DISCRETE MATHEMATICS (U19MA203)

Branch : CSE

Semester: III

MODULE IV

ALGEBRAIC STRUCTURES

Prepared by

Dr.N.Murugavalli

Associate Professor

Department of Mathematics

Sri Eshwar College of Engineering

ALGEBRAIC STRUCTURES

BINARY OPERATION

In the set of natural numbers N, we can add any two numbers a and b get a unique number a+b. The operation addition combines two numbers and yield a third number and so it is a binary operation. Suppose such an operation is to be defined in a set S, we have to view addition in different way.

i.e., $+ \ : N \times N \rightarrow N$ is defined by +(a,b) = a+b.

Definition: Binary operation

Let S be a non empty set. A binary operation $*$ on S is a function $* \ : S \times S \rightarrow S$. The image of any ordered pair (a, b) of elements of S under $*$ is defined by $a * b$.

Note: $+$, $-$, $\times$, $\div$, $\cup$, $\cap$, $\circ$, $*$,…… are some binary operations.

Definition: Algebraic structure (or) Algebraic system:

A non-empty set A together with one or more n-ary operations $*$ defined on it is called algebraic system and it is denoted by (A, $*$).

Example:

(Z, +, $*$) is an algebraic system where + and $*$ are the operations of addition and multiplication on Z.

Example :

The usual addition + on natural number set is a binary operation.

The number set N = Natural number set

= the set of positive numbers

N= {1,2,3,4,5,….}.

(N, +) is an algebraic structure since the sum of any two numbers in N is also in N.

i.e., If 3, 56 $\in$ N then 3+56 = 59 $\in$ N

but (N, $-$) is not an algebraic structure since the difference of any two numbers in N is not in N.

i.e., If 5, 9 $\in$ N then 5-9 = -4 $\notin$ N.

Notations:

N = the set of positive numbers ={1,2,3,4,5,……}

Z = the set of all integers ={0,±1, ±2, ±3, ±4, ±5,……}

R = the set of real numbers

Q^+ = the set of positive real numbers

C = the set of complex numbers

Q = the set of rational numbers = $\left\{ \frac{p}{q}\ such\ that\ p,q\ \in Z\ and\ q \neq 0 \right\}$

Q^+ = the set of positive rational numbers

Note: (R, +), (Z, +), (Z,−) and (C, +) are an algebraic structures.

Properties of Binary operations:

Let the binary operation be $* \ : G \times G \to G$. It is denoted by (G, $*$).

CLOSURE PROPERTY:

For all $,b\ \in G$, $a * b\ \in G$

For example, addition on N is closed since $5, 9\ \in N$, $5 + 9 = 14\ \in N$. Therefore (N,+) is closed

COMMUTATIVE PROPERTY:

For all $,b\ \in G$, $a * b = b * a$

For example, multiplication on Z is commutative since $-6, 9\ \in Z$, $(-6) \times 9 = 9 \times (-6) = -54\ \in Z$. Therefore (Z,×) is commutative.

Note: (Z, ÷) is not commutative.

ASSOCIATIVE PROPERTY:

For all $,b,c\ \in G$, $a * (b * c) = (a * b) * c$

For example, multiplication on N is associative since 2,5,8 $\in N$, $2 \times (5 \times 8) = (2 \times 5) \times 8 = 80 \in N$. Therefore (N, ×) is associative.

EXISTENCE OF IDENTITY:

An algebraic structure (G, $*$) is said to have an identity element $e \in G$ if $a * e = e * a = a$ for all $a\ \in G$

For example, In the algebraic structure (Z,+), 0 is the identity element because $a + 0 = 0 + a = a\ for\ all\ a\ \in Z$

EXISTENCE OF INVERSE ELEMENT:

If $a * b = b * a = e$ for any $a,b \in G$ then 'b' is called the inverse of 'a' and it is denoted by $b = a^{-1}$. (here e is identity element and $e \in G$)

For example, In the algebraic structure (Z,+), inverse of any element a is -a because $a + (-a) = (-a) + a = 0 \; for\; all\; a \in Z$.

Note: The set of real numbers R with usual + and x as binary operations is an algebraic struture or algebraic system.

Semigroup: A non empty set S together with binary operation $*$ an algebraic structure (S, $*$) is called semigroup if $*$ satisfies the following properties

(i) Closure property: For all $a,b \in S$, $a * b \in S$

(ii) Associative property: For all $a,b,c \in S$, $a * (b * c) = (a * b) * c$

Example: The set of all rational numbers Q is a semi group for the operation $*$ defined by a $*$ b = $\frac{ab}{2}$ $\forall$ a, b $\in$ Q.

Monoid : A non empty set M together with binary operation $*$ (or) an algebraic structure (M, $*$) is called monoid if $*$ satisfies the following properties

(i) Closure property: For all $a,b \in M$, $a * b \in M$

(ii) Associative property: For all $a,b,c \in M$, $a * (b * c) = (a * b) * c$

(iii) Identity property: There exists an element $e \in M$ such that $a * e = e * a = a$ for all $a \in M$

Group : A non empty set G together with binary operation $*$ (or) an algebraic structure (G, $*$) is called a group if $*$ satisfies the following properties

(i) Closure property: For all $a,b \in G$, $a * b \in G$

(ii) Associative property: For all $a,b,c \in G$, $a * (b * c) = (a * b) * c$

(iii) Identity property: There exists an element $e \in G$ such that $a * e = e * a = a$ for all $a \in G$

(iv) Inverse: For each $a \in G$, there exists an element a' such that $a * a' = a' * a = e$

Abelian group : A non empty set G together with binary operation $*$ (or) an algebraic structure (G, $*$) is called an abelian group if $*$ satisfies the following properties

(i) Closure property: For all $a,b \in G$, $a * b \in G$
(ii) Associative property: For all $a,b,c \in G$, $a * (b * c) = (a * b) * c$
(iii) Identity property: There exists an element $e \in G$ such that $a * e = e * a = a$ for all $a \in G$
(iv) Inverse: For each $a \in G$, there exists an element a' such that $a * a' = a' * a = e$
(v) Commutative property: For all $a,b \in G$, $a * b = b * a$

In other words, a group (G, $*$) is called abelian group if it satisfies commutative property i.e., for all $a,b \in G$, $a * b = b * a$

Order of a Group:

Let G be a group under the operation $*$. Then the number of elements in G is called the order of the group G and is denoted by O(G) (or) $|G|$.

If G has n elements then O(G) = n.

For example, If A = {a,e,i,o,u} then O(A) = 5 (or) $|A| = 5$

Finite and Infinite Group:

If the O(G) is finite then G is called a finite group. Otherwise it is called infinite group.

Subgroup:

Let (G, $*$) be a group . A non empty set H of G is said to be a subgroup of G if H is itself group under the same operation $*$ of G.

Cyclic Group:

A group (G, $*$) is said to be a cyclic group if for every element $x \in G$ can be expressed as $x = a^m$ or $x = ma$ for some $a \in G$ and m $\in Z$.

