Date.
Page.

Groups

If there exist a system such that it consists of a non-empty set & one or more operations on that set, then system is said to be an algebraic structure.

It is denoted by $(A, op_1, op_2 \cdots op_n)$ where A is non Empty Set & $op_1, op_2 \cdots op_n$ are operations.

~~An algebraic~~

Binary operation

Consider a non Empty set A & a function $f: A \times A \to A$ is called binary operation on A.

If $*$ is a binary operation on A then it written as $a*b$.

A binary operation can be denoted as $+, -, *, \oplus, \Delta$ etc.

* Operation of addition is a binary operation on set of natural no.'s

* The operation of Sustraction is a binary operation on set of int but not on natural no's as Sustraction of natural no may or may not be natural no

* The operation of multiplication is a binary operation on set of natural no, integers etc..

E.g. $A = \{1, 2, 3\}$ & $*$ is a binary operation on A as $a*b = 2a+2b$ Represent operation $*$ as table of A.

Sol

*	1	2	3
1	4	6	8
2	6	8	10
3	8	10	12

Properties of Binary operation

Closure property: Consider a non-Empty Set A and a binary operation $*$ on A. Then A is closed under operation $*$, if $a*b \in A$, where a and b are Elements of A.

for E.g. the operation of addition on Set of integers is a closed operation i.e. if $a, b \in Z$ then $a+b \in Z \; \forall \; a, b \in Z$.

Associative property: consider non-empty set A & a binary operation * on A then operation * on A is associative if $\forall\ a, b, c \in A$

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

e.g. Consider binary operation * on Q, set of rational no., defined by

$$a*b = a+b-ab \quad \forall\ a, b \in Q$$

Let $a, b, c \in Q$

$$(a*b)*c = (a+b-ab)*c$$
$$= a+b-ab+c-(a+b-ab)c$$
$$= a+b-ab+c-ac-bc+abc$$
$$= a+b+c-ab-bc-ac+abc$$

Now $a*(b*c) = a*(b+c-bc)$
$$= a+b+c-bc-a(b+c-bc)$$
$$= a+b+c-ab-bc-ac+abc$$

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

Commutative property :- Consider a non-empty set A and binary operation * on A then

$$a*b = b*a \quad \forall\ a, b \in A$$

Date.
Page.

Identity: Consider a non Empty set A & a binary operation * on A. then operation * has identity Element / property if there exist an Element e, in A such that

$a * e = a = e * a \quad \forall\ a \in A$

$a * e = a$ → Right identity

$e * a = a$ → Left identity

Q) Consider binary operation * on I_+, the set of +ve integers defined by $a * b = \frac{ab}{2}$. Determine identity for binary operation * if exists.

Sol Let us take a +ve no. e, then

$e * a = a, \quad a \in I_+$

$\Rightarrow \frac{ea}{2} = a$

$\Rightarrow \boxed{e = 2} \quad \rightarrow (1)$

Also $a * e = a; \quad a \in I_+$

$\frac{ae}{2} = a$

$\Rightarrow \boxed{e = 2} \quad \rightarrow (2)$

from (1) & (2) $e * a = a = a * e$

$\therefore$ 2 is Identity Element for binary operation *.

Date.
Page.

Semi-group → consider an algebraic system $(A, *)$ where $*$ is a binary operation on A. Then $(A, *)$ is semi-group if

i) The operation $*$ is closed operation on set A.
ii) The operation $*$ is an associative operation.

Monoid: Let us consider an algebraic system (A, o) where o is a binary operation on A. then (A, o) is said to be monoid if it satisfies following conditions:

i) The operation o is closed operation on set A.
ii) The operation o is an associative operation
iii) There exists an identity element wrt operation o.

Inverse: consider a non empty set A and a binary operation $*$ on A. then operation has inverse property if $\forall a \in A$ $\exists$ an element b in A s.t.

$$a * b = b * a = e$$ where b is called inverse of a.

Group: Consider an algebraic System $(G, *)$ where $*$ is binary operation on G. then System $(G, *)$ is said to be group if it satisfies following properties:

(i) operation $*$ is closed operation
ii) operation $*$ is an associative operation.
iii) $\exists$ an identity Element wrt operation $*$.
iv) $\forall\ a \in G$, $\exists$ an element $\bar{a} \in G$ st.

$$\bar{a}^{-1} * a = a * \bar{a}^{-1} = e.$$

for e.g. Algebraic System $(I, +)$ where I is set of integers and $+$ is an addition operation. is a group.
The element 0 is identity Element w.r.t operation $+$.
The Inverse of Every Element $a \in I$ is $-a \in I$.

Q) Determine whether algebraic system $(Q, +)$ is a group where Q is set of all rational numbers and $+$ is an addition operation.

Sol:

Closure property :→ The set Q is closed under $+$ as addition of two rational no's is a rational no.

Date.
Page.

Associative property: The operation + is associative as $a+(b+c) = (a+b)+c$
$\forall\ a,b,c \in Q$.

Identity → Element 0 is identity element hence $a+0 = a = 0+a\ \forall\ a \in Q$.

