DSTL UNIT-2: Algebraic Structures.

The algebraic structure is a type of non empty set G which is equipped with one or more than one binary operation.

→ Let assume $*$ → binary operation on non empty set G.
In this case $(G, *)$ will be known as the algebraic structure.

→ $(I,-)$, $(I,+)$, $(N,*)$ all are algebraic structure.

→ $(R,+,.)$ is a type of algebraic structure, which is equipped with two operations (+ and .)

Binary operation of Set

→ A binary operation is a type of operation that needs two inputs (operands)

→ The Two elements of a set are associated with binary operation: The result of these two elements will also be in the same set.

⇒ If we perform a binary operation on a set, then it will perform calculations that combine two elements of the set and generate another element that belongs to the same set.

→ Let us assume that there is a non-empty set called G. A function f from $G \times G$ to G is known as the binary operation on G.
So $f: G \times G \to G$ defines a binary operation on G.

Examples of Binary operation

(i) Addition.

$+ : N \times N \to N$ is derived by $(a, b) \to a+b$.
$+ : R \times R \to R$ is derived by $(a, b) \to a+b$

Self
Sister
Expectations
Body consciousness.

(ii) multiplication:

$+ : N \times N \rightarrow N$ is derived by $(a, b) \rightarrow a \times b$

$+ : R \times R \rightarrow R$ is derived by $(a, b) \rightarrow a \times b$

(iii) Subtraction:-

$- : R \times R \rightarrow R$ is derived by $(a, b) \rightarrow a - b$

(iv) Division:-

$\div : R \times R \rightarrow R$ is derived by $(x, y) \rightarrow x/y$

Properties of algebraic structure:-

(a) Commutative:- The operation $*$ is called to be associative in G if it holds the following relation:

$$x * y = y * x \quad \text{for all } x, y \text{ in } G$$

(b) Associative:- The operation $*$ is called to be associative in G if it holds the following relation:

$$(x * y) * z = x * (y * z) \text{ for all } x, y, z \text{ in } G$$

(c) Identity:- Suppose we have an algebraic system $(G, *)$ and set G contains an element e. That element will be called an identifying element of the set if it contains the following relation:

$$x * e = e * x = x \quad \text{for all } x$$

here, element e can be referred as an identity element of G, and we can also see that it is necessarily unique.

(d) Inverse:- Suppose G contains the elements x and y. The element y will be called an inverse of x if it satisfies the following relation:

$$x * y = y * x = e$$

$$\equiv x * x^{-1} = x^{-1} * x = e$$

(E) Cancellation Law :-

suppose set G contains a binary operation *. The operation * is called to be left cancellation law in G if it holds the fallowing relation.

$x*y = x*z$ ~~iff~~ implies $y=z$

It will be called the right cancellation law if it holds the fallowing relation:

$y*x = z*x$ implies $y=z$.

Types of Algebraic Structure.

- Semi group
- Monoid
- Group
- Abelian Group.

having wide application in particular to binary Coding and in many other disciplines.

(A) Semigroup.

Algebraic Structure $(G,*)$ will be known as semigroup if it satisfies the fallowing condition:

(i) Closure.:- The operation * is a closed operation on G that means $(a*b)$ belongs to set G for all $a,b \in G$.

(ii) Associative: The operation * shows an association operation between a, b and c that means $a*(b*c) = (a*b)*c$ for all a, b, c in G.

Note:- An algebraic structure is always shown by Semigroup.

Example (1): (Matrix, *) and (Set of integer, +)

Exam (2). (Set of positive integers, +), (Set of positive Integers, ·)

(B) Monoid:- A monoid is a semigroup, but it contains an extra identity element (E or e). ~~An algebraic structure (G,*) will be known as a~~

(i) Closure

(ii) Associative

(iii) Identity.

Note:- An algebraic structure and a semigroup are always shown by a monoid. ①

Ex:- (set of integers, *), (set of natural numbers, +) — Not Monoid, but Semigroup. (Monoid as I as identity ele.)

(set of whole numbers, +) — Monoid, 0 as identity element.

(C) Group

- ↳ closure
- ↳ Associative
- ↳ Identity
- ↳ Inverse.

Note:- An algebraic structure, semigroup, and monoid are always shown by a Group.

