Degree Part 2

ABSTRACT/MODERN ALGEBRA

Group

Define Group →

A non-empty set G with a binary operation "o" is called a group (G, o) if the binary operation satisfies the following laws

(i) Closure law :→ G is closed under the binary operation 'o'
i.e. $a \circ b \in G$ for all $a, b \in G$ [closure axiom]

(ii) Associative law :→ The associative law is satisfied
i.e. $a(ob)oc = ao(boc)$ for all $a, b, c \in G$. [Associative axiom]

(iii) Existence of identity element :→
There exists an element $e \in G$ such that $aoe = eoa = a \; \forall$ (for all) $e \in G$ [Identity axiom]

(iv) Existence of inverse elements :→
The inverse elements of all the elements of G exist i.e. for every $a \in G$ there exists an element $b \in G$ such that $aob = boa = e$, e being the inverse element.
The inverse element of a is denoted by $\bar{a}^1$ and so $aoa^{-1} = \bar{a}^1 oa = e$ [Inverse axiom]

Abelian or Commutative Group

A group G is said to be abelian or commutative group if it satisfies the commutative axiom

i.e. $a \circ b = b \circ a$, $\forall$ [forall] $a, b \in G$

Note → If the group G does not satisfy the commutative axiom i.e. $a \circ b = b \circ a$, for all $a, b \in G$ then G is called nonabelian group.

Ex → Group

(a) The set R of real numbers is a group under the binary operation '+' (addition)
i.e. $(R, +)$ is a group.

(b) The set R of real numbers is a group under the binary operation '×' (multiplication)
i.e. $(R, \times)$ is a group.

Q4) Show that the set I of all integers $\ldots -4, -3, -2, -1, 0, 1, 2, 3, 4, \ldots$ is a group with respect to the operation of addition of integers.

Ans → Set I with operation addition '+' is a group if it satisfies the following conditions.

(a) Closure :→ As the sum of two integers is also an integer i.e. $a+b \in I$ $\forall a, b \in I$ so I satisfies the closure law.

(b) Associative → As the addition of integers is an associative composition.
$a + (b+c) = (a+b) + c$, $\forall a, b, c \in I$.

Ex 3

(c) Identity → The number $0 \in I$.
Also $0 + a = a = a + 0 \quad \forall\, a \in I$
so, the integer 0 is the identity.

(d) Inverse → If $a \in I$
then $-a \in I$
Also we have
~~$a + (-a) = (-a) + a = 0 \quad \forall\, a \in I$~~
$(-a) + a = 0 = a + (-a)$. So every integer possesses additive inverse.

So we find that I is a group with respect to addition.

Some Definitions

(1) Quasi-group or Groupoid → A nonempty set G together with a binary operation '$\circ$' is called a quasi-group or groupoid $(G, \circ)$ if G is closed under '$\circ$'.

(2) Semigroup → A groupoid $(G, \circ)$ is called a semigroup if the associative law holds.

(3) Monoid → A semigroup $(G, \circ)$ is called a monoid if the identity element exists.

So we see that a monoid $(G, \circ)$ is called a group if inverse element for each element of G exists.

404

Define a finite group with example.

A group is called a finite group if the number of elements in the group is finite. The number of elements in a finite group is called the order of the group.

Ex (a) $\{1, -1, i, -i\}$ is a finite group under operation multiplication

(b) $\{1, w, w^2\}$ is a finite group with respect to multiplication. Here w is one of the imaginary cube roots of Unity.

Definite an infinite group with example.

If a group Contains an infinite number of elements then the group is called an infinite group.

Ex (a) The set of all integers is an infinite group under operation addition.

(b) The set of all nonzero rational numbers forms an infinite group under the familiar operation of multiplication of rational numbers.

Some important theorems

Group

(4) **Uniqueness of identity element**

Prove that the identity element in a group is unique.

Proof → Let G be a group and e be its identity element.

Suppose that e is not unique.

