Notes

Page No.:
Date: / /

Group theory

Groupoid or Binary Algebra : definition

→ A non-empty set G equipped with one binary operation '*' is called groupoid.
i.e G is a groupoid if G is closed for *
It is denoted by (G, *).

Ex:- (N, +), (Z, -), (Q, ×) etc.

Note: Groupoid is also called Quasi group

Semigroup :-

A algebric structure (G, *) is called semi-group if the binary operation * satisfies associative property i.e
(G, *) $(a*b)*c = a*(b*c)$ $\forall a \in G$

Ex:1 The algebric structures (N, +), (Z, +) (Z, ×), (Q, ×) are semi groups but the structure (Z, -) is not so because (-) is not associative.

Ex:-2 The structures (P(S), ∪) & (P(S), ∩) where P(S) is the power set are semi

Teacher's Signature

Notes

groups are both the operation union (∪) & intersection (∩) are not associative

Ex 1: The semigroup $(N, \times)$ is a monoid because 1 is the identity for the multiplication. But the semigroup $(N, +)$ is not a monoid, because 0 is the identity for addition is not in N.

Ex 2: The semigroup $(P(S), \cup)$ & $(P(S), \cap)$ are monoid because ϕ & S are the identities respectively for union (∪) & intersection (∩) in $P(S)$.

Group - definition

→ An algebraic structure to set G and a binary operation * defined on G i.e $(G, *)$ is called group if * satisfies the following postulate

[G_1] Closure $a \in G, b \in G \Rightarrow a * b \in G, \forall a, b \in G$

[G_2] Associativity: The combination * is associative on G i.e $(a * b) * c = a * (b * c), \forall a, b, c \in G$

[G_3] Existence of identity: There exists an identity element e in G such that $e * a = a * e = a, \forall a \in G$.

Teacher's Signature

Page No.:
Date: / /

Notes

[G_4] Existence of Inverse: each element in G is invertible, i.e for every $a \in G$, there exists a^{-1} in G such that $a * a^{-1} = a^{-1} * a = e$ (identity) then group $(G, *)$ is a monoid in which each of its element has a multiplicative inverse

* Abelian group or Commutative group: definition

→ A group $(G, *)$ is said to be abelian or commutative if $*$ is commutative also a group $(G, *)$ is an abelian group, if

[G_4] Commutative: $a * b = b * a$ $\forall a, b \in G$

G_1 ~~Associativity~~ ~~$a * b = b * a \; \forall a, b \in G$~~ semi-group.

G_2 Existence of identity } Monoid

G_3 Existence of Inverse } Group.

G_4 Commutativity → commutative or abelian group.

Teacher's Signature

Page No.:
Date: / /

Notes

Finite & infinite group

→ A group $(G, *)$ is said to be finite if its underlying set G is a finite set and a group which is not finite is called an infinite group.

→ order of a group:
→ The no. of elements in a finite group is called the order of the group.

→ It is denoted by $O(G)$
→ If $(G, *)$ is an infinite group, then it is said to be of infinite order

Example 1

Show that the set of Integers forms an abelian group under addition.

Let $G = \{0, \pm 1, \pm 2, \pm 3, \ldots\}$

G_1: Closure: let $a, b \in G \Rightarrow a+b \in G$
Closure law is satisfied.

G_2: Associative: let $a, b, c \in G$
$a+(b+c) = (a+b)+c$
Associative law is satisfied

G_3: Identity: let $a \in G$ and 0 be the identity $a+0 = 0+a$

Teacher's Signature

Notes

G_4 : Inverse - a and the inverse of a
$a + (-a) = 0$; $-a + a = 0$

G_3 : commutative : let $a, b \in G$
$a + b = b + a$

Hence, $(G, +)$ is an Abelian group under addition.

Q. 27 G is the set of rationals except -1 binary operations $*$ is defined by $a * b = a + b + ab$. Show that it is a group. $\{Q - (-1)\}$

G_1 : Let $a, b \in G \Rightarrow a * b = a + b + ab \in G$
closure law is valid.

