a+(-a) = 0$ [Inverse]

$(a+b)+c = a+(b+c)$ [Associativity]

$a+b = b+a$ [Commutativity]

e.g. $\mathbb{Q}, +$

e.g. $(\mathbb{Q}^*, \cdot)$

$$\mathbb{Q}^* = \left\{\frac{a}{b} \in \mathbb{Q} \;\middle|\; \frac{a}{b} \neq 0\right\}$$

e.g. $(\mathbb{Z}, -)$

general linear

e.g. $GL(2,\mathbb{R}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \;\middle|\; a,b,c,d \in \mathbb{R} \text{ and } \begin{vmatrix} a & b \\ c & d \end{vmatrix} \neq 0 \right\}$

$(GL(3, \mathbb{Z}_6))$

$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in GL(2,\mathbb{R})$

$GL(2,\mathbb{R})$, matrix $\cdot$

$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL(2,\mathbb{R})$ $B = \begin{bmatrix} e & f \\ g & h \end{bmatrix} \in GL(2,\mathbb{R})$

$$AB = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} e & f \\ g & h \end{bmatrix} = \begin{bmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{bmatrix}$$

$\det(AB) = R_{11}R_{22} - R_{12}R_{21} \neq 0$ $\det AB = (\det A)(\det B)$

$\Rightarrow AB \in GL(2,\mathbb{R})$

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

I_2 is the identity

MM is associative $\Rightarrow$ Associativity follows

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \left(\frac{1}{\det A} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \right) = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Inverse

Commutative? $A \cdot B = B \cdot A$?

$A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$ $B = \begin{bmatrix} 1 & -1 \\ -1 & -1 \end{bmatrix}$

$AB \neq BA \rightarrow GL(2,\mathbb{R})$ with MM is non commutative

---

<u>Definition (Group)</u>: A group is a set G and an operation $\cdot$ that satisfies the 4 axioms:

1. G is <u>closed</u> under $\cdot$ $s \cdot t \in G \ \forall s,t \in G$
2. There is an <u>identity</u> $0 \in G$ s.t. $0 \cdot s = s \cdot 0 = s \quad \forall s \in G$
3. There is an element (<u>inverse</u>) $t \in G$ s.t. $t \cdot s = s \cdot t = 0 \quad \forall s \in G$

④ __Associativity__: $(s\cdot t)\cdot u = s\cdot(t\cdot u)\ \ \forall s,t,u\in G$

⑤ Commutativity

If $\forall a,b\in G \cdot a\cdot b = b\cdot a$, then $(G,\cdot)$ is called an __abelian group__. (commutative group)

Otherwise, $(G,\cdot)$ is non-abelian

__Proposition__: In a group $(G,\cdot)$, the identity element is unique.

__Proof:__ Suppose $e\neq f\in G$ are two identity elements.

$e\cdot f = e$

$f\cdot e = f$

$\Rightarrow e = f$

$\lightning$ $\boxtimes$