Ex:- Matrix Multiplication and $(Z, +)$

(d) Abelian Group

- ↳ closure
- ↳ Associative
- ↳ Identity element
- ↳ Inverse Element
- ↳ Commutative law: There will be a commutative law such that $a*b = b*a$ such that a, b belong to G.

Note: $(Z, +)$ is an abelian group because, it is commutative. but matrix multiplication is not commutative so it is not an Abelian Group.

Example for ~~Identity element~~: Inverse Property.

Suppose an operation $*$ on a set S does have an identity element e. The inverse of an element a in S is an element b such that

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

If the operation is associative, then the inverse of a, if it exists, is unique.

Ex:- Consider the rational numbers $\mathbb{Q}$. Under addition, 0 is the identity element, and -3 and 3 are (additive) inverse since

$$(-3) + 3 = 3 + (-3) = 0$$

On the other hand; under multiplication, 1 is the identity element, and -3 and $-\frac{1}{3}$ are (multiplicative) inverses.

Since $$(-3) \cdot (-\tfrac{1}{3}) = (-\tfrac{1}{3}) \cdot (-3) = 1.$$

Note:- 0 has no multiplicative inverse.

Groups :- Let G be a non empty set with a binary operation. Then G is called group if the following axioms holds.

[G_1] : Associative Law :- for any a, b, c in G ; we have $(ab)c = a(bc)$

[G_2] : Identity Element :- There exists an element e in G such that

$$ae = ea = a \text{ for every } a \text{ in } G.$$

[G_3] : Inverse : For each a in G, there exists an element a^{-1} in G (the inverse of a) such that

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

→ The number of elements in a group G, ~~is Called~~ denoted by $|G|$, is called the order of G. G is called a finite group if its order is finite.

→ Group having Commutative property is known as Abelian Group

Ex: (a) The nonzero rational numbers $\mathbb{Q}\setminus\{0\}$ form an abelian group under multiplication. The number 1 is the identity element and q/p is the multiplicative inverse of the rational number p/q.

(b) Let S be the set of 2×2 matrices with rational entries under the operation of matrix multiplication. Then S is not a group since inverse do not always exist. However, let G be the subset of 2×2 matrices with a nonzero ~~base~~ determinant. Then G is group under matrix multiplication. The identity element is

$$I=\begin{bmatrix}1&0\\0&1\end{bmatrix} \text{ and the inver of } A=\begin{bmatrix}a&b\\c&d\end{bmatrix} \text{ is } A^{-1}=\begin{bmatrix}d/|A| & -b/|A|\\ -c/|A| & a/|A|\end{bmatrix}$$

$|A| = ad-bc$

This is an example of nonabelian group since matrix multiplication is noncommutative.

$\Rightarrow$ The formula to calculate the matrix $A=\begin{bmatrix}a&b\\c&d\end{bmatrix}$ is.

$$\Rightarrow A^{-1}=\frac{1}{ad-bc}\begin{bmatrix}d&-b\\-c&a\end{bmatrix}$$

Subgroups, Normal Subgroups and Homomorphisms

Subgroups: Let H be a subset of a group G. Then H is called a subgroup of G if H itself is a group under the operation of G.

$\to$ Simple criteria

A subset H of a group G is a subgroup of G if:

(i) The identity element $e\in H$.

(ii) H is closed under the operation of G, i.e, if $a,b\in H$, then $ab\in H$

(iii) H is closed under inverses, that is, if $a\in H$, then $a^{-1}\in H$.

Note:- Every Group G has the subgroup $\{e\}$ and G itself. Any other subgroup of G is called nontrivial subgroup.

\# Cosets :- Suppose H is a subgroup of G and $a \in G$, then the set

$$Ha = \{ha \mid h \in H\}$$

is called ~~the~~ a right ~~order~~ Coset of H. (aH is called a left coset of H)

Th^m ①:- Let H be a subgroup of a group G. Then the right Coset Ha form a patition of G.

Th^m ②:- Let H be a subgroup of a finite group G. Then the order ~~of~~ of H divides the order of G.

$\Rightarrow$ The number of right Cosets of H in G, called the index of H in G, ~~is~~ is equal to the number of left Cosets of H in G; and both numbers are equal to $|G|$ divided by $|H|$.

\# Normal Subgroups

→ A subgroup H of G is ~~called~~ a normal subgroup if $a^{-1}Ha \subseteq H$, for every $a \in G$, or, equivalently; if $aH = Ha$, i.e. the right and left Cosets Coincide.