G_2 : Let $a, b, c \in G$
$a * (b * c) = (a * b) * c$
LHS $b * c = b + c + bc = x$
$a * x = a + x + ax$
$= a + b + c + bc + a(b + c + bc)$
$= a + b + c + bc + ab + ac + abc$
$= a + b + c + c(a + b) + ab(1 + c)$

RHS
$a * (b * c)$
$\Rightarrow (a * b) * c = (a + b + ab) * c$
$= (a + b + ab) + c + (a + b + ab)c$
$= a + b + ab + c + ac + bc + abc$
$\Rightarrow a + b + c + ac + bc + abc$

Teacher's Signature

Notes

Page No.:
Date: / /

Associativity is Valid

G3: Identity Let $a \in G$ and e be the identity.

$$a * e = e * a = a$$

$$\Rightarrow a + e + ae = e + a + ea = a$$

$$\boxed{a + e + ae = a + e + ae}$$

Identity is satisfied

$$a + e + ae = a$$

$$e(1 + a) = 0$$

$$\boxed{e = 0}$$

$$\boxed{a \neq -1}$$

G4: Let $a \in G$ & a^{-1} be the inverse of a

$$a * a^{-1} = a^{-1} * a = e$$

$$a + a^{-1} + aa^{-1} = a^{-1} + a + a^{-1}a = e$$

$$\boxed{e = 0}$$

$$a + a^{-1} + aa^{-1} = a^{-1} + a + a^{-1}a = 0$$

Inverse is satisfied

$$a + a^{-1}(1 + a) = 0$$

$$\boxed{a^{-1} = \frac{-a}{1 + a}}$$

$(G, *)$ is a Group

Teacher's Signature

Notes

Page No.:
Date: / /

Q. In $\mathbb{Z}$ we define $a*b = a+b+1$ show that $(\mathbb{Z}, *)$ is an abelian group

Ans: G1: Let $a*b = a+b$ $a, b \in \mathbb{Z}$ then $a*b = a+b+1$

Closure property satisfied

G2: Let $a, b, c \in \mathbb{Z}$

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

LHS:

$\Rightarrow a*(b+c+1)$ $\quad [b*c = b+c+1]$

$\Rightarrow a+(b+c+1)+1$

$\Rightarrow \boxed{a+b+c+2}$

RHS

$= (a*b)*c \Rightarrow (a+b+1)*c$

$\Rightarrow (a+b+1)+c+1$

$\Rightarrow \boxed{a+b+c+2}$

$\boxed{LHS = RHS}$

$\Rightarrow$ Associativity Law is satisfied.

G3: Let $a \in \mathbb{Z}$ e be the identity of a $e \in \mathbb{Z}$.

$a*e = e*a = a$

$\Rightarrow (a+e+1) = (e+a+1) = a$

$a+e+1 = a$

$\boxed{e = -1}$

Here the existence of identity is present

Teacher's Signature

Q4: Existence of inverse.

Let $a \in \mathbb{Z}$, $2-a^{-1} \in \mathbb{Z}$ is the inverse of a.

$\Rightarrow a * a^{-1} = a^{-1} * a = e \quad [\because e = -1]$

$\Rightarrow a + a^{-1} + 1 = a^{-1} + a + 1 = a^{-1}$

$\Rightarrow a + a^{-1} + 1 = -1$

$a + a^{-1} + 2 = 0$

$\Rightarrow \boxed{a^{-1} = -a - 2}$

$\Rightarrow a^{-1} + a + 1 = -1$

$\Rightarrow a^{-1} + a = -2$

$\Rightarrow \boxed{a^{-1} = -2 - a}$

Here, the inverse exist.

Q5: Commutative Law?