Order of a group:

The number of elements in a group $(G, *)$ is called order of a Group and is denoted by $O(G)$.

Order of an element:

Let $(G, *)$ be a group and $a \in (G, *)$ **.** Then the least positive integer n such that $a^n = e$ is called the order of the element *a* .
(i.e., $a^n = e \Leftrightarrow O(a) = n$ **).**

Cosets:

Let (H, $*$) be a subgroup of a group (G, $*$).

Left coset of H: For any $a \in G$, the left coset of H is defined by

$a * H = \{a * h : h \in H\}$.

Right coset of H: For any $a \in G$, the right coset of H is defined by

$H * a = \{h * a : h \in H\}$.

NORMAL SUBGROUPS

A subgroup (H, $*$) of a group (G, $*$) is said to be a normal subgroup, for every $x \in G$ and for $h \in G$ if $x * h * x^{-1} \in H$ $i.e,$ $x * H * x^{-1} \subseteq H$.

Another form of definition: A subgroup (H, $*$) of a group (G, $*$) is called a normal subgroup if $x * h = h * x \; \forall \, x \in G$.

(or) A subgroup H of a group G is called a normal subgroup if
$xH = Hx \; \forall \, x \in G$.

Group Homomorphism:

Let (G, $*$) and (H, Δ) be any two groups. A mapping *f : G* *H* is called a group homomorphism if $f(a * b) = f(a) \, \Delta \, f(b)$ for all $a,b \in G$.

(or) Let (G, $*$) and (G', $*$) be two groups. A mapping *f : G* $G'$is called a group homomorphism if $f(a * b) = f(a) * f(b)$ for all $a,b \in G$.

Isomorphism:

Let (G, $*$) and (H, Δ) be any two groups. A mapping *f : G* *H* is called an isomorphism if

(i) *f* is homomorphism *i.e.,* $f(a * b) = f(a) \, \Delta \, f(b)$ for all $a,b \in G$.

(ii) f is ono to one (injective)

(iii) f is onto (surjective).

In otherwords, a bijective homomorphism is said to be an isomorphism.

Kernel of a homomorphism:

Let f : G $\rightarrow$ G' be a group homomorphism . The set of elements of G which are mapped into e' (i.e., e' is an identity element of G') is called the kernel of f and it is denoted by ***ker(f)***.

i.e., *ker(f)* ={ $x \in G$ / *f(x)* =*e′* }

Quotient group or Factor group:

Let (H, $*$) be a normal subgroup of a group (G, $*$) and G/H denotes the set of all left (or right) cosets of H in G. i.e., G/H = $\{a * H : \forall a \in G \}$. Then an algebraic structure (G/H, $\oplus$)is said to be a quotient group if $(a * H) \oplus (b * h) = (a * b) * H \;\; \forall a,b \in G$.

Natural Homomorphism:

Let (H, $*$) be a normal subgroup of a group (G, $*$). A mapping *f : G* $\rightarrow$ *G/H such that* $f(x) = H * x$, $\forall x \in G$ is called a natural homomorphism of the group G onto the quotient group G/H.

PROPERTIES OF GROUPS

PROPERTY 1: In a group (G,$*$), the identity element is unique.

Proof: If possible, let e_1 *and* e_2 be two identity elements in the group (G,$*$).

Since e_2 is an identity and $e_1 \in$ G,

we have $e_2 * e_1 = e_1 * e_2 = e_1$ $\rightarrow$ (1)

Since e_1 is an identity and $e_2 \in$ G,

we have $e_1 * e_2 = e_2 * e_1 = e_2$ $\rightarrow$ (2)

From (1) and (2) we have $e_1 = e_2$

Hence the identity element of a group is unique.

PROPERTY 2: The inverse of every element in a group is unique.

Proof: Let (G,$*$) be a group.

Let b and c be inverses of the element "a" $\forall$ a,b, c $\in$ G

Then a $*$ b = e $\rightarrow$ (1)

and a $*$ c = e $\rightarrow$ (2)

To prove : b = c

b = b ∗ e [since e is the identity element in G]

= b ∗ (a ∗ c) [by (2)]

= (b ∗ a) ∗ c [associative]

= (a ∗ b) ∗ c [Commutative]

= e ∗ c [by (1)]

= c.

∴ b = c.

∴ The inverse is unique.

PROPERTY 3: [INVOLUTION LAW]

In a group $(G,*)$, $\left(a^{-1}\right)^{-1} = a\ ,\forall\, a \in G$

OR

In a group $(G,*)$, the inverse of a^{-1} is a .

Proof: Let $(G,*)$ be a group.

Let e be the identity element of $(G,*)$

Let $a \in (G,*)$.

We know that a has unique inverse say a^{-1} .

Therefore $a^{-1} * a = a * a^{-1} = e$ ---------(1)

To prove : $\left(a^{-1}\right)^{-1} = a\ ,\forall\, a \in G$

Consider

$\left(a^{-1}\right)^{-1} * (a^{-1} * a) = \left(a^{-1}\right)^{-1} * e = \left(a^{-1}\right)^{-1}$ ---------(2)

$\left(a^{-1}\right)^{-1} * (a^{-1} * a) = \left(\left(a^{-1}\right)^{-1} * a^{-1}\right) * a = e * a = a$ ---------(3)

From (2) & (3) , $\left(a^{-1}\right)^{-1} = a\ ,\forall\, a \in G$.

PROPERTY 4 : [CANCELLATION LAW]

In a group $(G,*)$, for $a,b,c \in (G,*)$

(i) $a * b = a * c \Rightarrow b = c$ **[Left cancellation law]**

(ii) $b * a = c * a \Rightarrow b = c$ **[Right cancellation law]**

Proof: Let $(G,*)$ be a group.

Let $a \in (G,*) \Rightarrow a^{-1} \in (G,*)$ since every element in a group has unique inverse.

To prove: LEFT CANCELLATION LAW

Let $a * b = a * c$

Pre-operating by a^{-1} on both sides, we get

$$a^{-1} * (a * b) = a^{-1} * (a * c)$$
$$(a^{-1} * a) * b = (a^{-1} * a) * c$$
$$e * b = e * c$$
$$b = c$$

To prove: RIGHT CANCELLATION LAW

Let $b * a = c * a$

Post-operating by a^{-1} on both sides, we get

$$(b * a) * a^{-1} = (c * a) * a^{-1}$$
$$b * (a * a^{-1}) = c * (a * a^{-1})$$
$$b * e = c * e$$
$$b = c$$

PROPERTY 5 :

In a group, identity element is the only idempotent element.

Note: An element $a \in (G, *)$ is called and **Idempotent element** if $a * a = a$

(i.e., **An element operated with itself gives same element)**

Proof:

Let $(G, *)$ be a group.

Let e be the identity element of $(G, *)$

Clearly e is idempotent since $e * e = e$.

