

# Algebraic Structures: Groups, Rings, Field, Boolean Algebra

Groups:  $(G, \circ)$ ,  $G$ -set,  $\circ: G \times G \rightarrow G$  (binary operation)

- ① Closure:  $\forall a, b \in G, a \circ b \in G$
- ② Associative:  $\forall a, b, c \in G, a \circ (b \circ c) = (a \circ b) \circ c$
- ③ Identity( $e$ ):  $\forall a \in G \exists e \in G, \text{ s.t. } a \circ e = e \circ a = a$
- ④ Inverse( $i$ ):  $\forall a \in G \exists i \in G, \text{ s.t. } a \circ i = i \circ a = e$

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

Ex: ①  $(\mathbb{Z}, +) \xrightarrow{\text{int.}}$   $e = 0, a^{-1} = (-a)$  inverse. (Abelian)

②  $(\mathbb{R}, *) \rightarrow e = 1, \text{ inv}(0) \text{ does not exist}$

③  $(\mathbb{Q}, \circ)$  where  $a \circ b = a + b - ab$   $G = \{a, b \neq 1\}$  Abelian Group  
 $a, b \in \mathbb{Q}, b \neq 1$

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

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

$a \circ e = a \Rightarrow a + e - ae = a \Rightarrow e = 0$   $i = \frac{a}{a-1} = (a \circ b) \circ c$

① Id is unique:  $e_1, e_2 \in G$

$$\begin{aligned} \underline{e_1} \circ e_2 = e_2 & \Rightarrow e_1 = e_2 \\ e_1 \circ \underline{e_2} = e_1 & \end{aligned}$$

② Inv. is unique:  $x_1, x_2 \in G$

$$\begin{aligned} a^{-1} &= x_1 \\ a^{-1} &= x_2 \end{aligned}$$

$$\begin{aligned} x_1 &= x_1 \circ e = x_1 \circ (a \circ x_2) \\ &= (x_1 \circ a) \circ x_2 = e \circ x_2 = x_2 \end{aligned}$$

$$\begin{aligned} a^n &= \underbrace{a a \dots a}_{n \text{ times}} \quad 1, 1/a \\ na &= \underbrace{a + a \dots a}_{n \text{ times}} \quad 0, -a \end{aligned}$$

③ Cancellation:  $(G, \circ)$  group

$\forall a, b, c \in G$  (i)  $a \circ b = c \circ b \Rightarrow a = c$  (RC)

(ii)  $a \circ b = a \circ c \Rightarrow b = c$  (LC)

$$a \circ b = a \circ c$$

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

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

$$\Rightarrow e \circ b = e \circ c \Rightarrow b = c$$

Subgroup of  $(G, \circ)$

$(H, \circ)$  is a subgroup if  $H \subseteq G$  and  $(H, \circ)$  forms a group

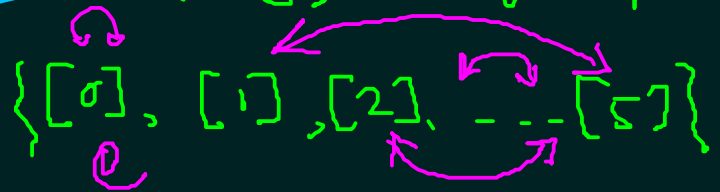
Ex:  $G = (\mathbb{Z}_6, +)$  group?

- $6k$
- $6k+1$
- $6k+2$

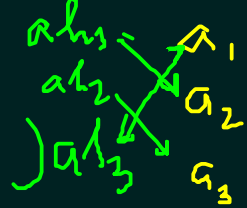
$$H \subseteq G \rightarrow \{ [0], [2], [4] \}$$

$(H, +)$  group?

order  $e \circ a = e$



Properties of Groups / Subgroups:  $(G, \circ)$   $\forall a, b \in G$



Proof:  $(a \circ b) \circ (b^{-1} \circ a^{-1}) = e$  ?  $\checkmark$   
 $\Rightarrow a \circ (b \circ b^{-1}) \circ a^{-1} = (a \circ e) \circ a^{-1} = a \circ a^{-1} = e$

②  $\emptyset \neq H \subseteq G$   $(H, \circ)$  is S.G. of  $G$   $(b^{-1} \circ a^{-1})^{-1} = a \circ b$   
 iff  $\left\{ \begin{array}{l} \text{(i) } \circ \text{ is closed under } H \\ \text{(ii) } \forall a \in H, \exists a^{-1} \in H \end{array} \right\} \checkmark$   $\forall a, b, c \in H \subseteq G$

Proof: " $\Rightarrow$ "  $(H, \circ)$  group  $\checkmark$  Assoc:  $a \circ (b \circ c) = (a \circ b) \circ c$   $\checkmark$  (inherits)  
 " $\Leftarrow$ " Closure  $\checkmark$  inverse  $\checkmark$