Let $a, b \in \mathbb{Z}$

$\Rightarrow \boxed{a * b = b * a}$

$\Rightarrow \boxed{a + b + 1 = b + a + 1}$

$\Rightarrow$ Commutative Law is valid

$(\mathbb{Z}, *)$ is an Abelian group.

Teacher's Signature

Notes

Q. 4

Let G be the set of all positive rational numbers and $*$ be the binary operations on G defined by $a*b = \frac{ab}{7}$ $\forall a, b \in G$. Prove that $(G, *)$ is an abelian group. Also solve $3*x = 2^{-1}$ in G

(4) Let G1: $a, b \in G$, $a*b = \frac{ab}{7} \in G$

Closure Law is satisfied

$\in$

G2: Let $a, b, c \in G$ then

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

$\Rightarrow a*\left(\frac{bc}{7}\right)$ $\quad [\because b*c = \frac{bc}{7}]$

$\Rightarrow \left[\frac{abc}{7}\right]$ $\quad [\because a*\left(\frac{bc}{7}\right) = \frac{abc}{7}]$

RHS $= (a*b)*c$

$= \left(\frac{ab}{7}\right)*c$

$= \frac{abc}{7}$

LHS = RHS

Associativity Law is valid

Teacher's Signature

Notes

G3: Let $a \in G$, e be the Identity $\forall a$

$\Rightarrow a * e = e * a = a$

$\Rightarrow \frac{ae}{7} = \frac{ea}{7} = a$

$\Rightarrow \frac{ae}{7} = a$

$\Rightarrow \boxed{e = 7}$

$\therefore$ Identity exist

G4: Let $a \in G$, $a^{-1} \in G$ then

$a * a^{-1} = a^{-1} * a = e$

$\Rightarrow a * a^{-1} = a^{-1} * a = 7 \quad [\because e = 7]$

$\Rightarrow \frac{aa^{-1}}{7} = \frac{a^{-1}a}{7} = 7$

$\Rightarrow \boxed{\begin{array}{l} a a^{-1} = \frac{49}{a} \\ a^{-1} a = \frac{49}{a} \end{array}} \quad \in Q^+$

Inverse also exists

G5: Let $a, b \in \mathbb{Z}$.

$a * b = b * a$

$\Rightarrow \boxed{\frac{ab}{7} = \frac{ba}{7}} \quad \in Q^+$

$\therefore$ Commutative Law is satisfied.

Teacher's Signature

$3 * x = 2^{-1}$

$\frac{3x}{4} = \frac{49}{2}$ $\quad [\because aa^{-1} = 4a \Rightarrow a^{-1} = \frac{49}{a}]$

$\Rightarrow x = \frac{1343}{6}$

Q5) Let $Q - \{3\}$ be the set of all rational nos except 3 with binary operation $*$ defined by $a * b = a + b - ab \quad \forall a, b \in Q - \{3\}$. Show that $Q - \{3\}$ is an abelian group. Solve $5 * x = 3$ in $Q - \{3\}$.

Proof

Let G1: $a, b \in Q$ then

$a * b = a + b - ab \in Q - \{3\}$

Closure law is satisfied

G2: Let $a, b, c \in Q - \{3\}$ then

LHS $\rightarrow a * (b * c) = (a * b) * c$

$\Rightarrow a * (b + c - bc) \quad [\because b * c = b + c - bc]$

$\Rightarrow a + b + c - bc - a(b + c - bc)$

$\Rightarrow a + b + c - bc - ab - ac + abc$

RHS: $(a * b) * c$

$\Rightarrow (a + b - ab) * c$

$\Rightarrow (a + b - ab) + c - (a + b - ab)c$

$\Rightarrow a + b + c - ab - ac - bc + abc$

LHS = RHS

Associativity Law satisfied.