Every subgroup of an abelian group is normal.

Examples on Group theory. Ex: 1:- Show that set of integers forms an abelian group under addition.

Ex2:- G is the set of rationals except -1 binary operation $*$ is defined by $\boxed{a*b = a+b+ab}$. Show that it is a group.

Ex3:- In z we define $a*b = a+b+1$ show that $(z,*)$ is an abelian group.

Ex4:- Let G be the set of all positive rational numbers and $*$ be the binary operation on G defined by $a*b = \frac{ab}{7}$ $\forall a,b \in G$. Prove that $(G,*)$ is an abelian group. (Q^+)

Solve $3*x = 2^{-1}$ in G.

Ex5:- Let $Q-\{1\}$ be the set of all rational numbers except 1 with binary operation $*$ defined by $\boxed{a*b = a+b-ab}$ $\forall a,b \in Q-\{1\}$, Show that $Q-\{1\}$ is an abelian group.

Solve $5*x = 3$ in $Q-\{1\}$.

Ex6:

P.T.O

Ex 1:- Show that set of integers forms an abelian group under addition.

Solution:

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

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

$$a+0 = 0+a = a$$

Identity exist.

G4:- Inverse: let $a \in G$ and 0 be the identity.

$$a * a^{-1} = 0$$

$$a^{-1} = -a \qquad -a \in G$$

so inverse exist.

G5:- Commutative: let $a, b \in G$

$$a+b = b+a$$

Commutative law satisfied for all integers under addition.

Ex 2:- G is the set of rationals except -1 binary operation $*$ is defined by $a*b = a+b+ab$. Show that it is a group.

Solution.

$$G = Q - \{-1\}$$

G_1: Let $a, b \in G \Rightarrow a*b = a+b+ab \in G$

Closure is satisfied.

G_2: Let $a, b, c \in G$

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

L.H.S.

$a^*(b^*c)$

$b^*c = b+c+bc = x$

$a^*x = a+x+ax = a+b+c+bc+a(b+c+bc)$

$= a+b+c+bc+ab+ac+abc$

R.H.S.

$(a^*b)^*c$

$a^*b = a+b+ab = x$

$x^*c = x+c+xc = a+b+ab+c+(a+b+ab)(c)$

$= a+b+c+ab+ac+bc+abc$

Since. L.H.S = R.H.S.

So Associative property satisfied.

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

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

$a^*e = a$

$a+e+ae = a$

$e+ae = 0$

$e(1+a) = 0$

$\boxed{e=0}$

$\boxed{a \neq -1}$

0 is identity element.

$0 \in G$.

So, Identity element exists. In G.

G4:- Inverse:- let $a, a^{-1} \in G$ and e be the identity

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

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

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

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

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

$a \neq -1$

Inverse exist.

under Condition

$a \neq -1$

So G^* is a Group

Ex 8:- In Z we define $a * b = a + b + 1$ show that $(Z, *)$ is and abelian group.

Solution :

G_1 : Let $a, b \in Z \Rightarrow a * b = a + b + 1 \in Z$

closure is satisfied.

G_2:- let $a, b, c \in Z$

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

L.H.S.

$$a * (b * c) = a * (b + c + 1)$$
$$= a + b + c + 1 + 1$$
$$= a + b + c + 2$$

R.H.S.

$$(a * b) * c = (a * b) + c + 1$$
$$= a + b + 1 + c + 1$$
$$= a + b + c + 2$$

since. L.H.S = R.H.S, so Associative Property Satisfied.

G3:- Identity:- let $a \in G$., and e be the identity.

$$a * e = e * a = a$$
$$a * e = a$$
$$a + e + 1 = a$$
$$\boxed{e = -1}$$ so Identity element exist.

G4:- Inverse:- let $a \in G$, and e be the identity.

$$a * a^{-1} = a^{-1} * a = e$$
$$a * a^{-1} = e$$
$$a + a^{-1} + 1 = -1$$
$$\boxed{a^{-1} = -2 - a}$$ Inverse exist.

So, $(G, *)$ is an Group.

Ex4:- Let G be the set of all positive rational numbers and * be the binary operation on G defined by $a*b = \frac{ab}{7}$ $\forall a,b \in G$

Prove that (G,*) is an abelian group.

Solve $3*x = 2^{-1}$ in G.

