WELCOME

WELCOME
TO
PITHAPUR RAJAH'S GOVERNMENT COLLEGE(A)
KAKINADA

DEPARTMENT OF MATHEMATICS

G.SYAM PRASAD

M.Sc.,M.Phil.,B.Ed.,APSET

Lecturer in Mathematics

GROUP THEORY

GROUP THEORY

Binary Operation :

Let S be a non-empty set. If f: S x S → S is a mapping, then f is called binary operation or binary composition in S or on S.

Thus if a relation in S such that every pair (distinct or equal) of elements of S taken in definite order is associated with a unique element of S then it is called a binary operation in S. Otherwise the relation is not binary operation in S and the relation is simply an operation in S.

Symbolism :

- For a,b ϵ S => a + b ϵ S then "+ " is a binary operation in S.
- For a,b ϵ S => a • b ϵ S then "• " is a binary operation in S.
- For a,b ϵ S => a○b ϵ S then " ○ "is a binary operation in S.
- This also called **closure law**.

Ex : 1. + , • are binary operations in N , since for a,b ϵ N => a + b ϵ N and a • b ϵ N . In other words N is said to be closed w.r.t the operation '+ ' and ' • '

2. the operations subtraction (-) and division (÷) are not binary operations in N for 3, 5 ϵ N does not imply 3-5ϵ N and 3/5 ϵ N.

Algebraic Structure :

A non-empty set G equipped with one or more binary operations is called an algebraic structure or an algebraic system .

If ' ○ ' is a binary operation on G , then the algebraic structure is written as (G,○).

Ex: (N,+), (Q,-), (R,+) are algebraic structure.

Associative Law :

' ○ ' is a binary operation in a set S. If for a,b,c ϵ S , $(a \circ b) \circ c = a \circ (b \circ c)$ then ' ○ ' is said to be associative in S . This is called Associative law . Otherwise ' ○ ' is said to be not associative in S .

Ex: 1. '+ ' and ' . ' are associative in N since for a,b,c ϵ N, $(a+b)+c = a+(b+ c)$ and $a(bc)=(ab)c$.

2. '○' is a composition in R such that $a \circ b = a+3b$ for a,b ϵ R. Then '○' is not associative in R.

Identity Element :

Let S be a non-empty set and '○' be a binary operation on S.

1. If there exists an element e_1 ϵ S such that $e_1 \circ a=a$ for a ϵ S then e_1 is called a left identity of S w.r.t. the operation '○'

2. If there exists an element $e_2 \in S$ such that $a \circ e_2 = a$ for $a \in S$ then e_2 is called a right identity of S w.r.t. the operation '$\circ$' .

3. If there exists an element $e \in S$ such that e is both left and a right identity of S w.r.t. '$\circ$' , then e is called an identity of S .

Ex: 1.In the algebraic system (Z,+), the number 0 is an identity element.

2. In the algebraic system (R, •), the number 1 is an identity element.

Invertible Element :

Let (S,$\circ$) be an algebraic structure with the identity element e in S w.r.t. '$\circ$'.

i) An element $a \in S$ is said to be left invertible or left regular if there exists an element $x \in S$ such that $x \circ a = e$. x is called a left inverse of a, w.r.t. '$\circ$' .

ii) An element a ϵ S is said to be right invertible or right regular if there exists an element y ϵ S such that a○y = e . y is called a right inverse of a, w.r.t. '○' .

Iii) An element x which is both a left inverse and a right inverse of 'a' is called an inverse of 'a' and 'a' is said to be invertible or regular.

Semi Group :

An Algebraic structure (S,○) is called a semi Group if the binary operation '○' is associative in S .

Ex: 1. (N,+) is a semi Group. For a,b ϵ N => a + b ϵ N and (a+b)+c = a+(b+ c) .

2. (Q,-) is not a semi Group . For 5, 3/2, 1 ϵ Q does not imply {5-(3/2) } -1 = 5- {(3/2)-1}.