To prove: e is the only idempotent element.

If possible let $a \in (G, *)$ be another idempotent element.

Therefore we have, $a * a = a$ **.**

Consider

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

Hence, e is the only idempotent element.

PROPERTY 6: In a group $(a * b)^2 = a^2 * b^2 \ \forall\ a, b \in G$ if G is abelian.

Proof: Assume that (G, ∗) is abelian.

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

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

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

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

[Since G is abelian, $(a * b) = (b * a)$]

$\therefore\ (a * b)^2 = (a * a) * (b * b) = a^2 * b^2$

PROPERTY 7: In a group G if $(a * b)^2 = a^2 * b^2 \ \forall\ a, b \in G$ then G is abelian.

Proof: To prove that (G, ∗) is abelian.

Now $(a * b)^2 = a^2 * b^2$

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

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

$\Rightarrow\ b * (a * b) = a * (b * b)$ (by left cancellation law)

$\Rightarrow\ (b * a) * b = (a * b) * b$

$\Rightarrow\ b * a = a * b$ (by right cancellation law)

$\therefore$ G is abelian.

PROPERTY 8 : A group (G, ∗) is an abelian if and only if $(a * b)^2 = a^2 * b^2 \ \forall\ a, b \in G$.

Solution: Let us assume that (G, ∗) is abelian.

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

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

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

Since G is abelian, $(a * b) = (b * a)$

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

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

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

Conversely, assume that $(a * b)^2 = a^2 * b^2$

To prove: G is abelian.

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

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

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

$$b * (a * b) = a * (b * b) \quad \text{[by left cancellation law]}$$

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

$$b * a = a * b \quad \text{[by right cancellation law]}$$

$\therefore a * b = b * a \ \forall\, a, b \in G$. Hence G is an abelian.

PROPERTY 9: A group $(G, *)$ is an abelian if and only if $(a * b)^{-1} = a^{-1} * b^{-1} \ \forall\, a, b \in G$.

Proof: Assume that $(G, *)$ is an abelian

$$\therefore a * b = b * a \ \forall\, a, b \in G$$

Now $(a * b)^{-1} = (b * a)^{-1} = a^{-1} * b^{-1}$

Conversely, assume that $(a * b)^{-1} = a^{-1} * b^{-1}$

But $a^{-1} * b^{-1} = (b * a)^{-1}$. $\therefore (a * b)^{-1} = (b * a)^{-1}$

Taking inverse on both sides, $((a * b)^{-1})^{-1} = ((b * a)^{-1})^{-1}$

$\Rightarrow a * b = b * a \ \forall\, a, b \in G$. Hence G is an abelian

PROPERTY 10 : If $(G, *)$ is an abelian group, then $(a * b)^n = a^n * b^n \ \forall\, a, b \in G$ where n is a positive integer.

Proof: Proof follows by Mathematical induction

Let $P(n) = (a * b)^n = a^n * b^n$

To Prove: P(1) is true

Since $(G, *)$ is an abelian group, $a * b = b * a$

$\forall\, a, b \in G \quad \rightarrow$ (i)

For $a, b \in G$, we have $(a * b)^1 = a^1 * b^1$ by (i)

and $\quad (a * b)^2 = (a * b) * (a * b)$

$= a * (b * a) * b$ [by associative law]

$= a * (a * b) * b$ by (i)

$= (a * a) * (b * b)$ [by associative law]

$= a^2 * b^2$.

Thus the required result is true for n = 1, 2.

Assume that the result is true for P(m).

i.e. $(a * b)^m = a^m * b^m \rightarrow$ (ii)

To Prove: P(m+1) is true

Now, $(a * b)^{m+1} = (a * b)^m * (a * b)$

$= (a^m * b^m) * (a * b)$ by (ii)

$= a^m * (b^m * a) * b$ [by associative law]

$= a^m * (a * b^m) * b$ since G is abelian.

$= (a^m * a) * (b^m * b)$

$= a^{m+1} * b^{m+1}$.

Hence by Mathematical induction, the result is true for all positive integer n.

Hence $(a*b)^n = a^n * b^n, \forall\, a, b \in G$ is true for every *n.*

PROPERTY 11 : If for any element 'a' in a group (G, $*$), $a^2 = e$ then G is an abelian group.

Proof: Let a, b $\in$ G. Then $(a * b) \in G$ so that $(a * b)^2 = e$.

Since $a \in G$, $a^2 = e \Rightarrow a * a = e$

$b \in G$, $b^2 = e \Rightarrow b * b = e$

Now $(a * b)^2 = e$

$\Rightarrow (a * b) * (a * b) = e * e$

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

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

$\Rightarrow b * (a * b) = a * (b * b)$ [by left cancellation law]

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

$b * a = a * b$ [by right cancellation law]

Hence G is an abelian group.

PROPERTY 12 :If G is a finite group of order n and a $\in$ G then $a^n = e$.

Solution: $(G, *)$ is an finite group of order n.

$\therefore$ The element $a \in G$ is of finite order.

Let $O(a) = m$. Then m is the least positive integer such that

$a^m = e$.

$\therefore$ $O(a)$ divides $O(G)$, m divides n.

$\therefore$ $n = mq$ for some integer q.

$\therefore$ $a^n = a^{mq} = (a^m)^q = e^q = e. \quad \Rightarrow a^n = e.$

PROPERTY 13 :In a group $(G, *)$, the equations $x * a = b$ and $a * y = b$ have unique solutions. (OR)

If a, b $\in$ G, the equation $a * x = b$ has the unique solution $x = a^{-1} * b$. Similarly the equation $a * y = b$ has the unique solution $y = b * a^{-1}$.

Proof: Consider $x * a = b$. Post multiplying by a^{-1}, $x * a = b$

$$x * a * a^{-1} = b * a^{-1}$$

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

$$x = b * a^{-1}$$

To prove uniqueness

Let x_1 and x_2 be two solutions of $x * a = b$. Then $x_1 * a = b$ and $x_2 * a = b$.

$\therefore$ $x_1 * a = x_2 * a$.

$\Rightarrow$ $x_1 = x_2$ by right cancellation law.

In a similar manner, the equation $a * y = b$ has a solution $y = a^{-1} * b$ and this solution is unique.

PROBLEMS ON GROUPS

PROBLEM 1: If $*$ is the binary operation defined on the set R of real numers defined by a $* b = a + b + 2ab$ for all $a,b \in R$.

(a) Verify (R, $*$) is monoid or not?

(b) Is it commutative?

(c) Which elements have inverse and what are they?

Solution:

To verify (a)

(i) Closure property:

For all $a,b \in R$, $a + b \in R$ $and\ 2ab \in R$

Therefore, $a + b + 2ab \in R \Rightarrow$ a $* b \in R$

‘ $*$ ‘ satisfies closure property

(R, $*$) is closure.

