Group and Ring

Shno Othman Ahmed

Group

Deffinition: A group is a set G together with a binary operation $*$, denoted by $(G, *)$

$$(a, b) \mapsto a * b : G \times G \to G$$

satisfying the following conditions:

G1: ***(closure)*** if $\forall$ a; b $\in$ G; $\quad a * b \in G$

G2: ***(associativity)*** for all a, b, c $\in$ G,

$$a * (b * c) = (a * b) * c$$

G3: **(existence of identity element)** $e \in G$ such that $\forall\, a \in G$; $e * a = a * e = a$

e is an ***identity element*** for (with respect to $*$)

G4: **(existence of inverses)** for each $\forall\, a \in G$, $\exists\, a^{-1} \in G$

such that $a * a^{-1} = a^{-1} * a = e$.

then a^{-1} is ***an inverse element*** of a.

then (G,*) is a group.

Note: If the * satisfy the ***commutative*** property ;
if $\forall$ a; b $\in$ G;

$$a * b = b * a$$

then (G,*) is commutative (abelian) group.

Proposition:Let (G,*) be any group, then:

1- The identity element is unique.
2- Any element a have one inverse element a^{-1}

Example :

Show that the set of all integers ...,**-4, -3, -2, -1, 0, 1, 2, 3, 4,** ... is an infinite Abelian group with respect to the operation of addition of integers ***(Z,+)***

Solution:

Let us test all the group axioms for Abelian group.

(G1) Closure Axiom. We know that the sum of any two integers is also an integer, i.e., for all $a, b \in \mathbb{Z}$, $a + b \in \mathbb{Z}$.

Thus $\mathbb{Z}$ is closed with respect to addition.

(G2) Associative Axiom . Since the addition of integers is associative, the associative axiom is satisfied, i.e.,

for $a, b, c \in \mathbb{Z}$

Such that $a + (b + c) = (a + b) + c$

(G3) Existence of Identity. We know that 0 is the additive identity and $0 \in \mathbb{Z}$, i.e., $0 + a = a = 0 + a \quad \forall a \in \mathbb{Z}$

Hence, additive identity exists.

(G4) Existence of Inverse. If $a \in \mathbb{Z}$, then $-a \in \mathbb{Z}$. Also,

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

Since addition of integers is a commutative operation, therefore $a+b=b+a \quad \forall a,b \in \mathbb{Z}$

Hence $(\mathbb{Z},+)$ is an Abelian group. Also, $\mathbb{Z}$ contains an infinite number of elements. Therefore $(\mathbb{Z},+)$ is an ***Abelian group*** of infinite order.

Example: (Q,+), (Q\{0},.) (R,+), (R|{0},.), (C , +) and (C\{0},.) are groups .

Example:(N,+),(N , .)and ***(Z,.)*** are not groups.

Semigroup: **is an algebraic structure consisting of a set together with an associative binary operation.**

or

A semigroup **is a pair (S, ∗) where S is a non-empty set and ∗ is an associative binary operation on S.**

Example:

(N,+) *is semi group*

***(N,+)* is semi group**

If a, b , c $\in$ Z then a*(b*c) $\in$ Z

a*(b*c)=a+(b+c)=(a+b)+c=(a*b)*
c

2+(6+1)=9=(2+6)+1=9

So it is associative

Subgroups

Definition: A subgroup **H** of a group G is a non-empty subset of G that forms a group under the binary operation of G.

or

Definition: *Let S be a nonempty subset of a group G. If*

S_1: $a; b \in S \longrightarrow a*b \in S$, *and*

S_2: $a \in S \longrightarrow a^{-1} \in S$

*then the (S, *) is a subgroup of a group (G, *).*

Example: $(Z,+)$ *is subgroup of group* $(Q,+)$.

$(Z,+)$ *is subgroup of group* $(R,+)$.

$(Q,+)$ *is subgroup of group* $(R,+)$.

$(R,+)$ *is subgroup of group* $(C,+)$.

$(Q\backslash\{0\},.)$ *is subgroup of group* $(R\backslash\{0\},.)$.

$(R\backslash\{0\},.)$ *is subgroup of group* $(C\backslash\{0\},.)$.

Z is a subset of Q

(Z,+) is a subgroup of (Q,+)

(Q,+) IS A GROUP

1) If a,b $\in$ Z then a+b $\in$ Z

-7 ,3 $\in$ Z

-7+3= -4 $\in$ Z

1) If a $\in$ Z then a^{-1} $\in$ Z

2 $\in$ Z then -2 $\in$ Z

-2 is inverse of 2

2+(-2)=0 0 is identiy of + in Z

Ring

A ring is defined as a non-empty set R with two binary operations $+ , \cdot : R \times R \to R$ *with the properties:*

(i) $(R, +)$ *is an abelian group (zero element 0);*

(ii) $(R, \cdot)$ *is a semigroup;*

(iii) for all $a, b, c \in R$ *the distributivity laws are valid:*

$$(a + b)c = ac + bc, \qquad a(b + c) = ab + ac.$$

And it's denoted by $(R,+,.)$

Note:

1-The ring R is called commutative if $(R, \cdot)$ is a commutative semigroup, i.e. if $ab = ba$ for all $a, b \in R$.

2-If there is an identity for multiplication, then R is said to have identity.

Example:

$(Z,+,.)$ is a commutative ring with identity 1.

$(Q,+,.)$ is a commutative ring with identity 1.

$(R,+,.)$ is a commutative ring with identity 1.

$(C,+,.)$ is a commutative ring.

EXAMPLE :-

(Z,+,.) IS RING

(Z,+) is ablian group

for all $a, b \in \mathbb{Z}$, $a + b \in \mathbb{Z}$.

Thus $\mathbb{Z}$ is closed with respect to addition.

for $a, b, c \in \mathbb{Z}$

Such that $a + (b + c) = (a + b) + c$

(G3) Existence of Identity. We know that 0 is the additive identity and $0 \in \mathbb{Z}$, i.e., $0 + a = a = 0 + a \quad \forall a \in \mathbb{Z}$

Hence, additive identity exists.

(G4) Existence of Inverse. If $a \in \mathbb{Z}$, then $-a \in \mathbb{Z}$. Also

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

Therefore $\mathbb{Z}$ is a group with respect to addition.

Since addition of integers is a commutative operation, therefore $a+b=b+a \quad \forall a,b \in \mathbb{Z}$

Hence $(\mathbb{Z},+)$ is an Abelian group. Also, $\mathbb{Z}$ contains an infinite number of elements. Therefore $(\mathbb{Z},+)$ is an ***Abelian group*** of infinite order.

(Z,.) is semi group

If a, b c $\in$ Z then a.(b.c) $\in$ Z

a*(b*c)=a.(b.c)=(a.b).c=(a.b).c

2.(6.1)=12=(2.6).1=12

1 is identity for multiplication (.)

1.a=a

5.1=5