Solution.:-

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

Closure is satisfied.

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

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

∴ L.H.S. $b*c = \frac{bc}{7} = x$

$$a*x = \frac{ax}{7} = \frac{abc}{49}$$

R.H.S. $a*b = \frac{ab}{7} = x$

$$x*c = \frac{\frac{ab}{7}\cdot c}{7} = \frac{abc}{49}$$

since L.H.S = R.H.S., Associative Property satisfied.

G3: Identity.:- Let $a \in G$, e be the identity element.

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

$$a*e = a$$

$$\frac{ae}{7} = a \qquad e \in G$$

$$\boxed{e = 7}$$ Identity element exists.

G4:- Inverse.:- Let $a \in G$, e be the Identity element.

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

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

$$\boxed{a^{-1} = \frac{49}{a}} \quad \boxed{\frac{49}{a} \in Q^{+}}$$

$\boxed{a^{-1} = \frac{49}{a}}$ Inverse is satisfied.

G5:- Commutative Property :- let $a, b \in G$.

$$a * b = b * a$$

L.H.S.

$$a * b = \frac{ab}{7}$$

R.H.S.

$$b * a = \frac{ba}{7}$$

L.H.S = R.H.S. Commutative Property satisfied, So $(G, *)$ is an abelian group.

Solving $3 * x = 2^{-1}$ in G

$$\frac{3x}{7} = 2^{-1}$$

$$\boxed{2^{-1} = \frac{49}{2}}$$

$$\Rightarrow \frac{3x}{7} = \frac{49}{2}$$

$$x = \frac{49 \times 7}{2 \times 3} \Rightarrow \boxed{x = \frac{343}{6}}$$

Ex 5:- Let $Q-\{1\}$ be the set of all rational numbers except 1 with binary operation $*$ defined by $a*b = a+b-ab \; \forall a, b \in Q-\{1\}$. Show that $Q-\{1\}$ is an abelian group. solve $5*x = 3$ in $Q-\{1\}$

Solution:- G1: Let $a, b \in Q-\{1\} \Rightarrow a*b = a+b-ab \in Q-\{1\}$ closure is satisfied.

G2: Let $a, b, c \in Q - \{1\}$

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

L.H.S. $b*c = b+c-bc = x$

$a*x = a+x-ax = a+b+c-bc-a(b+c-bc)$

$= a+b+c-bc-ab-ac+abc$.

R.H.S.

$a*b = a+b-ab = x$

$x*c = a+b-ab+c-(a+b-ab).c$

$= a+b+c-ab-ac-bc+abc$

Since L.H.S = R.H.S, so Associative Law satisfied.

G3:- Identity:- let $a \in Q-\{1\}$, and e be the identity element.

$a*e = e*a = a$

$a*e = a$

$a+e-ae = a$

$e-ae = 0$

$e(1-a) = 0$ since. $a \neq 1$.

so $\boxed{e = 0}$ Identity elenet exist.

G4:- Inverse.:- let $a \in Q-\{1\}$, and e be the identity element.

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

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

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

$\boxed{a^{-1} = -\frac{a}{(1-a)}}$ $a \neq 1$

so Inverse exist in $Q-\{1\}$ for $\forall a \in Q-\{1\}$

G5:- Commutative:- let $a, b \in Q-\{1\}$.

$a*b = b*a$

L.H.S.

$$a * b = a + b - ab$$

R.H.S.

$$b * a = b + a - ba$$

since L.H.S = R.H.S.

So, commutative property holds in algebraic structure

So. $(G, *)$ is an abelian group.

Solving:- $5 * x = 3$ in $Q - \{1\}$

$$5 * x = 3$$

$$5 + x - 5x = 3$$

$$x(1-5) = -2$$

$$x = \frac{2}{4} = 1/2 \qquad \boxed{x = 1/2}$$

Ex6:- Show that the cube root of unity is an abelian group under multiplication.

Sol^n:-

$$x = \sqrt[3]{1}$$

$$x = 1^{1/3}$$

$$x^3 = 1$$

$$x^3 - 1 = 0$$

$$\Rightarrow (x-1)(x^2 + x + 1) = 0$$

$$\Rightarrow x = 1$$

$$x = \frac{-1 \pm i\sqrt{3}}{2}$$

roots:- $x = 1, \frac{-1+i\sqrt{3}}{2}, \frac{-1-i\sqrt{3}}{2}$

$$\downarrow 1 \qquad \downarrow \omega \qquad \downarrow \omega^2$$

$$\boxed{\omega^3 = -1}$$

$$\boxed{1 + \omega + \omega^2 = 0}$$

Table.