(ii) Associative property:

To prove : $a * (b * c) = (a * b) * c \ \ \forall\ a,b,c \in R$

Now ,

$$a * (b * c) = a * (b + c + 2bc)$$
$$= a + (b + c + 2bc) + 2a(b + c + 2bc)$$
$$= a + (b + c + 2bc) + 2ab + 2ac + 4abc$$
$$a * (b * c) = a + b + c + 2ab + 2bc + 2ac + 4abc \ \ ......(1)$$

Consider

$$(a * b) * c = (a + b + 2ab) * c$$
$$=(a + b + 2ab) + c + 2c\,(a + b + 2ab)$$
$$(a * b) * c = a + b + c + 2ab + 2bc + 2ac + 4abc \ \ ....(2)$$

From (1) and (2), $a * (b * c) = (a * b) * c\ \forall\ a,b,c \in R$

‘ $*$ ‘ satisfies associative property

(R, $*$) is associative.

(iii) To find the Identity element:

Let e be the identity element of R

Now $a * e = a \ \ \forall\ \ a \in R$

a+e+2ae = a $\Rightarrow$ (1+2a)e =0 $\Rightarrow$ e =0 $\in R$

Identity element exist.

Since ‵ $*$ ‵ satisfies Closure, Associative and identity properties.

(R, $*$) is a monoid.

(b) To verify commutative property

Consider $a * b$ =a+b+2ab = b+a+2ba = $b * a$

Therefore, $a * b = b * a \ \forall \ a,b \in R$

(R, $*$) is commutative.

(c) To find the inverse element:

Let a' be the inverse element of $a \in R$.

Then $a * a' = e \Rightarrow$ a+a′+2aa′ = e ⇒ a+(1+2a) a′ =0 (since e =0)

⇒ (1+2a) a′ = -a ⇒ a′ = $\frac{-a}{(1+2a)}$ if a $\neq -\frac{1}{2}$.

Hence the inverse element of $a \in R$ is a′ = $\frac{-a}{(1+2a)}$ except a = $-\frac{1}{2}$

PROBLEM 2: Show that (Q^+, $*$) is an abelian group where $*$ defined by $a * b = \frac{ab}{2}$ for all $a,b \in Q^+$.

Solution:

(i) Closure property:

For all $a,b \in Q^+ \Rightarrow ab \in Q^+ \Rightarrow \frac{ab}{2} \in Q^+$

Therefore, $a * b = \frac{ab}{2} \in Q^+ \Rightarrow a * b \in Q^+$

‵ $*$ ‵ satisfies closure property

(Q^+, $*$) is closure.

(ii) Associative property:

To prove : $a * (b * c) = (a * b) * c \ \forall \ a,b,c \in Q^+$

Now ,

$$a * (b * c) = a * \left(\frac{bc}{2}\right)$$

$$= \frac{\frac{abc}{2}}{2}$$

$$a * (b * c) = \frac{abc}{4} \quad \ldots..(1)$$

Consider

$$(a * b) * c = \left(\frac{ab}{2}\right) * c$$

$$= \frac{\frac{abc}{2}}{2}$$

$$(a * b) * c = \frac{abc}{4} \quad \ldots\ldots.(2)$$

From (1) and (2), $a * (b * c) = (a * b) * c \ \forall \ a,b,c \in Q^+$

' $*$ ' satisfies associative property.

$(Q^+, *)$ is associative.

(iii) To find the Identity element:

Let e be the identity element of R

Now, $a * e = a \ \forall \ a \in Q^+$

$\left(\frac{ae}{2}\right)$ = a $\Rightarrow \left(\frac{e}{2}\right)$ = 1 $\Rightarrow$ e =2 $\in Q^+$

Identity element exist.

(iv) To find the inverse element:

Let a' be the inverse element of $a \in Q^+$.

Then $a * a' = e \Rightarrow \left(\frac{a\,a'}{2}\right)$ = e $\Rightarrow \left(\frac{a\,a'}{2}\right)$ = 2 (since e =2)

$\Rightarrow a\,a' = 4 \quad \Rightarrow$ a$'$ = $\frac{4}{a} \in Q^+$

(v) To verify commutative property

Consider $a * b = \left(\frac{ab}{2}\right) = \left(\frac{ba}{2}\right) = b * a$

Therefore, $a * b = b * a \ \forall \ a,b \in Q^+$

$(Q^+, *)$ is commutative.

Hence $(Q^+, *)$ is an abelian group

PROBLEM 3: If S is the set of all ordered pairs (a,b) of real numbers with the binary operation $\oplus$ defined by $(\boldsymbol{a},\boldsymbol{b}) \oplus (\boldsymbol{c},\boldsymbol{d}) = (\boldsymbol{a}+\boldsymbol{c},\ \boldsymbol{b}+\boldsymbol{d})$ where a,b,c,d are real, prove that $(S,\ \oplus)$ is a commutative group.

Solution:

Given S = {(a,b): a, b ∈ R}

Let x,y,z ∈ S where x= (a,b), y=(c,d), z=(e,f) and a,b,c,d,e,f are real numbers.

(i) Closure property:

Let x, y ∈ S

$x \oplus y = (a,b) \oplus (c,d) = (a+c,\ b+d) \in$ S (since a+c, b+d ∈ R)

$\Rightarrow x \oplus y \in$ S

' $\oplus$' satisfies closure property

$(S,\ \oplus)$ is closure.

(ii) Associative property:

To prove : $x \oplus (y \oplus z) = (x \oplus y) \oplus z \quad \forall\ x,y,z \in S$

Now ,

$$x \oplus (y \oplus z) = (a,b) \oplus ((c,d) \oplus (e,f))$$

$$= (a,b) \oplus (c+e,\ d+f)$$

$$x \oplus (y \oplus z) = (a+c+e,\ b+d+f) \text{ ....(1)}$$

$$(x \oplus y) \oplus z = ((a,b) \oplus (c,d)) \oplus (e,f)$$

$$= (a+c, b+d) \oplus (e,f)$$

$$(x \oplus y) \oplus z = (a+c+e,\ b+d+f) \quad \text{.....(2)}$$

From (1) and (2), $a * (b * c) = (a * b) * c \ \forall\ a,b,c \in Q^+$

' $\oplus$ ' satisfies associative property

$(S, \oplus)$ is associative.

(iii) To find the Identity element:

Let x $\in S$ and e=(e_1, e_2) be the identity element of S where $e_1, e_2 \in R$

Now $x \oplus e = x \;\; \forall \;\; x \in S$

$\Rightarrow (a, b) \oplus (e_1, e_2) = (a, b)$

$\Rightarrow (a + e_1,\ b + e_2) = (a, b) \Rightarrow a + e_1 = a$ and $b + e_2 = b$

$\Rightarrow e_1$ =a-a =0 and e_2 =b-b =0

$\Rightarrow (e_1, e_2)$ = (0,0)

Identity element of S is e = (e_1, e_2) = (0,0)

(iv) To find the inverse element:

Let $x' = (a', b') \in S$ where $a', b' \in R$ and $x' = (a', b')$ be the inverse element of $x = (a, b) \in S$.