Inverse: the inverse of every Element $a \in Q$ is $-a \in Q$. Hence inverse of every Element exists.
Since algebraic system $(Q,+)$ satisfies all the properties of group.
Hence $(Q,+)$ is a group.

Q) Prove that $G = \{1, 2, 3, 4, 5, 6\}$ is a finite abelian group of order 6 under multiplication modulo 7.

Sol $G = \{1, 2, 3, 4, 5, 6\}$

X_7	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

Date
Page

from table it is clear that Each Element in table is also an Element of G.
∴ G is closed under multiplication modulo 7.

ii) Also $\forall\ a, b, c \in G$
$a \times_7 (b \times_7 c) = (a \times_7 b) \times_7 c$ i.e. associative law holds.

iii) We observe first 1st row inside the table is identical; with top row of table.
∴ 1 is identity of G.

iv) Again $2 \times_7 4 = 1$
$3 \times_7 5 = 1$
$4 \times_7 2 = 1$
$5 \times_7 3 = 1$
$6 \times_7 6 = 1$
Hence Each Element of G has inverse.
i.e. inverse of 2 is 4 & of 4 is 2.
inverse of 3 is 5 & of 5 is 3
Inverse of 6 is 6.

∴ Hence G is a group under multiplication modulo 7.

Date.
Page.

Th^m: Show that identity Element in a group is unique.

Pf: Let us assume that there exists two identity elements i.e. e & e' of G.

Since $e \in G$ & e' is an identity

$\therefore e'e = ee' = e \rightarrow (1)$

Also $e' \in G$ & e is an identity

$\therefore e'e = ee' = e' \rightarrow (2)$

$\therefore e = e'$ [from (1) & (2)]

Hence identity in a group is unique.

Th^m Show that inverse of an Element a in a group G is unique.

Sol. Let $a \in G$ be an Element. Let $\vec{a}_1$ & $\vec{a}_2$ be two inverse Elements of a

$\therefore \vec{a}_1 a = a\vec{a}_1 = e$ &

$\vec{a}_2 a = a\vec{a}_2 = e$

Now $\vec{a}_1 = \vec{a}_1 e = \vec{a}_1 (a\vec{a}_2)$

$= (\vec{a}_1 a)\vec{a}_2$

$= e\,\vec{a}_2$

$= \vec{a}_2$

i.e. $\vec{a}_1 = \vec{a}_2$ so inverse of an Element is unique

Left Cancellation Law:

$ab = ac \Rightarrow b = c \quad \forall\ a, b, c \in G$

Right cancellation law:

$ba = ca \Rightarrow b = c \quad \forall\ a, b, c \in G$.

Subgroup :→ Let us Consider a group $(G, *)$ Also let $S \subseteq G$; then $(S, *)$ is Called Subgroup iff it satisfies foll. Conditions:

i) operation $*$ is closed operation on S.
ii) operation $*$ is an associative operation.
iii) As e is Identity element of G. It must belong to S.
Identity Element of $(G, *)$ must belong to $(S, *)$.
iv) $\forall\ a \in S$, a^{-1} also belongs to S.

for e.g. $(G, +)$ be a group. where G is set of all integers an $(+)$ is an addition operation. Then $(H, +)$ is subgroup of group G where $H = \{2m : m \in G\}$ the set of all Even integers.

Th^{m} A subset H of a group G is a subgroup iff
(i) the Identity element $e \in H$
ii) H is closed under same operation as in G

Date.
Page.

iii) H is closed under inverse i.e.
If $a \in H$ then $\vec{a} \in H$.

or A subset H of group G is a subgroup of G iff $a * \vec{b} \in H$.

Pf. Since G is a group & H is a subset of G.
let H is a subgroup of G then by def of subgroup (i), ii), iii) are true.

Converse: let (i), (ii), (iii) holds.
We show: H is subgroup of G.
we show the associativity of elements of H.

Let $a, b, c \in G$ & $H \subseteq G$
$\Rightarrow a, b, c \in H$
Since elements of G are also elements of H
$\therefore$ Associativity holds for H.
Hence the theorem.

Th^{m}. If H and K are two subgroups of G then $H \cap K$ is also subgroup of G.

Pf We know a subset H of group G is subgroup of G iff $a\vec{b} \in H \ \forall \ a, b \in H$.

let $a, b \in H \cap K$
To Prove $a\vec{b} \in H \cap K$.

Let $a \in H \cap K \Rightarrow a \in H$ and $a \in K$

Also $b \in H \cap K \Rightarrow b \in H$ & $b \in K$

Since H is a subgroup of G & $a, b \in H$

$\Rightarrow a\vec{b} \in H$ ∴ (a subset H of gp. G is subgroup of G iff $a\vec{b} \in H$) → (1)

Also K is subgroup of G and $a, b \in K$

$\Rightarrow a\vec{b} \in K$ → (2)

from (1) & (2)

$a\vec{b} \in H \cap K$

∴ $H \cap K$ is also subgroup of G.

