Section 4 Groups

A *group* is one of the most general structures in which it's meaningful to do algebra. The concept is a distilation of $+$ on $\mathbb{R}$, and occurs in many many places in mathematics. If you understand groups, you are in a position to better understand most branches of mathematics.

★ **Definition** A *group* is a binary structure $\langle G, *\rangle$ satisfying

- $\mathcal{G}_1$: Associativity $(a*b)*c = a*(b*c) \quad \forall\, a, b, c \in G$.
- $\mathcal{G}_2$: Identity property There is $e \in G$ with $a*e = a = e*a \ \forall a \in G$
- $\mathcal{G}_3$: Inverse property Every $a \in G$ has an *inverse* $a' \in G$ satisfying $a*a' = e$ and $a'*a = e$

Ex $\langle \mathbb{R}, +\rangle$ is a group $\begin{cases} \mathcal{G}_1 & \text{associative} \\ \mathcal{G}_2 & e = 0 \quad 0+a = a \quad a+0 = a \\ \mathcal{G}_2 & a' = -a \end{cases}$

Ex $\langle \mathbb{R}, \cdot\rangle$ is not a group $\begin{cases} \mathcal{G}_1 & \text{associative } \checkmark \\ \mathcal{G}_2 & e = 1 \checkmark \\ \mathcal{G}_2 & a' = \frac{1}{a} \text{ but } 0 \in \mathbb{R} \text{ has no inverse } \times \end{cases}$

Ex $\langle \mathbb{R}^+, \cdot\rangle$ is a group

Ex $GL(n, \mathbb{R}) = \{ A \mid A \text{ is } n\times n \text{ invertible matrix with entries from } \mathbb{R} \}$

$\langle GL(3, \mathbb{R}), \cdot\rangle$ is a group $\begin{cases} \mathcal{G}_1 & \text{Matrix mult. is associative} \\ \mathcal{G}_2 & e = I = \begin{bmatrix} 1&0&0\\0&1&0\\0&0&1\end{bmatrix} \\ \mathcal{G}_3 & A' = A^{-1} \end{cases}$

Ex $M_{m\times n}(\mathbb{R}) = \{ A \mid A \text{ is } m\times n \text{ matrix, entries from } \mathbb{R} \}$

$\langle M_{2\times 3}(\mathbb{R}), +\rangle$ is a group $\begin{cases} \mathcal{G}_1 & \text{Matrix addition is associative} \\ \mathcal{G}_2 & e = \begin{bmatrix} 0&0&0\\0&0&0\end{bmatrix}. \\ \mathcal{G}_3 & A' = -A. \end{cases}$

Ex $\langle U_4, \cdot\rangle$ is a group. $\begin{cases} \mathcal{G}_1 & \text{mult. in } \mathbb{C} \text{ is associative} \\ \mathcal{G}_2 & e = 1. \\ \mathcal{G}_3 & 1' = 1 \quad i' = -i \quad -1' = -1 \quad -i' = i \end{cases}$

☆ <u>Definition</u> Group $\langle G, * \rangle$ is <u>abelian</u> if it's commutative

i.e. $a * b = b * a$ for all $a, b \in G$.

<u>Ex</u> Every group we've seen so far is abelian except $GL(3, \mathbb{R})$.

$A \cdot B \neq B \cdot A$ for all $A, B \in GL(3, \mathbb{R})$.

<u>From text:</u>

(2) Is $\langle 2\mathbb{Z}, + \rangle$ a group? $(2\mathbb{Z} = \{\ldots -2, 0, 2, 4, \ldots\})$ Yes.

(4) Is $\langle \mathbb{Q}, \cdot \rangle$ a group? No

(5) Is $\langle \mathbb{C}\ * \rangle$ where $z * w = |zw|$ a group?

(7) Find a group with 1000 elements: U_{1000}

Important Properties of a Group $\langle G, * \rangle$

<u>Cancellation</u> Suppose $a, b, c \in G$

(1) $a * b = a * c \Rightarrow b = c$ (left-cancellation)

(2) $b * a = c * a \Rightarrow b = c$ (right-cancellation)

<u>Proof of (1)</u> Suppose $a * b = a * c$. By $\mathcal{G}_3$ there is an $a' \in G$ with $a * a' = e$

Then $a' * (a * b) = a' * (a * c)$

so $(a' * a) * b = (a' * a) * c$ $\quad (\mathcal{G}_1)$

and $e * b = e * c$ $\quad (\mathcal{G}_3)$

so $b = c$. $\quad (\mathcal{G}_2)$

<u>Warning</u> If $a * b = c * a$, you can't necessarily conclude $b = c$ (unless G is abelian).

<u>Ex</u> $a * b = c * a$ but $b \neq c$.

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} = \begin{bmatrix} 4 & 3 \\ 2 & 1 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$\begin{bmatrix} 3 & 1 \\ 4 & 2 \end{bmatrix} = \begin{bmatrix} 3 & 1 \\ 4 & 2 \end{bmatrix}$$

Inverse of a product

If $a, b \in G$ then $(a * b)' = b' * a'$

Reason: $\underbrace{(b' * a')}_{\text{inverse of } (a*b)} * (a * b) = ((b' * a') * a') * b$

$= (b' * (a * a')) * b$

$= (b' * e) * b$

$= b' * b$

$= e$

Solving linear equations in a group $\langle G, * \rangle$

Solve $a * x = b$ .... $x = a' * b$

Solve $x * a = b$ ... $x = b * a'$

The Klein 4-group $\langle V, * \rangle$

$V = \{e, a, b, c\}$

*	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

$V = \{00, 01, 10, 11\}$

	00	01	10	11
00	00	01	10	11
01	01	00	11	10
10	10	11	00	01
11	11	01	01	00