Now $x \oplus x' = e$

$\Rightarrow (a, b) \oplus (a', b') = (e_1, e_2)$

$\Rightarrow (a + a',\ b + b') = (0, 0) \quad \Rightarrow a + a' = 0$ and $b + b' = 0$

$\Rightarrow a'$ =0-a =-a and b' =0-b =-b

$\Rightarrow x' = (a', b')$ = (-a.-b)

Therefore, the inverse of $x = (a, b)$ is x' = (-a.-b)

So, the inverse axiom is satisfied.

Hence $(S, \oplus)$ is a group

(v) To verify commutative property

Consider $x \oplus y = (a,b) \oplus (c,d) = (a + c,\ b + d)$

$= (c + a,\ d + b)$

$= y \oplus x$

Therefore, $x \oplus y = y \oplus x \;\; \forall\, x, y \in S$

$(Q^+, *)$ is commutative.

Hence $(S, \oplus)$ is an abelian group

PROBLEM 4: Examine G $= \left\{ \begin{pmatrix} a & a \\ a & a \end{pmatrix} : a \neq 0 \in R \right\}$ is a commutative group under matrix multiplication where R is the set of real numbers.

Solution:

To verify (G·, ·) is commutative group

Given G $=\left\{\begin{pmatrix} a & a \\ a & a \end{pmatrix} : a \neq 0 \in R\right\}$

Let A = $\begin{pmatrix} a & a \\ a & a \end{pmatrix}$, B = $\begin{pmatrix} b & b \\ b & b \end{pmatrix}$ and C = $\begin{pmatrix} c & c \\ c & c \end{pmatrix}$ be any three matrices in G and $a \neq 0, b \neq 0, c \neq 0 \in R$.

(i) Closure property:

Let A,B ∈ G

$AB = \begin{pmatrix} a & a \\ a & a \end{pmatrix}\begin{pmatrix} b & b \\ b & b \end{pmatrix} = \begin{pmatrix} 2ab & 2ab \\ 2ab & 2ab \end{pmatrix}$ ∈ G (since 2ab ∈ R)

$\Rightarrow AB \in$ G

$(G, \cdot)$ is closure.

(ii) Associative property:

WKT, matrix multiplication is associative

Therefore A(BC)=(AB)C ∈ G

$(G, \cdot)$ is associative.

(iii) To find the Identity element:

Let I $=\begin{pmatrix} x & x \\ x & x \end{pmatrix} \in G$ be the identity element of G where $x \neq 0 \in R$

Now $AI = A \Rightarrow \begin{pmatrix} a & a \\ a & a \end{pmatrix}\begin{pmatrix} x & x \\ x & x \end{pmatrix} = \begin{pmatrix} a & a \\ a & a \end{pmatrix}$

$\Rightarrow \begin{pmatrix} 2ax & 2ax \\ 2ax & 2ax \end{pmatrix} = \begin{pmatrix} a & a \\ a & a \end{pmatrix}$

$\Rightarrow 2ax = a \Rightarrow x = \frac{1}{2}$

Identity element of G is I = $\begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix}$

Therefore, the identity element exist for $(G, \cdot)$

(iv) To find the inverse element:

Let $A' = \begin{pmatrix} a' & a' \\ a' & a' \end{pmatrix} \in G$ where $a' \neq 0 \in R$ and $A' = \begin{pmatrix} a' & a' \\ a' & a' \end{pmatrix}$ be the inverse element of $A = \begin{pmatrix} a & a \\ a & a \end{pmatrix} \in G$.

Now $A.A' = I$

$\Rightarrow \begin{pmatrix} a & a \\ a & a \end{pmatrix} \begin{pmatrix} a' & a' \\ a' & a' \end{pmatrix} = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix}$

$\Rightarrow \begin{pmatrix} 2aa' & 2aa' \\ 2aa' & 2aa' \end{pmatrix} = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix}$

$\Rightarrow 2aa' = \frac{1}{2} \Rightarrow a' = \frac{1}{4a}$

Therefore, the inverse of $A = \begin{pmatrix} a & a \\ a & a \end{pmatrix}$ is $A' = \begin{pmatrix} \frac{1}{4a} & \frac{1}{4a} \\ \frac{1}{4a} & \frac{1}{4a} \end{pmatrix}$

So, the inverse axiom is satisfied.

Hence $(G, \cdot)$ is a group

(v) To verify commutative property

Since ab = ba $\forall\ a, b \in R$, for any $A = \begin{pmatrix} a & a \\ a & a \end{pmatrix}, B = \begin{pmatrix} b & b \\ b & b \end{pmatrix} \in G$,

we have AB = BA

$(G, \cdot)$ is commutative.

Hence $(G, \cdot)$ is an abelian group or commutative group

PROBLEM 5: Show that the set G ={0,1,2,3,4,5} is a group under addition modulo 6.

Solution:

To Prove: (G, $+_6$) is a group

Given G ={0,1,2,3,4,5}

We can form Cayley table and verify the group axioms

The Cayley table is

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

(i) Closure property:

The body of the table contain only elements of G once is each row and column.

Therefore, $(G, +_6)$ is closure.

(ii) Associative property:

Since usual addition is associative, $+_6$ is associative

[For example, let $2, 3, 5 \in G$

Then $2 +_6 (3 +_6 5) = 2 +_6 2 = 4$

$(2 +_6 3) +_6 5 = 5 +_6 5 = 4$

$2 +_6 (3 +_6 5) = (2 +_6 3) +_6 5$]

$(G, +_6)$ is associative.

(iii) To find the Identity element:

0 is the identity element.

Therefore, the identity element exist for $(G, +_6)$,

(iv) To find the inverse element:

Inverse of 0 is 0.
Inverse of 1 is 5.
Inverse of 2 is 4.
Inverse of 3 is 3.

Hence $(G, +_6)$ is a group

To Prove: $(G\cdot, +_6)$ is an abelian group

(v) To verify commutative property

Since usual addition is commutative, $+_6$ is commutative.

{For example, let $3, 4 \in G$

Then $(3 +_6 4) = 1$

$(4 +_6 3) = 1$

$(3 +_6 4) = (4 +_6 3)$ }

$(G, +_6)$ is commutative.

Hence $(G, +_6)$ is an abelian group or commutative group

PROBLEM 6: Let S = Q x Q be the set of all ordered pairs of rational numbers and given by (a, b) ∗ (x, y) = (ax, ay + b).

(i) Check (S, ∗) is a semi group. Is it associative?
(ii) Also find the identity element of S.

Solution:

To prove: Closure property:

For all $(\mathbf{a}, \mathbf{b}), (\mathbf{c}, \mathbf{d}) \in \mathbf{Q} \times \mathbf{Q}$,

$(a, b) * (x, y) = (ax, ay + b) \in \boldsymbol{Q} \times \boldsymbol{Q}$

' ∗ ' satisfies closure property

(S, ∗) is closure.