Monoid:

A semi Group (S,○) with the identity element w.r.t. '○' is known as a monoid. i.e (S,○) is a monoid if S is a non-empty set and '○' a binary operation in S such that '○' is associative and there exists an identity element w.r.t. '○' .

Ex: 1. (Z,+) is a monoid and the identity element is 0.

2. (Z,.) is a monoid and the identity element is 1.

Group:

If G is a non-empty set and '○' is a binary operation defined on G such that the following three laws are Satisfied then (G,○) is a group.

i). Associative law

ii). Identity law

iii). Inverse law.

Ex : (Z,+), (Q,+), (R,+), (C,+) are all groups.

Note :

i) A group is an algebraic structure. It can also be written by $< G,\circ >$.

Ii) A semi group ($G,\circ$) is a group if identity law and inverse law are satisfied.

Iii) A monoid ($G,\circ$) is a group if inverse law is satisfied.

Abelian Group or Commutative Group :

For the Group $a,b \in G$, $a\circ b = b\circ a$ is satisfied , then ($G,\circ$) is called an abelian group or a commutative group.

Ex : ($Z,+$) is a commutative group.

Finite and Infinite Group :

If the set G contains a finite number of elements then the group ($G,\circ$) is called a finite group.

Otherwise the group ($G,\circ$) is called an infinite group.

Order of a Group :

The number of elements in a finite group (G,○) is called the order of the group and is denoted by O(G). If G is infinite , then we say that the order of G is infinite.

Thus : i) If the number of elements in a group G is n, then $O(G) = n$.

ii) If the group G is finite we some times write $O(G) < \infty$.

iii) If $O(G) = 2n$, $n \in N$,we say that the group is of even order.

iv) If $O(G) = 2n-1$, $n \in N$ we say that the group is of odd order.

Cancellation Laws :

Let S be non-empty set and ○ be binary operation on S.

For $a,b,c \in S$,

i) $a \circ b = a \circ c \Rightarrow b = c$ (is called left cancelation law)

ii) $b \circ a = c \circ a \Rightarrow b = c$ (is called Right cancelation law)

i) and (ii) are called cancelation laws.

Theorem :

In a group G, identity element is unique.

Proof:

If possible let e_1 , e_2 be two identity elements in the group ($G, \circ$).

Therefore $e_1 \circ e_2 = e_2 \circ e_1 = e_2$ is an identity in G.......... (i)

And $e_2 \circ e_1 = e_1 \circ e_2 = e_1$ is an identity in .... (ii)

Therefore from (i) and (ii) we get $e_1 = e_2$

Hence identity element is unique.

Theorem :

In a group G, inverse of any element is unique.

Proof:

Let e be the identity element in the group $(G, \bullet)$.

If $a \in G$ then a will have an inverse.

If possible , let $b, c \in G$ be two inverses of a in G.

Therefore $a.b = b.a = e$ and $a.c = c.a = e$.

Now $c.(a.b) = c.e = c$ .... (i)

And $c.(a.b) = (c.a).b = e.b = b$ ....(ii)

From (i) and (ii) we get $b = c$.

Therefore inverse of any element is unique.

1. Show that set Q_+ of all +ve rational numbers forms an abelian group under the composition defined by * such that $a*b = ab/3$ for $a,b \in Q_+$.

Sol :

Let Q_+ is the set of all +ve rational numbers and for $a,b \in Q_+$.

We have the operation * such that $a*b = ab / 3$.

We now prove that $(Q_+ , *)$ is an abelian group .

Closure law :

Let $a,b \in Q_+$. Then $a*b = ab / 3 \in Q_+$

Therefore * is a binary operation in Q_+ .

Associative law :

Let $a , b , c \in Q_+$.

