§2. 群.

"·" binary operation on $S \iff$

$\cdot : S\times S \longrightarrow S$. $\cdot(a,b) = a\cdot b$.

$(G,\cdot)$ abel group $\iff$

1. $\forall a,b,c \in G.\ a\cdot(b\cdot c) = (a\cdot b)\cdot c$ 结合律.

单位元 identity element.

2. $\exists e \in G.\ \forall a\in G.\ a\cdot e = e\cdot a = a$.

3. $\forall a\in G,\ \exists a^{-1} \in G,\ a\cdot a^{-1} = a^{-1}\cdot a = e$.

逆元 inverse element.

4. $\forall a,b\in G,\ a\cdot b = b\cdot a$ 交换律.

$(G,+)$ abel group $\iff$

1. $\forall a,b,c\in G.\ a+(b+c) = a+(b+c)$ 结合

加法单位元

2. $\exists e\in G.\ \forall a\in G.\ a+e = e+a = a$

逆元

3. $\forall a\in G,\ \exists(-a)\in G,\ a+(-a) = (-a)+a = e$

交换

4. $\forall a,b\in G,\ a+b = b+a$.

Abel group "加群".

Ex1. $(\mathbb{Z},+)$. $(\mathbb{Q},+)$. $(\mathbb{R},+)$. $(\mathbb{C},+)$

1	✓	✓	✓	✓
2	0 ✓	0 ✓	0 ✓	0 ✓
3	$(-a)$ ✓	$-\frac{q}{p}$ ✓	$(-a)$ ✓	$(a+bi)$ $-a-bi$ ✓
4	✓	✓	✓	✓

Ex2: $(n\mathbb{Z}, +)$. $n \in \mathbb{N}^*$.

$n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$.

$2\mathbb{Z} = \{\cdots, -2, 0, 2, 4, 6, 8, \cdots\}$.

$3\mathbb{Z} = \{\cdots, -6, -3, 0, 3, 6, \cdots\}$.

① ✓ ② 0 ✓ ③ nk, $-nk = n(-k)$ ④ ✓

⓪ "+" 封闭.

Ex3: $(\mathbb{N}, +)$ not a group.

~~③~~ 1 没有加法逆元.

Assume $a+1=0$. $a=-1 \notin \mathbb{N}$.

Ex4: $(\mathbb{R}, \cdot)$ not a group.

$a \cdot 1 = 1 \cdot a = a$.

$\cancel{③}$. $a \cdot 0 = 1$.

$a \cdot 0 = 0 \neq 1$. $\Rightarrow \Leftarrow$.

0 没有乘法逆元.

Ex5: $\mathbb{R}^\times$. $(\mathbb{R} \setminus \{0\}, \cdot)$, $\mathbb{Q}^\times$. $(\mathbb{Q} \setminus \{0\}, \cdot)$ abel group

① $a \neq 0, b \neq 0 \Rightarrow ab \neq 0$. $ab = 0 \Rightarrow a = 0$ or $b = 0$.

② $1 \in \mathbb{R}^\times$. $1 \in \mathbb{Q}^\times$, ①. ④ ✓.

③ $a \neq 0$. $\frac{1}{a}$. $\left(\frac{q}{p}\right)^{-1} = \frac{p}{q}$.

Ex6: $(\mathbb{Z} \setminus \{0\}, \cdot)$ not group.

⓪ ✓ ① ✓ ② $1 \in \mathbb{Z}$. ✓

$\cancel{③}$. ④. ✓

$a \cdot 2 = 1$. $a = \frac{1}{2} \notin \mathbb{Z} \setminus \{0\}$ $\Rightarrow \Leftarrow$.

Ex 7: $(\mathbb{R}^n, +)$ abel group.

$u = (u_1, \cdots, u_n)$. $v = (v_1, \cdots, v_n)$.

$u + v = (u_1 + v_1, \cdots, u_n + v_n)$

⓪. ✓ ①. $u + (v + w) = (u_1 + (v_1 + w_1), \cdots)$

$(u+v)+w = ((u_1+v_1)+w_1, \cdots)$ ✓

④ ✓ ②. $(0, \cdots, 0) + (v_1, \cdots, v_n) = (v_1, \cdots, v_n)$

③. $-(v_1, \cdots, v_n) = (-v_1, \cdots, -v_n)$. $+$ $= (0, \cdots, 0)$

Ex 8: $(\mathbb{R}^{m \times n}, +)$ abel group.

$A = (a_{ij})$ $B = (b_{ij})$. $A + B = (a_{ij} + b_{ij})$

⓪. ✓ ①. ✓ ④. ✓.

②. $\begin{bmatrix} 0 & \cdots & 0 \\ \vdots & & \vdots \\ 0 & \cdots & 0 \end{bmatrix} = 0$. ③. $A = (a_{ij})$ $-A = (-a_{ij})$

✓.

Ex 9: $(\mathbb{R}^{n \times n}, \cdot)$ not group.

$I_n = \begin{bmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{bmatrix}$. $A \cdot I = I \cdot A = A$.

0 not invertible.

$0 = A \cdot 0 = I$ $\Rightarrow \Leftarrow$.

Ex 10: $GL_n(\mathbb{R}) := \{A \in \mathbb{R}^{n\times n} : \det(A) \neq 0\}$.

$(GL_n(\mathbb{R}), \cdot)$ group. but not abel.

General Linear Group

(0). $\det(A) \cdot \det(B) \neq 0$. $\det(AB) = \det(A)\det(B) \neq 0$.

(1). ✓ . (2). $I_n = \begin{bmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{bmatrix}$. $\det(I_n) = 1 \neq 0$. ✓

(3). $\det(A) \neq 0. \Rightarrow A$ invertible. ✓.

Ex 11: $SL_n(\mathbb{R}) := \{A \in \mathbb{R}^{n\times n} : \det(A) = 1\}$.

$(SL_n(\mathbb{R}), \cdot)$ group, but not abel.

Special Linear Group.

(0). $\det(A) = 1$, $\det(B) = 1$ $\det(AB) = 1 \cdot 1 = 1$.

(1). ✓ . (2). $I_n = \begin{bmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{bmatrix}$ $\det(I_n) = 1$. ✓.

(3). $\det(A) = 1 \neq 0$. $\exists A^{-1}$.

Check. $\det(A^{-1}) = 1$. $AA^{-1} = I$.

$\det(A)\ \det(A^{-1}) = \det(I) = 1$.

$\det(A^{-1}) = \frac{1}{\det(A)} = \frac{1}{1} = 1.$

Group. Abel Group.

Abel.

"+" $(\mathbb{Z}, +)$. $(\mathbb{Q}, +)$. $(\mathbb{R}, +)$ $(\mathbb{C}, +)$.

$(n\mathbb{Z}, +)$ $(\mathbb{R}^n, +)$. $(\mathbb{R}^{m\times n}, +)$

"$\cdot$" $(\mathbb{Q}^\times, \cdot)$. $(\mathbb{R}^\times, \cdot)$. $\underline{(\mathbb{C}^\times, \cdot)}$ Abel.

$(GL_n(\mathbb{R}), \cdot)$ $(SL_n(\mathbb{R}), \cdot)$

$\| \qquad \|$

$\{n\times n \text{ invertible matrices}\}$ $\{n\times n \text{ matrices with } \det = 1\}$.