群 環 體

Group Ring Field

[1] $(G, *)$ is a group

[2] $(G, +, \times)$ is a ring

[3] $(G, +, \times)$ is a field

$(G, *)$ is a group

if ① $*$ is closed

$$a, b \in G \Rightarrow a * b \in G$$

② $*$ is associative

$$a, b, c \in G \Rightarrow (a * b) * c = a * (b * c)$$

③ $\exists$ identity $e \in G$

$$a \in G \Rightarrow a * e = e * a = a$$

④ $\exists\, a^{-1} \in G$ for any $a \in G$

s.t. $a * a^{-1} = a^{-1} * a = e$

If furthermore

⑤ $*$ is commutative

$a, b \in G \Rightarrow a * b = b * a$

we call $(G, *)$ is a commutative group

(or an abelian group)

Eg.

① $(\mathbb{R}, +)$ is a group

② $(\mathbb{R}\setminus\{0\}, \times)$ is a group

③ $(\mathbb{Z}, +)$ is a group

④ $(\mathbb{Z}_m, +)$ is a group

⑤ $(\mathbb{Z}_m\setminus\{0\}, \times)$ is a group

for prime m

$(G, +, \times)$ is a ring

if ① $(G, +)$ is abelian group

② $\times$ is closed

③ $\times$ is associative

④ distribution property is satisfied

$\Downarrow$

$a, b, c \in G$

$\Rightarrow (a+b) \times c = (a \times c) + (b \times c)$

$a \times (b+c) = (a \times b) + (a \times c)$

E.g. ① $(\mathbb{Z}, +, \times)$ is a ring

② $(\mathbb{Z}_m, +, \times)$ is a ring

③ $(\mathbb{Q}, +, \times)$ is a ring

④ $(\mathbb{R}, +, \times)$ is a ring

$(G, +, \times)$ is a field

① $(G, +, \times)$ is a ring

② $(G \setminus \{0\}, \times)$ is an abelian group

where 0 is the additive identity

Eg:

infinite

1. $(\mathbb{Q}, +, \times)$ is a field
2. $(\mathbb{R}, +, \times)$ "
3. $(\mathbb{C}, +, \times)$ "

finite

4. $(\mathbb{Z}_p, +, \times)$ "
5. $(GF(p^k), +, \times)$ "

Note:

1. $(\mathbb{Z}, +, \times)$ is not a field
2. $(\mathbb{Z}_m, +, \times)$ is not a field if m is not a prime