Abelian group: Consider algebraic system $(G, *)$ where $*$ is a binary operation on G. then $(G, *)$ is abelian group if it satisfies all the properties of group along with the following property:

(i) The operation $*$ is Commutative

$a * b = b * a \quad a, b \in G$

for eg. Consider algebraic System $(I, +)$

$(I, +)$ is abelian group because it satisfies all properties of group.

Also operation $+$ is Commutative $\forall\ a, b \in I$

Date
Page

Cosets: consider algebraic system $(G, *)$ where $*$ is binary operation. Now if $(G, *)$ be a group & let a is an element of G & $H \subseteq G$ then

left coset $a*H$ of H is set of elements s.t. $a*H = \{a*h;\ h \in H\}$

Right coset $H*a$ of H is set of elements s.t. $H*a = \{h*a;\ h \in H\}$

The subset H is itself a left and right coset since $e*H = H*e = H$.

Q) Let $(I, +)$ is a group where I is a set of all integers & $+$ is an operation and let $H = \{\ldots -4, -2, 0, 2, 4, 6, 8, \ldots\}$ be the subgroup consisting of multiples of 2. Determine all left cosets of H in I.

Sol: There are two distinct left cosets of H in I.

$0+H = \{\ldots -6, -4, -2, 0, 2, 4, 6 \ldots\} = H$

$1+H = \{\ldots -5, -3, -1, 1, 3, 5, 7 \ldots\}$

$2+H = \{\ldots -4, -2, 0, 2, 4 \ldots\} = H$

$3+H = \{\ldots -3, -1, 1, 3, 5 \ldots\} = 1+H$

& so on.

There is no other distinct left coset because any other coset coincides with cosets given above.

Q) Let $G = (I, +)$ be a group, where I is set of integers and $+$ is an addition operation also let $G_1 = \{\ldots -14, -7, 0, 7, 14, 21 \ldots\}$ be a subgroup consisting of multiples of 7. Determine cosets of G_1 in I.

Sol^n: Set I has 7 different cosets (left or right) of G_1 which are shown as below:

$0+H = \{\ldots -14, -7, 0, 7, 14, 21 \ldots\}$
$1+H = \{\ldots -13, -6, 1, 8, 15, 22 \ldots\}$
$2+H = \{\ldots -12, -5, 2, 9, 16, 23 \ldots\}$
$3+H = \{\ldots -11, -4, 3, 10, 17, 24 \ldots\}$
$4+H = \{\ldots -10, -3, 4, 11, 18, 25 \ldots\}$
$5+H = \{\ldots -9, -2, 5, 12, 19, 26 \ldots\}$
$6+H = \{\ldots -8, -1, 6, 13, 20, 27 \ldots\}$
$7+H = \{\ldots -7, 0, 7, 14, 21, 28 \ldots\} = H$

All other cosets will coincides with any one of cosets shown above. So we will not count them.

Th^m: Let H be a subgroup of group G then right cosets ~~ha~~ form a partition of G.
~~any two~~ Or
Any two right (left) cosets in a group G are either disjoint or Equal.

Pf let Ha & Hb be two right cosets & suppose $Ha \cap Hb \neq \phi$
We shall show $Ha = Hb$

Let $x \in Ha \cap Hb$
$\Rightarrow x \in Ha$ & $x \in Hb$
$\Rightarrow x = h_1 a$ & $x = h_2 b$ for $h_1, h_2 \in H$
$\Rightarrow h_1 a = h_2 b \in Hb$
$\Rightarrow h_1 a \in Hb$
$\Rightarrow Ha \subseteq Hb \rightarrow (1)$
Also $h_2 b = h_1 a \in Ha$
$\Rightarrow h_2 b \in Ha$
$\therefore Hb \subseteq Ha \rightarrow (2)$

from (1) & (2)
$Ha = Hb$

Lagrange's theorem

Statement: If G be a finite group & H is a subgroup of G then $O(H) \mid O(G)$

Sol Since H is subgroup of a finite group G.
$\therefore H$ is also finite.
Let $H = \{h_1, h_2 \cdots h_n\}$ where each h_i is distinct.

Consider $Ha = \{h_1a, h_2a \cdots h_na\}$.

We claim all h_ia's are distinct

If $h_ia = h_ja$

$\Rightarrow h_i = h_j$ (Right Cancellation law)

which is a Contraction as all h_i's are distinct.

Hence Ha has distinct elements.

Now G is finite.

$\therefore$ No. of distinct right Cosets of H in G is also finite say k.

let $G = Ha_1 \cup Ha_2 \cup \cdots \cup Ha_k$

$$= \bigcup_{i=1}^{k} Ha_i.$$

$\Rightarrow O(G) =$ No of Elements in Ha_1 + No. of Elements in Ha_2 + $\cdots$ + no. of Elements in Ha_k

$$O(G) = \underbrace{n + n + n + \cdots + n}_{k \text{ times}}$$

$$O(G) = nk$$

$\Rightarrow n \mid O(G)$

$\Rightarrow O(H) \mid O(G)$

Hence the m^{th}