Algebraic Structures: Groups, Rings, Field, Boolean Algebra

Groups: $(G, \circ)$, G - set, $\circ : G \times G \to G$ (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): $\forall a \in G$ $\exists e \in G$, s.t $a \circ e = e \circ a = a$
4. Inverse(i) $\forall a \in G$ $\exists i \in G$, 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 $(\mathbb{Z}, +)^{\to \text{inf.}}$ $\rightarrow$ $e = 0$, $a^{-1} = (-a)$ inverse. (Abelian)

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

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

$a \in \mathbb{Q}$, $b \in \mathbb{Q}$

$a \circ (\underbrace{b \circ c}_{b+c-bc}) = a + (b + c - bc) - a(b + c - bc)$ $e(1-a) = 0$

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

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

① Id is unique: $e_1, e_2 \in G$

$\left.\begin{array}{l} e_1 \circ e_2 = e_2 \\ e_1 \circ e_2 = e_1 \end{array}\right\} \Rightarrow e_1 = e_2$

② Inv. is unique: $x_1, x_2 \in G$

$a^{-1} = x_1$

$a^{-1} = x_2$

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

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

$a^n = \underbrace{aa\ldots}_{n \text{ times}}$ $1, 1/a$

$na = \underbrace{a + a \ldots}_{n \text{ times}}$ $0, -a$

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)

$a \circ b = a \circ c$

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

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

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

Subgroup of $(G, \circ)$

$(H, \circ)$ is if $H \subseteq G$ and $(H, \circ)$ forms Group

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

$0 = 6$

$\{[0], [1], [2], \ldots [5]\}$
e

$6k$

$6k+1$

$6k+2$

$H \subseteq G$

$\{[0], [2], [4]\}$
e

$(H, +) \longrightarrow$ group?

$\boxed{\text{order}}$

$e \circ e = e$

Properties of Groups / Subgroups: $\boxed{(G, \circ)}$

1. $\forall a, b \in G$

P.T. $(a \circ b)^{-1} = (b^{-1} \circ a^{-1})$

$a h_1 = a_1$, $a h_2 = a_2$, $a h_3 = a_3$

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

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

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

2. $\phi \neq H \subseteq G$ $(H, \circ)$ is S.G. of G

iff $\left\{ \begin{array}{l} \text{(i) } \circ \text{ is closed under } H \\ \text{(ii) } \forall a \in H, \ \exists a^{-1} \in H \end{array} \right\}$

$\forall a, b, c \in H \subseteq G$

Proof: "$\Rightarrow$" $(H, \circ)$ group

Assoc: $a \circ (b \circ c) = (a \circ b) \circ c$ (inherits)

"$\Leftarrow$" Closure, inverse

Iden: $a \in H$ $\exists a^{-1} \in H$

$\underbrace{a \circ a^{-1}}_{\text{closure}} = e = a^{-1} \circ a$ (in G)

3. G is finite

$(H, \circ)$ is S.G $\Longleftrightarrow \{ \circ$ is closed $\}$

"$\rightarrow$"

"$\leftarrow$" $a \in H \rightarrow aH = \{ah \mid h \in H\}$

$\boxed{aH = H}$

$aH \subseteq H \Rightarrow |aH| \leq |H| \rightarrow |aH| < |H|$

$ah_1 = ah_2$

$h_1 = h_2$

Ident: $ab = ae \Rightarrow b = e$

$ax = e$

aH, H, ab, a

$(xa)^2 = (xa)(xa) = x(ax)a = x(ea) = (xa)e \rightarrow xa = e$???

Homo-morphism: $f : (G, \circ) \longrightarrow (H, *)$ group homo. M.

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

Ex: $f : (\mathbb{Z}, +) \rightarrow (\mathbb{Z}_4, +)$ $\quad [0]\ [1]\ [2]\ [3]$

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

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

$a^n a^m = a^{m+n} = a^m a^n$

$\langle -i \rangle$

① $e_H = f(e_G)$

② $f(a^{-1}) = [f(a)]^{-1}$

Isomorphism

if f is bijective.

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

cyclic

$i^2 = -1$

$i^1 = i$

$i^3 = -i$

$i^4 = 1$

$f(1) = [0]$

$f(-1) = [2]$

$f(i) = [1]$

$f(-i) = [3]$

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

$f(i * -i) = f(1) = [0] = [1] + [3] = f(i) + f(-i)$

Rings: $\boxed{(R, +, *) \text{ is Ring}}$ $\quad \forall a, b, c \in R$

① $a+b = b+a$ ✓ ② $(a+b)+c = a+(b+c)$

③ $0+a = a+0 = a$ $\quad 0 \in R$ ✓ ④ $-a \in R$ $\quad a+(-a) = (-a)+a = 0$ ✓

⑤ $a*(b*c) = (a*b)*c$

⑥ $a*(b+c) = a*b + a*c$

$a + x - ax = a$

$x(1-\cancel{a}) = 0$

0

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

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

$1*a = a*1 = a$

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

$\cancel{(a+1)}$

$\hookrightarrow$ Ring – Yes!, Commutative $\rightarrow$ Yes! $\quad 0 = 1$ $\quad (-a)^{\#} = 2-a$

Ring with identity — Yes!

$a \odot \boxed{0} = \boxed{0} \odot a = a$

$\boxed{a+0-a\times 0} = a$

$1 = 0$

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

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

(a, b is a units.)

Field: Ring with every non-zero elements as units.
(non add. id)

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

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

if $f(a+b) = f(a) \oplus f(b)$ ✓

and $f(a * b) = f(a) \odot f(b)$ ✓

+ bijection $f \Rightarrow$ Isomorphism

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

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

Subrings