To prove: Associative property

Consider [(a, b) ∗ (x, y)] ∗ (c, d) = [(ax, ay + b) ∗ (c, d)]

= [axc, axd + (ay + b)]

= [acx, adx + ay + b] → (i)

Now, (a, b) ∗ [(x, y) ∗ (c, d)] = (a, b) ∗ [xc, xd + y]

= [axc, a(xd + y) + b]

= [axc, axd + ay + b]

= [acx, adx + ay + b] → (ii)

From (i) and (ii), we have

[(a, b) ∗ (x, y)] ∗ (c, d) = (a, b) ∗ [(x, y) ∗ (c, d)]

∴ ∗ is associative.

∴ (S, ∗) is a semi group.

To prove: Commutative property.

(a, b) ∗ (x, y) = (ax, ay + b) → (iii)

(x, y) ∗ (a, b) = (xa, xb + y)

= (ax, bx + y) → (iv)

From (iii) and (iv) (a, b) ∗ (x, y) ≠ (x, y) ∗ (a, b)

∴ (S, ∗) is not commutative.

Existence of identity property.

Let (e_1, e_2) be the identity element of $(S, *)$.

Then for any $(a, b) \in S$, $(a, b) * (e_1, e_2) = (a, b)$

$(a e_1, ae_2 + b) = (a, b) \Rightarrow ae_1 = a$ and $ae_2 + b=b$

$\Rightarrow e_1 = 1$ and $e_2 = \frac{b-b}{a} = 0$ $(a \neq 0)$

$\therefore$ The identity element $= (e_1, e_2) = (1, 0)$.

PROBLEM 7: If Z_6 is the set of equivalence classes generated by the equivalence relation " congruence modulo 6 ", prove that $\{Z_6, x_6\}$ is a monoid where the operation x_6 on Z_6 is defined as $[i] \ x_6 \ [j] = [(i \times j) \ (\text{mod } 6)]$ for any $[i], [j] \in Z_6$. Which elements of the monoid are invertible?

Solution:

Congruence table:

x_6	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]
[2]	[0]	[2]	[4]	[0]	[2]	[4]
[3]	[0]	[3]	[0]	[3]	[0]	[3]
[4]	[0]	[4]	[2]	[0]	[4]	[2]
[5]	[0]	[5]	[4]	[3]	[2]	[1]

The operation x_6 is associative.

For example, $\{[2] \ x_6 \ [4]\} \ x_6 \ [5] = [2] \ x_6 \ [5] = [4]$

Also, $[2] \ x_6 \ \{[4] \ x_6 \ [5]\} = [2] \ x_6 \ [2] = [4]$

We see that [1] is the identity element of $\{Z_6, x_6\}$ as $[1] \ x_6 \ [1] = [1]$ and $[5] \ x_6 \ [5] = [1]$

$\therefore$ The elements [1] and [5] alone are invertible and their inverses are [1] and [5] respectively.

2. CYCLIC GROUP

A group $(G, *)$ is called a cyclic group if for every $x \in G$ can be expressed as $x = a^m$ or $x = ma$ for some $a \in G$ and $m \in Z$.

Here '*a*' is called the generator of the cyclic group G.

Note: A cyclic group can have more than one generator.

Example

Consider the group $(G, \times) = (\{1, -1, i, -i\}, \times)$ under usual multiplication.

We have , $i^1 = i,\ i^2 = -1, i^3 = -1,\ i^4 = 1$

So i is a generator of the group.

Similarly, we have $-i$ is another generator of the group.

Order of a group:

The number of elements in a group $(G, *)$ is called order of a Group and is denoted by $O(G)$ **.**

Order of an element:

Let $(G, *)$ be a group and $a \in (G, *)$ **.** Then the least positive integer n such that $a^n = e$ is called the order of the element *a* .
(i.e., $a^n = e \Leftrightarrow O(a) = n$ **).**

Example

Consider the group $(\{1, -1, i, -i\}, \times)$

$i^1 = i\ ; i^2 = -1\ ; i^3 = -i\ ; i^4 = 1\ ; i^8 = 1\ ; i^{12} = 1, \ldots$
Therefore $O(i) = 4$

THEOREM 2.1: Every cyclic group is an abelian.

PROOF:
Let $(G, *)$ be a cyclic group with generator 'a'.

To prove: $(G,*)$ is abelian .i.e $(G,*)$ is commutative.

Let $b, c \in (G,*)$

$\Rightarrow b = a^m, c = a^n$ since a is the generator of G

Consider

$b * c = a^m * a^n$

$= a^{m+n}$

$= a^{n+m}$

$= a^n * a^m$

$= c * b$

Therefore, $(G,*)$ is commutative.

Hence, $(G,*)$ is abelian.

Hence, every cyclic group is an abelian.

Note: The converse of the above theorem need not be true.
i.e., Every abelian group need not be cyclic.

THEOREM 2.2:

If a is a generator of the cyclic group $(G,*)$, then a^{-1} is also a generator of $(G,*)$.

PROOF:

Let $(G,*)$ be a cyclic group with generator 'a'.

Then every element $x \in G$ can be written as $x = a^m$, where m is an integer.

$x = a^m$

$x = (a^{-1})^{-m}$, where $-m$ is an integer

$\Rightarrow a^{-1}$ is also a generator of $(G,*)$

THEOREM 2.3:

Let $(G,*)$ be a finite cyclic group generated by $a \in G$.

If $O(G)=n$ then $a^n = e$ so that $G = \{a, a^2, ..., a^n = e\}$ where e is the identity element for $*$ in G.

Furthermore, n is the least positive integer for which $a^n = e$.

PROOF:

Let $(G,*)$ be a cyclic group of order n. i.e., $O(G)=n$

Let $a \in G$ be the generator of G.

To prove this theorem, we should prove two result:

Claim 1: n is the least positive integer for which $a^n = e$.

Claim 2: Every element of $G = \{a, a^2, \ldots, a^n = e\}$ are distinct.

To prove: claim1: n is the least positive integer for which $a^n = e$.

Contradictorily, assume that there exist $m < n$ such that $a^m = e$.
Let $x \in G$
Then $x = a^k$ since a is the generator of G.

Divide *k* by *m*.

$$m)\ k\ (q$$
$$\overline{\quad r \quad}$$

By division algorithm, $k = mq + r,\ 0 \le r < m$

Consider,

$$x = a^k = a^{mq+r} = a^{mq} * a^r = \left(a^m\right)^q * a^r = e^q * a^r = a^r$$

For $x \in G$ We get, $x = a^r,\ 0 \le r < m$.

Therefore every element of G is of the form $x = a^r,\ 0 \le r < m$.

$$\Rightarrow G = \{a^0, a^1, a^2, \ldots, a^{m-1}\}$$

$\Rightarrow O(G) = m < n$ which is a contradiction to the fact that $O(G) = n$.

Therefore our assumption is wrong.

