GROUPS

G = Set of elements
$\circ$ = Binary Operation } $(G, \circ)$ group if

① Closure : $\forall a, b \in G$, $a \circ b \in G$

② Associativity : $\forall a, b, c \in G$, $a \circ (b \circ c) = (a \circ b) \circ c$

Generally, $(a_1 \circ a_2 \circ \dots \circ a_r) \circ (a_{r+1} \circ \dots \circ a_n)$ $(n \in \mathbb{Z}^+$
$= a_1 \circ a_2 \circ \dots \circ a_r \circ a_{r+1} \circ \dots \circ a_n$ $n \geq 3)$

③ Identity : $\forall a \in G$ $\exists e \in G$ such that
$a \circ e = e \circ a = a$

④ Inverse : $\forall a \in G$, $\exists x \in G$ such that $a \circ x = x \circ a = e$

Abelian Group / Commutative Group :
$\forall a, b \in G$, $a \circ b = b \circ a$

Ex:

① $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$, $(\mathbb{C},+)$ — Abelian Groups

id $= 0$

inv $= (-a)$

$(\mathbb{Z},*)$ ← id $= 1$, inv $= 1/a$? ✗

$(\mathbb{R},*)$, $(\mathbb{Q},*)$, $(\mathbb{C},*)$ — id $= 1$

inv for '0' $= 1/0$ ✗

→ $\neg$ GROUPS

$(\mathbb{Q}^*,*)$, $(\mathbb{R}^*,*)$, $(\mathbb{C}^*,*)$ — Abelian Gr.

② $(R,+,*)$ Ring, then $(R,+)$ group

$(F,+,*)$ Field, then $(F^*,*)$ group — Abelian

③ $(\mathbb{Z}_n,+)$ Abelian Group

$(\mathbb{Z}_p^*,*)$ ↗

Units of $(\mathbb{Z}_n,+,*)$ ⟹ $n = 1, 2, 4, p^e, 2p^e$ ✓

④ $(\mathbb{Z}_n,+,*)$ Ring → Units of Ring $*$

$U_9 = \{[1],[2],[4],[5],[7],[8]\}$

$= \{[a] \mid \gcd(a,9) = 1\}$

$(U_9,*)$ group (Abelian)

id $= [1]$ inv: $[2] \sim [5]$, $[8] \sim [8]$, $[4] \sim [7]$

ORDER of Groups: $|(G,\circ)| = |G|$

finite $\rightarrow$ $(\mathbb{Z}_n,+)$

$o(\mathbb{Z}_n,+)=n$

$o(\mathbb{Z}_p^*,*)=p-1$

infinite $\longrightarrow$ Ex: $(\mathbb{Z},+)$

$\rightarrow$ Units of Ring $(\mathbb{Z}_n,+,*)$ under $*$

$o(U_n,*)=\phi(n)$ $\leftarrow$ Euler Phi function

PROPERTIES OF GROUPS:

① Identity is Unique $\longrightarrow$ $e_1, e_2 \in G$ as identity

$e_1 \circ e_2 = e_2$ and $e_1 \circ e_2 = e_1$ $\Rightarrow$ $e_1 = e_2$ ✓

② Inverse is Unique $\longrightarrow$ $x_1, x_2 \in G$ are inverses of $a \in G$

$$x_1 = x_1 \circ e = x_1 \circ (a \circ x_2) = (x_1 \circ a) \circ x_2 \Rightarrow x_1 = x_2$$
$$= e \circ x_2 = x_2$$
✓

Cancellation Laws: $(G, \circ)$ group

① $\forall a, b, c \in G$ and $a \circ b = a \circ c \Rightarrow b = c$

(Left Cancellation)

② $\forall a, b, c \in G$ and $b \circ a = c \circ a \Rightarrow b = c$

(Right Cancellation)

$a \sim a^{-1}$ as inverse(a)

Proof: $a \circ b = a \circ c$

$\Rightarrow a^{-1} \circ (a \circ b) = a^{-1} \circ (a \circ c)$

$\Rightarrow (a^{-1} \circ a) \circ b = (a^{-1} \circ a) \circ c \Rightarrow e \circ b = e \circ c$

$\Rightarrow b = c$ ✓

Similar for Right Cancel. ?