Let e' be another identity element of the group

Now we have

$a \circ e = e \circ a = a$ ....(1) $\forall a \in G$ [when e is identity]

again $a \circ e' = e' \circ a = a$ ..(2) $\forall a \in G$ [when e' is identity]

Since (1) is true $\forall a \in G$ and $e' \in G$

So putting $a = e'$ in (1) we get

$$e' \circ e = e \circ e' = e' \quad \text{..(3)}$$

Similarly putting $a = e$ in (2) we get

$$e \circ e' = e' \circ e = e \quad \text{..(4)}$$

from (3) & (4) we get

$$e' = e$$

So it Contradicts our assumption that $e' \neq e$

Hence our suppositin is not true.

Thus the identity element in a group is unique.

406

Uniqueness of Inverse element.

(*) Prove that the inverse elements of an element in a group is unique.

Proof → Let a be any element of a group G with e as an identity element.

Suppose that b and c are two inverse elements of a

then $boa = e = a \circ b$ ... (1)

& $coa = e = a \circ c$ ... (2)

Again → by associative law of group.

$b \circ (a \circ c) = (b \circ a) \circ c$

or $b \circ e = e \circ c$ [using (1) & (2)]

or $b = c$

So we conclude that inverse elements of an element in a grp is unique.

(*) Show that if every element of a group is its own inverse then the group is abelian.

Proof → Let $a, b \in G$, where G is a grp

then $ab \in G$

given that $(ab)^{-1} = ab$ ... (1)

But we know in any grp

$(ab)^{-1} = b^{-1}a^{-1}$ ... (2)

40?

from ① & ②

$ab = b^{-1}a^{-1}$

also $a^{-1} = a$ [As every element is its own inverse]

and $b^{-1} = b$

$\therefore ab = ba$

So the group is abelian.

Reversal rule

Prove that $(ab)^{-1} = b^{-1}a^{-1}$, $a, b \in G$

(or)

Prove that the inverse of the product of two elements of group, is the product of the inverses of the elements in the reverse order.

Proof → we have

$(ab)(b^{-1}a^{-1}) = [(ab)b^{-1}]a^{-1}$ [Associative axiom]

$= [a(bb^{-1})]a^{-1}$ [Associative axiom]

$= [ae]a^{-1}$ [existence of inverse element]

$= aa^{-1}$ [existence of identity element]

$= e$ [inverse element]

So, $(ab)(b^{-1}a^{-1}) = e$

Again → $(b^{-1}a^{-1})(ab) = b^{-1}[a^{-1}(ab)]$ [Associative axiom]

$= b^{-1}[(a^{-1}a)b]$ ["]

$= b^{-1}(eb)$ [existence of inverse elements]

$= b^{-1}b$ [" " identity "]

$= e$ [" " inverse "]

Thus we proved that $(ab)(b^{-1}a^{-1}) = (b^{-1}a^{-1})(ab) = e$

408 So by definition of inverse axiom of group, $(ab)^{-1} = b^{-1}a^{-1}$

So the inverse of product of two elements of a group is the product of the inverses of the elements in the reverse order.

(☆) Prove that $(ab)^2 = a^2b^2$ $\forall\, a, b \in G$ which is a group $\Leftrightarrow$ G is an abelian group

Proof Let in a group G

$(ab)^2 = a^2b^2$

or $(ab)(ab) = (aa)(bb)$

or $\bar{a}^1\{(ab)(ab)\} = \bar{a}^1\{(aa)(bb)\}$

or $(\bar{a}^1a)\{b(ab)\} = (\bar{a}^1a)\{a(bb)\}$ [Associative law]

or $e\{b(ab)\} = e\{a(bb)\}$ [$\because \bar{a}a = e$, e is the identity element]

or $b(ab) = a(bb)$ [identity element]

or $(ba)b = (ab)b$ [By associative law]

or $ba = ab$ [By the right Cancellation law]

So G is abelian.

Again Let G be an abelian group then $ab = ba$ $\forall\, a, b \in G$

Now, $(ab)^2 = (ab)(ab)$

$= a(ba)b$ [Associative law]

$= a(ab)b$ [$\because ab = ba$]

$= (aa)(bb)$

or $(ab)^2 = a^2b^2$