

(1) Group:

Definition: A set combined with a binary operations such that

- ★ There exists an identity element within the group
- ★ The group has the property of invertibility:
Every element in the group has an inverse
- ★ The operator is associative:

Assuming that the group is a set G containing elements a, b, c and the operator $*$, $a*(b*c)$ must be equal to $(a*b)*c$

- ★ The group is closed under the operation

If two elements a & b exist in the group, then $a*b$ also exists in the group.

Eg: The set of all integers and the operation " $+ \text{ mod } 5$ " a group, since " $+ \text{ mod } 5$ " gives values between 0 to 4 and is associative, has an identity element 0, and is invertible

★ Rings:

Definition: A ring is a set S with two binary operations $+$ and $*$ satisfying the following:

$$\forall a, b, c \in S, (a+b)+c = a+(b+c)$$

$$\forall a, b \in S, a+b = b+a$$

There exists an element 0 belonging to S such that $\forall a \in S \quad 0+a = a+0 = a$

for every $a \in S$ there exists $-a \in S$ such that $a+(-a) = -a+a = 0$

$$\forall a, b, c \in S \quad (a*b)*c = a*(b*c)$$

$$\forall a, b, c \in S \quad a*(b+c) = (a*b) + (a*c)$$
$$(b+c)*a = (b*a) + (c*a)$$

$\forall a, b, c \in S \quad a*b = b*a$ (This is optional, rings following this are called commutative rings)

There exists an element 1 belonging to S such that $\forall a \in S \quad 1*a = a*1 = a$
(This is also optional, as explained at the bottom of the assignment)

Eg: The set of all integers with operations of addition⁽⁺⁾ and multiplication^(*).
Since the operation of multiplication doesn't have an inverse that is an integer, but all other properties hold, it doesn't form a field.
But it is a ring

* Fields:

Definition: Fields are rings which have an additional property that multiplication operation (i.e. $*$) is invertible for all $a \in S, a \neq 0$. (Fields also require commutativity, associativity, identity and invertibility under $*$)

for every $a \in S$ (a $\neq 0$) There exists $a^{-1} \in S$ such that $a*a^{-1} = a^{-1}*a = 1$

Eg: The set of all rational numbers with operations addition⁽⁺⁾ and multiplication^(*) form a field

Note: In the case of rings, the operation ' $*$ ' may not have an identity element, may not be commutative, or rarely not even associative. These properties are optional. But are compulsory for fields.