Teacher's Signature

Notes

Q3: Let $a \in (Q-\{1\})$ then e be the identity of a, $e \in (Q-\{1\})$

$\Rightarrow a * e = e * a = a$

$\Rightarrow a + e - ae = e + a - ea = a$

$\Rightarrow a + e - ae = a$

$e(1-a) = 0$

$e = 0$ | $a \neq 1$

Identity exists

Q4: Let $a \in (Q-\{1\})$, $a^{-1} \in (Q-\{1\})$ then

$a * a^{-1} = a^{-1} * a = e$

$\Rightarrow a + a^{-1} - aa^{-1} = a^{-1} + a - a^{-1}a = 0$

$\Rightarrow a + a^{-1} - aa^{-1} = 0$

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

$\Rightarrow a^{-1} = \frac{-a}{1-a}$

$\Rightarrow \boxed{a^{-1} = \frac{a}{a-1}}$

~~$a^{-1} * a = e$~~ $\boxed{a^{-1} = -\frac{a}{1-a}}$

Inverse exists.

Q5:- Let $a, b \in (Q-\{1\})$ then

$a * b = b * a$

$\Rightarrow a + b - ab = b + a - ba$

$\Rightarrow$ Commutative law is valid

$(Q-\{1\}, *)$ is an Abelian group.

Teacher's Signature

$ax_1 = b$ & $ax_2 = b$

$ax_1 = ax_2$

$x_1 = x_2$ [By Left Cancellation Law]

Therefore the soln of $ax = b$ is unique in G.

Subgroups

→ A non-empty subset H of a group G is called subgroup of G if

(i) H is stable (closed) for the composition defined on G i.e

$a \in H, b \in H \Rightarrow ab \in H$

(ii) H itself is a group for the composition induced by that of G.

Teacher's Signature

Notes

Page No.:
Date: / /

Proper & improper (or Trivial) Subgroup:

→ Every group G of order greater than 1 has at least two subgroups which are

(i) G (itself)
(ii) {e} is the group of the identity alone.

→ The above two subgroups are known as improper or trivial subgroups.

Subgroup other than these two is known a proper subgroup.

Important Remark

→ If any subset of the group G is a group for any operation other than the composition of G, then it is not called a subgroup of G.

→ For ex: the group {1, -1} is a part of (C, +) which is group for the multiplication but not for the composition (+) of the base group.
Therefore, this is not the subgroup of (C, +)

$$N \leq Z \leq Q \leq R \leq C$$

Page No.:
Date: / /

Notes

Ex

(I) Additive groups

Ex 1 $(Z,+)$ is a subgroup of $(Q,+)$
is $(Q,+)$ is a subgroup $(R,+)$

Ex 3 :- The set mZ of multiples of some given integer m is a sub group of $(Z,+)$

Ex-4 The group $\{0,4\}$ is a subgroup $(Z_8,+)$

(II) Multiplicative groups

Ex 1 : $(Q^+,\times)$ is a subgroup of $(R^+,\times)$

Ex 2 : $\{1,-1\}$, $\{1,\omega,\omega^2\}$, $\{1,-1,i,-i\}$ are subgroups of $(C_0,\times)$ the group of non-zero complex no.s.

Ex 3) For multiplication operation $\{1,-1,\times\}$ is a subgroup of $\{1,-1,i,-i\}$.

Teacher's Signature

Notes

Theorem - 3

If H is a subgroup of a G, then

a) the identity of H is the same as that of G

b) the inverse of any element a of H is the same as the inverse of same regarded as an element of G.

c) the order of any element a of H is the same as the order of a in G

Proof:

a) Let a e & e' be the identities of G & H respectively.