$\times$	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

$G = 1, \frac{-1+i\sqrt{3}}{2}, \frac{-1-i\sqrt{3}}{2}$

$G = 1, \omega, \omega^2$

Note: $\omega\omega^2 = \omega^3 = 1$, $1+\omega+\omega^2 = 0$

The above entries in the table satisfying all the axioms.

G_1 : Let $a, b \in G$ $a.b \in G$

Closure satisfied.

$\underline{G_2}$: let $a, b, c \in G$.

$$a.(b.c) = (a.b).c$$

~~H.P L.H.S~~. $abc = abc$

Associative is satisfied.

G3: 1 is the top row indicates the identity.

$$a \cdot 1 = 1.a = a$$

G3 is satisfied.

$\underline{G4}$: Let $(1)^{-1} = 1$, $(\omega^{-1}) = \omega^2$, $(\omega^2)^{-1} = \omega$

Inverse is satisfied.

G5: Let $a, b \in G$ $a.b = b.a$

Commutative is satisfied.

so $\Rightarrow$ $(G, *)$ is an abelian group under multiplication.

Ex 7:- If $G = \{f_1, f_2, f_3, f_4\}$ of four functions defined by $f_1(x) = x$, $f_2(x) = -x$, $f_3(x) = \frac{1}{x}$, $f_4(x) = -\frac{1}{x}$ $\forall\, x \in \underbrace{R}_{\text{Real NO.}} - \{0\}$ is an abelian group. operation $\boxed{f \circ g = f(g(x))}$

Solution.:

Let $x \in R - \{0\}$

$f_1 \circ f_1(x) = f_1(x) = x = f_1$

$f_2 \circ f_2(x) = f_1(f_2(x)) = f_1(-x) = -x = f_2$

$\circ$	f_1	f_2	f_3	f_4
f_1	f_1	f_2	f_3	f_4
f_2	f_2	f_1	f_4	f_3
f_3	f_3	f_4	f_1	f_2
f_4	f_4	f_3	f_2	f_1

G_1:- Closure Property ~~exist sty~~ satisfied
since all the composite operation result $\in G$.

G_2:- Associative.

$$f_2 * (f_3 * f_4) = (f_2 * f_3) * f_4$$

$$\Rightarrow f_2 \circ (f_3 \circ f_4) = (f_2 \circ f_3) \circ f_4$$

L.H.S.

$$f_3 \circ f_4 = f_3(f_4(x)) = f_3\left(-\frac{1}{x}\right) = \underbrace{-x}_{\alpha}$$

$$f_2 \circ (\alpha) = f_2(-x) = \underline{x}$$

R.H.S.

$$f_2 \circ f_3 = f_2(f_3(x)) = f_2\left(\frac{1}{x}\right) = -\frac{1}{x} = \underline{f_4}$$

$$(f_2 \circ f_3) \circ f_4 = f_4 \circ f_4 = f_4(f_4(x)) = f_4(-1/x)$$

$$= x.$$

Since. L.H.S. = R.H.S. so Associative property satisfied.

G3:- Identity:- f_1 is identity as shown in top row.

that $f_1 \circ f_1 = f_1$, $f_2 \circ f_1 = f_2$, $f_3 \circ f_1 = f_3$, $f_4 \circ f_1 = f_4$

G4:- Inverse:-

$\cancel{f_2 \circ f_2^{-1} = f_1}$

from table check diagonal.

$f_1^{-1} = f_1$, $f_2^{-1} = f_2$, $f_3^{-1} = f_3$, $f_4^{-1} = f_4$

so Inverse all ~~ele~~ elements exist.

G

G5:- Commutative:-

Table is having symmetric property so, it is

ie

Abelian group.

Ex:-

$f_1 \circ f_2 = f_2$

$f_2 \circ f_1 = f_2$

$\Rightarrow f_1 \circ f_2 = f_2 \circ f_1$.

Ex:8:- Show that the fourth root of unity is an abelian group under multiplication.