▷ **Multiplicative Groups** : $(G, \cdot)$ group

$$a^0 = e \,,\quad a^1 = a \,,\quad a^2 = a \cdot a \,,\quad \ldots$$

$$a^n = a^{n-1} \cdot a = a \cdot a^{n-1}$$

$$\hookrightarrow a^m \cdot a^n = a^{m+n} = a^n \cdot a^m$$

Identity $= 1$ and inverse$(a) = a^{-1}$

▷ **Additive** Groups : $(G, +)$ group

$$0a = e \,,\quad 1a = a \quad 2a = a + a \,,\quad \ldots$$

$$na = (n-1)a + a = a + (n-1)a$$

$$\hookrightarrow ma + na = (m+n)a = na + ma$$

Identity $= 0$ and inverse$(a) = (-a)$

Ex: $G = \{a \in \mathbb{Q} \mid a \neq -1\}$ and

$a \circ b = a + b - ab \quad (\forall a, b \in G)$

→ Is $(G, \circ)$ an Abelian Group? $\boxed{\text{YES}}$

Solution: ① $a \circ b \in \mathbb{Q}$ → closure

② $a \circ (b \circ c) = a \circ (b + c - bc) = a + b + c - bc - a(b + c - bc)$

$= a + b + c - ab - bc - ca + abc$

$= (a \circ b) \circ c$

↳ Associativity

③ $a + e - ae = a \Rightarrow e = 0$ (as $a \neq -1$)

↳ identity

④ $a + x - ax = 0 \Rightarrow x = \frac{a}{a-1} \in \mathbb{Q}$ ← inverse of $a \in G$

$\boxed{*}$ $a \circ b = a + b - ab = b + a - ba = b \circ a$ (Abelian)

SUBGROUPS of GROUP ; $(G, \circ)$ group

$\phi \neq H \subseteq G$ and $(H, \circ)$ also forms Group

↳ then H as a subgroup of G

Ex: ① $G = (\mathbb{Z}_6, +)$ and $H = (\{[0], [2], [4]\}, +)$

↳ $H \neq \phi$ and $H \subseteq G$ as well as Group

② $(\mathbb{Z}_9, +, *)$ Ring ⟶ Units of it $(U_9, *) \triangleleft G$

Subgroups of $(U_9, *)$ $\begin{cases} H = (\{[1], [4], [7]\}, *) \\ H' = (\{[1], [8]\}, *) \end{cases}$

PROPERTIES OF SUBGROUPS : $(G,\circ)$ group

① $\phi \neq H \subseteq G$, H is a subgroup of G iff

(i) $\circ$ is closed under H

(ii) $\forall a \in H$ there exist $a^{-1} \in H$

Proof: [$\rightarrow$] $(H,\circ)$ group and by definition

[$\leftarrow$] Associativity: $a,b,c \in H \subseteq G$

$a\circ(b\circ c) = (a\circ b)\circ c$ (in G)

INHERITS the prop of G

Identity: $a \in H$ and $a^{-1} \in H$ $\quad H \subseteq G$

$\Rightarrow a \in G$ and $a^{-1} \in G$

$\therefore a\circ a^{-1} = e = a^{-1}\circ a$ (in G)

Hence, closure indicates $e \in H$

② $(G, \circ)$ is group and $\phi = H \subseteq G$ (and finite) ×
then H is a subgroup iff $\circ$ is closed.