Now $a*(b*c) = a*(bc/3) = a(bc/3) / 3 = abc / 9$

and $(a*b)*c = (ab /3)*c = (ab/3)c / 3 = abc / 9$

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

Therefore * is associative on Q_+ .

Existence of identity :

Let $a \in Q_+$ and $e \in Q_+$ such that $a*e = e*a = a$.

Now $a*e = a \Longrightarrow ae / 3 = a$

$\Longrightarrow a(e-3)=0 \quad \Longrightarrow e-3 = 0 \Longrightarrow e = 3 \in Q_+$

Clearly $a*e = a*3 = (a \times 3) / 3 = a$

Therefore " e " is an element in Q_+ such that

$a*e = e*a = a$

Therefore $e =3$ is the identity element in Q_+ .

Existence of inverse :

Let $a \in Q_+$ and $b \in Q_+$ such that $a*b = b*a = e$.

Now $a*b = e \Longrightarrow ab / 3 = e \Longrightarrow b = 3e / a = 9/a$.

Therefore for every $a \in Q_+$ there exists $b = 9/a \in Q_+$ such that $a*b = b*a = e$.

Therefore "a" has inverse in Q_+ .

Commutative :

For $a , b \in Q_+ \Longrightarrow a*b = b*a$.

Since $a*b = ab/ 3 = ba /3 = b*a$.

Therefore " * " is commutative in Q_+ .

Hence $(Q_+ , *)$ is an abelian group .

Theorem:

Prove that cancellation laws holds in a group .

Let G be a group . Then for a , b , c $\in$ G ; ab = ac $\Longrightarrow$ b = c and ba = ca $\Longrightarrow$ b=c.

Proof:

Let G be a group and e be the identity in G .

For a , b , c $\in$ G , ab = ac $\Longrightarrow a^{-1}(ab) = a^{-1}(ac)$

$\Longrightarrow (a^{-1}a)b = (a^{-1}a)c$

$\Longrightarrow eb = ec$

$\Longrightarrow b = c$

$\Longrightarrow$ left cancellation law

Similarly $ba = ca \Longrightarrow (ba)a^{-1} = (ca)a^{-1}$

$\Longrightarrow b(aa^{-1}) = c(aa^{-1})$

$\Longrightarrow be = ce$

$\Longrightarrow b = c$

$\Longrightarrow$ right cancellation law

Therefore for a , b , $c \in G$;

$ab = ac \Longrightarrow b = c$ (left Cancellation law)

and $ba = ca \Longrightarrow b=c$ (right Cancellation law)

Therefore cancellation laws holds in a group .

Theorem:

If every element of a group $(G , \cdot)$ is its own inverse , show that $(G,\cdot)$ is an abelian group .

Proof:

Given $(G , \cdot)$ is a group .

Let $a , b \in G$. By hypothesis $a^{-1} = a$ and $b^{-1} = b$.

Then $ab \in G$ and hence $(ab)^{-1} = ab$.

Now $(ab)^{-1} = ab \Longrightarrow b^{-1}a^{-1} = ab$

$\Longrightarrow ba = ab$

$\Longrightarrow (G,\cdot)$ is an abelian group .

Theorem:

In a group G for a,b $\in$ G,

$(ab)^2 = a^2b^2 \Leftrightarrow$ G is abelian.

Proof:

Case:1

Let a , b $\in$ G and $(ab)^2 = a^2b^2$

To prove that G is abelian .

Now $(ab)^2 = a^2b^2 \Longrightarrow (ab)(ab)=(aa)(bb)$

$\Longrightarrow a(ab)b = a(ab)b$

$\Longrightarrow ba = ab$

$\Longrightarrow$ G is abelian

Case: 2

Let G be abelian

To prove that $(ab)^2 = a^2b^2$

Now $(ab)^2 = (ab)(ab) = a(ba)b = a(ab)b = (aa)(bb) = a^2b^2$.

Therefore $(ab)^2 = a^2b^2 \Leftrightarrow$ G is abelian .