$x = \sqrt[4]{1}$

$x = 1^{1/4}$

$x^4 = 1$

$\Rightarrow (x^2-1)(x^2+1) = 0$

$\Rightarrow (x^2-1) = 0, (x^2+1) = 0$

$\Rightarrow x^2 = 1, \quad x^2 = -1$

$\Rightarrow x = \pm 1, \quad x = \pm\sqrt{-1} = \pm i$

$G = 1, -1, i, -i$

x	1	-1	i	-i
1	1	-1	i	-i
-1	-1	1	-i	i
i	i	-i	-1	1
-i	-i	i	1	-1

G1:- Closure:- all results lie in G.
so closure satisfied.

G2:- Associative :- let $a, b, c \in G$.

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

So Associative satisfied.

G3:- Identity :-
from table top row. 1 is the identity element.

G4:- Inverse.
from table.
$1^{-1} = 1, \quad -1^{-1} = -1, \quad i^{-1} = -i, \quad -i^{-1} = i$

Inverse exist.

G5:- Commutative
Let $a, b \in G$.

$$a*b = b*a.$$

$a.b = b\,a.$ satisfied by all $a, b \in G$.

So. $(G, \times)$ is an Abelian group.

Subgroups

Defⁿ:- A non empty subset H of a group G is called a subgroup of G if.

(i) H is stable (closed) for the composition defined in G i.e. (binary operation)

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

and

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

* Proper and Improper (or Trivial) Subgroup:-

Every group G of order greater than 1 has atleast two subgrops which are: (No. of elements)

(i) G (itself)

(ii) $\{e\}$. i.e. the group of the identity alone.

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

✓ A subgroup other than ~~trivial~~ these are known as a proper subgroup.

* Note:- 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 example, the group $\{1,-1\}$ is a part of $(C,+)$ which is a group for multiplication but not for the composition $(+)$ of the basic group. Therefore this is not the subgroup of $(C,+)$

Examples of Subgroup:

$N \subseteq Z \subseteq Q \subseteq R \subseteq C$ — complex.

(i) Additive Groups

Ex1: $(Z,+)$ is a subgroup of $(Q,+)$

Ex2: $(Q,+)$ is a subgroup of $(R,+)$

Ex3: The set E of even integers is a proper subgroup of additive group $(E,+)$. whereas the set O of odd integers is not a subgroup of the additive groups $(Q,+),(Z,+)$.

Ex4:- The set ~~no~~ $m\mathbb{Z}$ of multiples of some given integers m is a subgroup of $(\mathbb{Z}, +)$.

Ex5:- The group $\{0, 4\}$ is subgroup of $(\mathbb{Z}_8, +_8)$ modulo 8.

ii) multiplicative Groups

Ex 1: $(Q', \times)$ is a subgroup of $(R', \times)$ multiplication of ^{n}

Ex 2:- $\{1, -1\}$, $\{1, \omega, \omega^2\}$, $\{1, -1, i, -i\}$ are subgroups of $(\mathbb{C}_0, \times)$ the group of non zero complex numbers.

Ex3:- for multiplication operation $(\{1, -1\}, \times)$ is subgroup of $\{1, -1, i, -i\}$.

Theorem(1)

If H is a subgroup of a G, then:

(a) The identity of H is ~~a~~ the same as that of G,

(b) The inverse of any element a of H is the same as the inverse of the same ~~gr~~ 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 e and e' be the identities of G and H respectively.

If $a \in H$, then $ae' = e'a = a$ --- (1)

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

Again

$\therefore \; ae = ea = a$ --- (2)

~~$a \in H \Rightarrow a$~~

for (1) and (2): $ae' = ae$

$\Rightarrow \boxed{e' = e}$ [by Cancellation law]

(b). Let $a \in H$ and $a \in G$.

let b is the inverse of a in H, and

c is the inverse of a in G.

So $ab = ba = e \xrightarrow[\text{(i)}]{}$ e is the common identity elem.

$ac = ca = e$

$\Rightarrow ab = ac$

$\Rightarrow \underline{b = c}$

(c). Let the order of $a \in H$ be m and n in H and G respectively, if e be the identity, then by the definition of order.

$$a^m = e \text{ and } a^n = e \Rightarrow a^m = a^n$$

$\Rightarrow a^m . a^{-n} = a^n . a^{-n} = a^0$

$\Rightarrow a^{m.n} = e$

$\Rightarrow m - n = 0 \qquad [\because m - n < m = O(a) \text{ in } H]$

$\Rightarrow m = n \qquad [m - n < n = O(a) \text{ in } G]$

Therefore the order of any element of subgroup is the same as that of the subgroup and the original group.