Hence n is the least positive integer for which $a^n = e$.

To prove: claim 2: Every element of $G = \{a, a^2, \ldots, a^n = e\}$ are distinct.

Contradictorily, assume that

$$a^i = a^j \text{ for some } i < j$$

Post operating by a^{-i} on both sides

$$a^i * a^{-i} = a^j * a^{-i}$$

$$e = a^{j-i}$$

Hence we get $a^{j-i} = e$ for $j - i < n$ which is a contradiction to **claim-1.**

Hence our assumption is wrong.

Therefore All the elements of G are distinct.

Hence the Theorem.

3. SUBGROUP

Definition: Subgroup: Let $(G, *)$ be a group and $H \subseteq G$.

$(H, *)$ is called a Sub-group of $(G, *)$ if $(H, *)$ is itself a group.

i.e., $(H, *)$ is (i) closed (ii) Associative (iii) Existence of identity
(iv) Every element in H has Inverse with respect to $*$.

Example:

(i) $(Q, +)$ is a subgroup of $(R, +)$.
(ii) $(R, +)$ is a subgroup of $(C, +)$.

THEOREM 3.1

The identity element of a subgroup is the same as the identity element of the group.

PROOF:

Let $(G, *)$ be group.
Let $(H, *)$ be a sub-group.
Let e be the identity element of the group $(G, *)$.

To Prove: e is the identity element of the subgroup $(H, *)$.

If possible assume that e' be the identity element of $(H, *)$.
Let $a \in H \Rightarrow a \in G$
Since e is the identity element of $(G, *)$, we have

$a * e = a$ --------------------------(1)

Since e' is the identity element of $(H, *)$, we have

$a * e' = a$ --------------------------(2)

From (1) & (2) we have

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

$$e = e' \quad [\ left\ cancellation\ law\ ]$$

Hence identity element of a subgroup is the same as the identity element of the group.

THEOREM 3.2:

NECESSARY AND SUFFICIENT CONDITION FOR A SUBGROUP

The necessary and sufficient condition for a non-empty subset H of a group G to be a subgroup is $a, b \in H \Rightarrow a * b^{-1} \in H, \forall a, b \in H$.

Necessary Part:

Assume that H is a subgroup of G.
$\Rightarrow$ H is a group itself. i.e., H is closed, associative, has identity and inverse exist.

To Prove: $a, b \in H \Rightarrow a * b^{-1} \in H, \forall a, b \in H$

Let $a, b \in H$

We have $b \in H \Rightarrow b^{-1} \in H$ (Existence of inverse)

Hence $a, b^{-1} \in H \Rightarrow a * b^{-1} \in H$ (Closure Property)

Therefore $a, b \in H \Rightarrow a * b^{-1} \in H, \forall a, b \in H$.

Sufficient Part:

Assume that $a, b \in H \Rightarrow a * b^{-1} \in H, \forall a, b \in H$

To Prove: H is a subgroup of G.

i.e., To prove $(H, *)$ is (i) close (ii) Associative(iii) Existence of identity (iv) Every element in H has Inverse with respect to $*$.

Existence of identity:

Choose $b = a$

$So,\ a, a \in H \Rightarrow a * a^{-1} \in H \Rightarrow e \in H$

Hence Existence of identity.

Every element in H has Inverse with respect to $*$:

Let $e, a \in H \Rightarrow e * a^{-1} \in H \Rightarrow a^{-1} \in H$

Therefore $a \in H \Rightarrow a^{-1} \in H$.

Hence every element has inverse in H.

Closure:

Let $a, b \in H$

We have $b \in H \Rightarrow b^{-1} \in H$ (Existence of inverse)

Hence $a, b^{-1} \in H \Rightarrow a * (b^{-1})^{-1} \in H$ (Closure Property)

$\Rightarrow a * b \in H$

Therefore $a, b \in H \Rightarrow a * b \in H$

Hence H is closed.

Associative:

Since $(G, *)$ is a group, $(G, *)$ is Associative.

Hence $(H, *) \subset (G, *)$ is also associative.

Hence $(H, *)$ is a subgroup of $(G, *)$.

Another form of proof:

Prove that the necessary and sufficient conditions for a non-empty subset H of a group G to be a subgroup is a, b $\in$ H $\Rightarrow$ a $*$ b^{-1} $\in$ H.

(OR)

A non-empty subset H of a group G is a subgroup of G iff a $*$ b^{-1} $\in$ H $\forall$ a, b $\in$ H

Proof:

Necessary condition: Let us assume that H is a subgroup of G.

Then H itself is a group under $*$.

$\therefore$ a, b $\in$ H $\Rightarrow$ a $*$ b $\in$ H (closure property)

Since b $\in$ H, b^{-1} $\in$ H

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

Sufficient condition: Let a $*$ b^{-1} $\in$ H for a, b $\in$ H

Now we prove that H is a subgroup of G.

Let a $\in$ H. $\therefore$ a^{-1} $\in$ H $\Rightarrow$ a $*$ a^{-1} $\in$ H $\Rightarrow$ e $\in$ H

Hence the identity element 'e' exists in H

If a $\in$ H is any element then a, e $\in$ H $\Rightarrow$ e $*$ a^{-1} $\in$ H $\Rightarrow$ a^{-1} $\in$ H

Every element 'a' of H has its inverse a^{-1} in H.

Theorem 3.3:

The intersection of two subgroups of a group G is also a subgroup of G.

Proof: Let H and K be two subgroups of a group (G, $*$). As e $\in$ H and e $\in$ K, e $\in$ H $\cap$K where e is the identity element of G.

So H $\cap$K is non-empty $\rightarrow$ (i).

Let a, b $\in$ H $\cap$K. Then a, b $\in$ H and a, b $\in$ K. Since H and K are subgroups of G,

a $*$ b^{-1} $\in$ H and a $*$ b^{-1} $\in$ k. $\therefore$ a $*$ b^{-1} $\in$ H $\cap$K $\rightarrow$ (ii)

From (i) and (ii) , H $\cap$K is a subgroup of G.

RESULT:

The union of two subgroups need not be a subgroup.

PROOF:

The proof is given by the following example:

Consider the group $(Z,+)$, where Z is the set of integers.

Consider the following two subgroups $(H_1,+)$ and $(H_2,+)$ of $(Z,+)$ where

$H_1=\{.........., -4, -2, 0, 2, 4 ,..........\}$ and

$H_2=\{.........., -6, -3, 0, 3, 6 ,..........\}$

$\Rightarrow H_1 \cup H_2=\{.........., -6, -4, -3, -2, 0, 2, 3, 4, 6 ,..........\}$

Clearly $2, 3 \in H_1 \cup H_2$.

But $2 + 3 = 5 \notin H_1 \cup H_2$

$\Rightarrow H_1 \cup H_2$ is not closed.

Therefore $H_1 \cup H_2$ is not a subgroup.

Hence, The union of two subgroups need not be a subgroup.