③  ~~$G$~~   $G$  is finite  $\checkmark$   
 $(H, \circ)$  is S.G.  $\Leftrightarrow \{ \circ \text{ is closed} \} \checkmark$   
 " $\Leftarrow$ "  $a \in H \rightarrow aH = \{ ah \mid h \in H \}$   
 $aH \subseteq H \Rightarrow |aH| \leq |H| \rightarrow |aH| < |H| \rightarrow ah_1 = ah_2 \rightarrow h_1 = h_2$   
 $\boxed{aH = H} \checkmark$   
 Ident:  $ab = ae \Rightarrow b = e$   
 $(xa)^2 = (xa)(xa) = x(ax)a = x(e)a = (xa)e \rightarrow xa = e ???$   
 Ident:  $ax = e$   
 Diagram:  $a, b$  in a circle  $\xrightarrow{aH}$   $a$  in a circle  $\xrightarrow{H}$   $a$  in a circle

Homomorphism:  $f: (G, \circ) \rightarrow (H, *)$  group homo. M.

if  $\forall a, b \in G$   $f(a \circ b) = f(a) * f(b)$

Ex:  $f: (\mathbb{Z}, +) \rightarrow (\mathbb{Z}_4, +)$   $\begin{matrix} [0] & [1] & [2] & [3] \\ \swarrow & & & \end{matrix}$

$$f(x) = [x] = \{x + 4k \mid k \in \mathbb{Z}\}$$

$$f(x+y) = [x+y] = [x] + [y] = f(x) + f(y)$$

group  
h.o.m.

$$a^n a^m = a^{n+m} \\ = a^m a^n \quad \langle -i \rangle$$

Isomorphism

if  $f$  is bijective.

①  $e_H = f(e_G)$

②  $f(a^{-1}) = [f(a)]^{-1}$

Ex:  $G = \{-1, 1, i, -i\}$   $f: (G, *) \rightarrow (\mathbb{Z}_4, +)$   $\langle i \rangle$

Cyclic  $f(1) = [0]$

$$f(-1) = [2]$$

$$f(i) = [1]$$

$$f(-i) = [3]$$

$$f(1 * -1) = f(-1) = [2] = [2] + [0]$$

$$f(i * -i) = f(1) = [0] = f(1) + f(-1)$$

$$= [1] + [3] = f(i) + f(-i)$$

$$\begin{matrix} i^2 = -1 \\ i^3 = -i \\ i^4 = 1 \end{matrix}$$

Rings:  $(R, +, *)$  is Ring

$\forall a, b, c \in R$

- ①  $a + b = b + a$  ✓
- ②  $(a + b) + c = a + (b + c)$
- ③  $0 + a = a + 0 = a$
- ④  $-a \in R$   $a + (-a) = (-a) + a = 0$
- ⑤  $a * (b * c) = (a * b) * c$
- ⑥  $a * (b + c) = a * b + a * c$

$a + x - ax = a$   
 $x(-a) = 0$   
 $0$

$(R, +, *)$  is commutative  $\rightarrow$  " $a * b = b * a$ "

$(R, +, *)$  ring with identity  $\rightarrow 1 \in R$   $\forall a \in R$

Ex:  $(\mathbb{Z}, \oplus, \odot) \rightarrow \begin{cases} a \oplus b = a + b - 1 \\ a \odot b = a + b - ab \end{cases}$  ✓  
 $\underline{1} * a = a * \underline{1} = a$

$0 = 1$

$\rightarrow$  Ring - Yes!, Commutative  $\rightarrow$  Yes!  $(-a)^{\oplus} = 2 - a$

Ring with identity - Yes!

$a \odot 0 = 0 \odot a = a$

$(\mathbb{Q}, +, *)$ ,  $(\mathbb{R}, +, *)$

$a + 0 - a \times 0 = a$   $1 = 0$

Units:  $\exists b \in R$  s.t.  $ab = b^*a = 1_{\text{idem}(*)}$   $\begin{cases} b = a^{-1} \\ \text{or } b^* = a \end{cases}$   
( $a, b$  is a units.)

Field: Ring with <sup>every</sup> non-zero elements as units.  
(non ass. id.)

Ex  $(\mathbb{Q}, +, *)$ ,  $(\mathbb{R}, +, *) \longrightarrow$  fields.

Homomorphisms:  $f: (R, +, *) \rightarrow (T, \oplus, \odot)$

$$\text{if } f(a+b) = f(a) \oplus f(b) \checkmark$$

$$\text{and } f(a*b) = f(a) \odot f(b) \checkmark$$

+ bijection  $f \Rightarrow$  Isomorphism

$$f: (\mathbb{Q}, +, *) \rightarrow (\mathbb{Q}, +, *)$$

$$G(V, \wedge, \nabla)$$

Subrings