If a ∈ H, then $ae' = e'a = a$ — (1)

Again $a \in H \Rightarrow a \in G$

$ae = ea = a$ — (2)

From (1) & (2)

$ae' = ae$ [By Cancellation Law]

$e' = e$ A.P

b) Let a ∈ H & b & c is inverse of a & if e is identity of G & H

$ab = ba = e$

$ac = ca = e$

$ab = ac$ Inverse are equal

$b = c$

Teacher's Signature

Notes

Page No.:
Date: / /

Cf Let the order of $a \in H$ be m & n in H & G respectively. e_H & e be the identity, then by definition of order.

$$a^m = e \quad , a^n = e \Rightarrow a^m = a^n$$
$$a^m a^{-n} = a^n a^{-n} = a^0$$
$$a^{m-n} = a^0$$
$$m - n = 0 \quad [\because m - n < m = O(a) \text{ in } H$$
$$m = n \quad \{m - n < n = O(a) \text{ in } G\}$$

Therefore the order of any element of sub-groups is the same as that of the subgroups & the original group.

In the light of the above results, we conclude that a subset of H of a group G is a subgroup iff:

I. $a \in H, b \in H \Rightarrow ab \in H$

II. $e \in H$ where e is the identity of G

III. $a \in H \exists a^{-1} \in H$ where a^{-1} is the inverse of a in G

Teacher's Signature

Notes

Page No.:
Date: / /

Theorem-2

A non-void subset H of a group G is a subgroup iff

$a \in H, b \in H \Rightarrow ab^{-1} \in H$

Proof: ($\Rightarrow$) Let H be a subgroup of the group G. $a, b \in H$

then $b \in H \Rightarrow b^{-1} \in H$ [by existence of inverse in G]

$\therefore a \in H, b \in H \Rightarrow a \in H, b^{-1} \in H$

$\Rightarrow ab^{-1} \in H$ [by closure property in H]

Therefore if H is a sub group of G, then the cond^n is necessary.

Conversely ($\Leftarrow$): Suppose the given cond^n is true in H, then we shall prove that H will be a sub-group

$\therefore H \neq \phi \therefore$ Let $a \in H$

Therefore identity exists in H.

Again by definition: $e \in H, a^{-1} \in H \Rightarrow ea^{-1} = a^{-1} \in H$

Thus the inverse of every element exists in H

Finally, $a \in H, b \in H \Rightarrow a \in H, b^{-1} \in H$

$\Rightarrow a(b^{-1})^{-1} = ab \in H$

H is closed for the operation of G.

Teacher's Signature

Notes

Page No.:
Date: / /

Therefore H is a subgroup of G which proves that the given condition is sufficient for H to be a sub-group

Theorem 3

A non-void finite subset H of a group G is a subgroup iff
$a \in H, b \in H \Rightarrow ab \in H$

Proof: ($\Rightarrow$) Let H be a finite subgroup of the group G, then H will be closed for the operation of G

$\therefore a \in H, b \in H \Rightarrow ab \in H$

Conversely ($\Leftarrow$): If $a \in H, b \in H \Rightarrow ab \in H$

Then $a \in H \Rightarrow aa = a^2 \in H$

Again $a \in H, a^2 \in H \Rightarrow aa^2 = a^3 \in H$

Thus we will see that $a^{n-1} \in H, a \in H$
$\Rightarrow a^n \in H \quad \forall n \in N$

Therefore $a, a^2, a^3, \ldots a^n \ldots$ are all element of H. But H is a finite subset of G, so all the powers of a cannot be distinct

Teacher's Signature

Page No.:
Date: / /

Notes

Let $a^i = a^j$, $i > j$

$\Rightarrow a^i a^{-j} = a^j a^{-j}$ [Multiplying by a^{-j} on both sides]

$\Rightarrow a^{i-j} = a^0 = e$ [$\because a^i \in H \Rightarrow (a^i)^{-1} = a^{-i} \in H$]

$\Rightarrow a^{i-j} = e$ where e is the identity of G

$\Rightarrow a^r = e \in H$ [$\because i - j = r \in N, r > 0$]

Therefore identity element exists in H

Again $a^{r-1} \in H \Rightarrow a^r a^{-1} \in H$

$\Rightarrow e a^{-1} = a^{-1} \in H$

Thus each element of H has its inverse in H.

Hence H is a subgroup of G