In the light of the above results, we conclude that a subset H of a group G is 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) $a \in H \Rightarrow a^{-1} \in H$, where a^{-1} is the inverse of a in G.

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 and $b \in H$

then $b \in H \Rightarrow b^{-1} \in H$ [by existance 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 subgroup of G, then the condition is necessary.

Conversely. ($\Leftarrow$): Suppose the given condition is true in H, then we shall prove that H will be a subgroup

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

therefore identity exist in H.

Again by the same condition, $e \in H, a^{-1} \in H \Rightarrow ea^{-1} = a^{-1} \in H$.

Thus the inverse of every element exist 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.

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

Thm 3:- A nonvoid finite subset H of a group G is a subgroup iff $a \in H, b \in H \Rightarrow ab \in H$

Thm 4:- The intersection of any two subgroups of a group G is again a subgroup of G.

Criteria for the product of two subgroups to be a subgroup.

If H and K are two subgroups of any group G, then their product HK or KH need not be subgroup.

Thm 5:- If H and K are two subgroups of a group G, then HK is a subgroup of G iff ($\Leftrightarrow$) $HK = KH$.

Examples of Subgroups.

① Show that $H = \{0,2,4\}$ is a subgroup of the group that $G = \{0,1,2,3,4,5\}$ under addition modulo 6.

Soln:- clearly $H = \{0,2,4\} \subset G$ . . . (1)

TPT

(i) closure axioms: All the entries in the table are the elements of H.

Therefore the closure axiom is satisfied.

(ii) Associative

(iii) Identity element is zero

(iv) $0^{-1} = 0$, $2^{-1} = 4$, $4^{-1} = 2$

$+_6$	0	2	4
0	0	2	4
2	2	4	0
4	4	0	2

Cayle's table or a composition table.

Order of a group.

⇒ The group's order can be described by its cardinality, which means the number of its elements.

⇒ In a group, the order of element 'a' is the positive integer "m"

$$\boxed{a^m = e}$$

a^m is used to specify the product of m copies of a.
e is used to specify the identity element of a group.

Ex:① $G = \{1, \omega, \omega^2\}$

$1^1 = 1 \Rightarrow O(1) = 1$

$\omega^3 = 1 \Rightarrow O(\omega) = 3$

$(\omega^2)^3 = \omega^6 = 1 \Rightarrow O(\omega^2) = 3$

Ex2 $G = \{1, -1, i, -i\}$

$1^1 = 1 \Rightarrow O(1) = 1$

$(-1)^2 = 1 \Rightarrow O(-1) = 2$

$(i)^4 = 1 \Rightarrow O(i) = 4$

$(-i)^4 = 1 \Rightarrow O(-i) = 4$

Ex 3:- $G = \{0, 1, 2, 3\}$

$(G, +_4)$

$2 +_4 2 = 0$

$O(2) = 2$

$3 +_4 3 +_4 3 +_4 3 = 0$

$O(3) = 4$

Cyclic Group.

A group (multiplicative) G is said to be cyclic if its all elements can be generated by its a single element.

Ex: In case of multiplicative group,

$G = \{x : x = a^n\}$ where $a \in G$, n is any positive integer.

[cyclic group.]

Another way of representation:-

$G = (a)$ Generator.

Ex:-

$G = \{1, -1, i, -i\}$

let $a = i$ $\quad i^1 = i, \; i^2 = -1, \; i^3 = -i, \; i^4 = 1$

let $a = -i$ $\quad (-i)^1 = -i, \; (-i)^2 = -1, \; (-i)^3 = i, \; (-i)^4 = 1.$

so. $(G, \cdot)$ is an cyclic group.

Ex: $G = \{0, 1, 2, 3, 4\}$ A group under addition modulo 5.

let $a = 1$,

$1 +_5 1 = 2, \quad 1 +_5 1 +_5 1 = 3, \quad 1 +_5 1 +_5 1 +_5 1 = 4,$

$1 +_5 1 +_5 1 +_5 1 +_5 1 = 0, \quad 1 +_5 1 +_5 1 +_5 1 +_5 1 +_5 1 = 1.$

So, given $(G, +)$ is a cyclic group.