Proof: $[\rightarrow]$ by definition ✓

$[\leftarrow]$ $aH = \{ah \mid h \in H\}$ If $a \in H$, $aH \subseteq H$

$\Rightarrow |aH| \leq |H|$

If $|aH| < |H|$ then

$ah_1 = ah_2 \longrightarrow$ (in G) $h_1 = h_2$ $\Rightarrow |aH| = |H|$

▷ $aH \subseteq H$ and $|aH| = |H|$ (H finite) $\Rightarrow$ $\boxed{aH = H}$

Identity: $ab = a$ $\Rightarrow$ $ab = ae$ (in G) $\Rightarrow$ $b = e$ ✓

Inverse: $ac = e$ Can I prove: $ca = e$? YES

$(ca)^2 = (ca)(ca) = c(ac)a = c(ea) = ca$

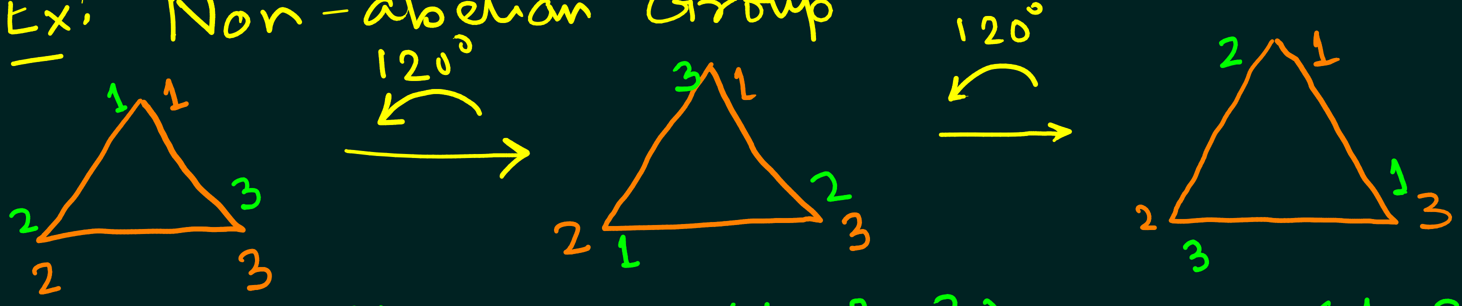
$= (ca)e$

$\therefore ac = e = ca$

$\Rightarrow \boxed{c = a^{-1}}$ ✓ $\Rightarrow ca = e$

$\boxed{(\mathbb{Z}, +) \xrightarrow{\text{sub groups}} (\mathbb{Z}^+, +)^{\text{inv} \times}, (\mathbb{N}, +) \times}$

Ex: Non-abelian Group



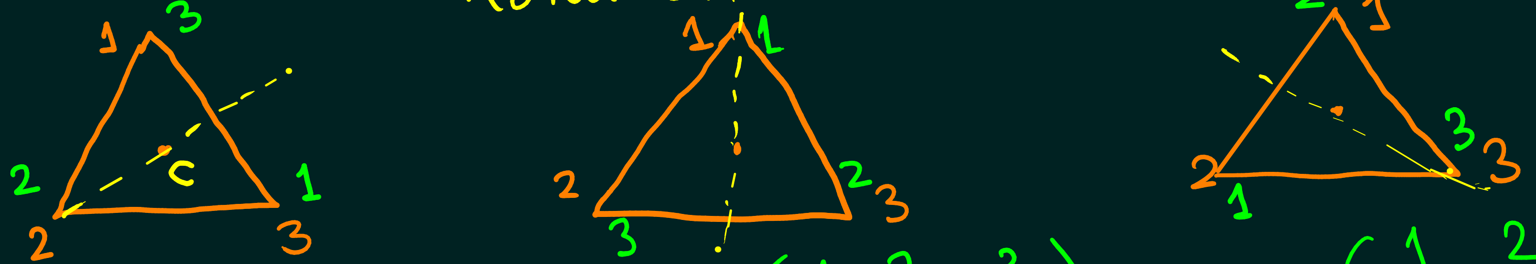
$$\pi_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \qquad \pi_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \qquad \pi_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

Rotational Positions

SYMMETRIC GROUP

$$G = \{\pi_0, \pi_1, \pi_2, r_1, r_2, r_3\}$$

S_3



$$r_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \qquad r_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \qquad r_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

Reflectional Position

o ← Rigid Motional Positioning

$O(G) = 3! = 6$

$\pi_0 =$ identity ✓ $\quad \pi_1^{-1} = \pi_2$ ✓ $\quad \pi_2^{-1} = \pi_1$ ✓ $\quad r_1^{-1}, r_2^{-1}, r_3^{-1} = ??$ ✓

$$\pi_1 \circ r_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \neq r_2 \circ \pi_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

NOT ABELIAN

☒ $(G, \circ)$ and $(H, *)$ are two Groups.

$((G \times H), \cdot)$ defined as

$\forall g_1, g_2 \in G$ and $\forall h_1, h_2 \in H$

$$(g_1, h_1) \cdot (g_2, h_2) = (g_1 \circ g_2), (h_1 * h_2)$$

→ $(G \times H)$ is a group over $\cdot$ binary operation.

↳ Why this is a group? (verify)