Cosets:

let $(G, \times)$ is multiplicative group.

and H is a subgroup of G.

let 'a' be any element of G.

then. $Ha = \{ ha : h \in H \}$ → Right Coset of H in G

$aH = \{ ah : h \in H \}$ → left Coset of H in G.

Note:- $a \in G$, a may or may not belong to H.

~~$H+a = \{$~~

In Case of Additive group:-

$(G, +)$, $(H, +)$, $a \in G$

$H+a = \{ h+a, h \in H \}$ → Right Coset of H in G

$a+H = \{ a+h, h \in H \}$ → left coset of H in G.

Ex:- G = set of Real numbers.

H = Set of integers. $\{0, \pm 1, \pm 2, \pm 3 \ldots\}$

let $\frac{1}{2} = a \in G$

$H + a = H + \frac{1}{2} = \{ h + \frac{1}{2} : h \in H \}$ right Coset of H in G.

So Right Coset: $\{ \frac{1}{2}, \pm \frac{1}{2}, \pm \frac{3}{2}, \pm \frac{5}{2}, \pm \frac{7}{2} \} \ldots$

Ex:- $G = \{1, -i, i, -1\}$, $H = \{1, -1\}$ ⟶ multiplicative

$Hi = \{ h \cdot i : h \in H \}$ right Coset of H in G.

$= \{ i, -i \}$

Lagrange's Theorem :-

The order of each subgroup of a finite group a divisor of order of group. i.e. $\frac{O(G)}{O(H)}$

Proof :- Let H be the subgroup of finite group G and order of H

& $O(H) = m$, $O(G) = n$ $(m < n)$

Let $a \in G \Rightarrow aH$ is a ~~right~~ left coset of H in G and have m distinct elements.

$$aH = \{ah_1, ah_2, ah_3, \ldots, ah_m\}$$

first we show aH has 'm' distict elements. For this suppose conversely. i.e. $ah_i = ah_j$ where $i \neq j$

i.e.

$\Rightarrow h_i = h_j$ for $h_i, h_j \in H$

$\Rightarrow$ H has two same elements.

$\Rightarrow O(H) \neq m < m$

$\Rightarrow$ Its a contradiction.

$\Rightarrow$ Every ~~Right~~ left coset has m distinct element.

Since G is finite so by ~~Right~~ left coset decomposition of G,

$$G = a_1H \cup a_2H \cup a_3H \cup \ldots \cup a_kH$$

$$[a_iH \cap a_jH = \phi]$$

$$\Rightarrow O(G) = O(a_1H) + O(a_2H) + \ldots + O(a_kH)$$

$$n = m + m + \ldots + m \ldots k \text{ times}$$

$$n = mk$$

$$k = \frac{n}{m} \Rightarrow \frac{O(G)}{O(H)}$$

Hence Proved.

Normal Subgroups:

Def^n: Let H is the Subgroup of group G. If for all $h \in H$ and ~~for all~~ for all $x \in G$.

$$xhx^{-1} \in H$$

Then H is called normal subgroup of G.

→ Normal subgroup can also be denoted by $xHx^{-1}, x \in G$.

Important Results

(1). If $x \in H \Rightarrow xHx^{-1} = x(Hx^{-1}) = xH = H$ $[\forall a \in H \Rightarrow aH = Ha = H]$

(2). for all $x \in G \Rightarrow xH = Hx$

$$\Rightarrow xHx^{-1} = Hxx^{-1}$$

$$\Rightarrow xHx^{-1} = He$$

$$\Rightarrow \boxed{xHx^{-1} = H}$$

$aH = Ha = H$ — left coset, right coset, Subgroup

Th^n: Prove that Intersection of two normal subgroups is normal subgroup.

Proof: Let H and K are two normal Subgroups of Group G.

we conclude our proof by showing that for all $y \in H \cap K$ and for all $x \in G \Rightarrow xyx^{-1} \in H \cap K$

Now, since $y \in H \cap K \Rightarrow y \in H$ and $y \in K$

Now for all $x \in G$, we have $xyx^{-1} \in H$ ($\because$ H is normal and $y \in H, x \in G$)

Similarly. K is also normal subgroup so. for any $y \in K$ and $x \in G$

$$\Rightarrow xyx^{-1} \in K$$

i.e. for all $y \in H \cap K$ and $x \in G \Rightarrow \boxed{xyx^{-1} \in H \cap K}$