4. COSETS

DEFINTION: Let (H, $*$) be a subgroup of a group (G, $*$).

Left coset of H: For any $a \in G$, the left coset of H is defined by

$a * H = \{a * h : h \in H\}$.

Right coset of H: For any $a \in G$, the right coset of H is defined by

$H * a = \{h * a : h \in H\}$.

Note: The right and left cosets are also denoted by aH and Ha respectively.

Example: Consider the group G = {1, -1 ,i, -i} and subgroup H = {1, -1} under the usual multiplication. (i.e $*$ $is\ multiplication$)

The left cosets are

1* H =1H = {1, -1}

-1*H =-1H= {-1 ,1} = {1, -1} = 1H

i * H = iH = {i, -i}

-i * H = -iH = {-i, i} = {i, -i} =iH.

Therefore ,the distinct left cosets are 1H = {1, -1} and iH = {i, -i}.

Note:

(i) Both left and right cosets of H in G is non empty
(ii) Since $e \in H$, $e * H = H * e = H$
(iii) $H * a$ and $a * H$ are also subsets of G
(iv) If G is abelian, then $a * H = H * a$
(v) The union of all left or right cosets of H in G is equal to G
(vi) Cosets are either disjoint or identical

Example: consider the group $Z_4 = \{[0],[1],[2],[3]\}$ of integers modulo 4. Let H = $\{[0], [2]\}$ be a subgroup of Z_4 under $+_4$ (addition modulo 4).

Solution: Given $(H, +_4)$ is a subgroup of a group $(Z_4, +_4)$

The left cosets of H are

[0] + H = $\{[0], [2]\}$ = H

[1] + H = $\{[1], [3]\}$

[2] + H = $\{[2], [4]\}$ =$\{[2], [0]\}$ =$\{[0], [2]\}$ = H

[3] + H = $\{[3], [5]\}$ = $\{[3], [1]\}$ = $\{[1], [3]\}$ = [1] + H

Therefore , the two distinct left cosets are [0] + H and [1] + H of H in Z_4 .

Note: The union of all distinct left or right cosets form a group

In previous example, union of [0] + H and [1] + H is Z_4

since [0] + H U [1] + H =$\{[0], [2]\}$ U $\{[1], [3]\}$ = $\{[0],[1],[2],[3]\}$ = Z_4

Theorem 4.1: Any two right (or left) cosets of H are either identical or disjoint.

Proof: Let $H * a \; and \; H * b$ be two right cosets of a subgroup h of G.

Let $a,b \in G$.

To prove : $(H * a) \cap (H * b) = \emptyset$ (or) $(H * a) = (H * b)$

Suppose $(H * a) \cap (H * b) \neq \emptyset$, then there exists an element

$x \in (H * a) \cap (H * b)$

$\Rightarrow x \in (H * a) \; and \; x \in (H * b)$

If $x \in (H * a) \;\; then \; H * x = H * a$ -----(1)

[by theorem, $if \; a \in (H * b) \;\; then \;\; H * a = H * b$]

If $x \in (H * b) \;\; then \; H * x = H * b$………(2)

From (1) and (2)

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

Hence the proof.

Theorem : Let (H, $*$) be a subgroup of a group (G, $*$).The set of left (or right) cosets of H in G forms a partition of G.

Proof: Given (G, $*$) be a group and (H, $*$) be a subgroup.

Let us first prove that every element of G appears in atleast one left coset.

Let $a * H = \{a * h : h \in H\}$ be a left coset of H for all $a \in G$.

For $e \in H \Rightarrow a * e \in a * H \Rightarrow a \in a * H$.

Therefore, every element of G appears in atleast one left coset.

We know that , any two left (or right) cosets of H are either identical or disjoint.

Hence, each element of G appears in exactly one and only one left coset of H in G.

Since the union of all distinct left (or right) cosets of H in G is equal to G, the set of left (or right) cosets forms a partition of G.

Lagrange's theorem: If H is a subgroup of a finite group then order of H divides order of G [i.e., O(H)/O(G)]

(or)

The order of each subgroup of a finite group is a divisor of the order the group.

Proof: Let (G, $*$) be a finite group of order n. i.e., O(G) = n

and (H, $*$) be a subgroup of order m. i.e., O(H) = m.

To prove : $O(H)$ *divides* $O(G)$ *i.e.,* $O(H)/O(G)$ *i.e.,* m/n

i.e., $\frac{n}{m} = k$, k *a constant* i.e., $\frac{O(G)}{O(H)} = k$

Since G is a finite group of order n, the number of left cosets of H in G is finite.

Let k be the number of **distinct** left cosets of H in G.

Let the k cosets be $a_1 * H, a_2 * H, a_3 * H, \ldots\ldots a_k * H$.

We know that the left cosets of H form a partition of G.

Therefore , G = $(a_1 * H) \cup (a_2 * H) \cup (a_3 * H) \ldots\ldots \cup (a_k * H)$

$\Rightarrow O(G) = O[(a_1 * H) \cup (a_2 * H) \cup (a_3 * H) \ldots\ldots \cup (a_k * H)]$

$\Rightarrow O(G) = O(a_1 * H) + O(a_2 * H) + O(a_3 * H) \ldots\ldots + O(a_k * H)$

$\Rightarrow O(G) = O(H) + O(H) + O(H) \ldots\ldots + O(H)$ [since $(a * H) = O(H)$]

$\Rightarrow O(G) = k\, O(H)$

$\Rightarrow$ n = km

$\Rightarrow \frac{n}{m} = k$

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

$\Rightarrow \; O(H)/O(G)$

$\Rightarrow \; O(H) \; divides \; O(G)$

Hence the proof.

5. NORMAL SUBGROUPS

A subgroup (H, $*$) of a group (G, $*$) is said to be a normal subgroup, for every $x \in G$ and for $h \in G$ if $x * h * x^{-1} \in H$ $i.e,\; x * H * x^{-1} \subseteq H$.

Another form of definition: A subgroup (H, $*$) of a group (G, $*$) is called a normal subgroup if $x * h = h * x \; \forall \; x \in G$.

(or) A subgroup H of a group G is called a normal subgroup if $xH = Hx \; \forall \; x \in G$.

Theorem 5.1: A subgroup (H, $*$) of a group (G, $*$) is normal subgroup if and only if $\mathrm{x * h * x^{-1} = H} \;\; \forall \, \mathrm{x \in G}$ and $\mathrm{h \in H}$

Proof:

Necessary Part:

$Let\; x * h * x^{-1} = H \;\; \Rightarrow \;\; x * H * x^{-1} \subseteq H \;\; \forall \, x \in G$

$\Rightarrow$ H is a normal subgroup of G

Sufficient Part:

Conversely, assume that H is a normal subgroup of G.

$\Rightarrow x * H * x^{-1} \subseteq H \;\; \forall \, x \in G$ ....(1)

Now $x \in G \; \Rightarrow \; x^{-1} \in G$

i.e., $x^{-1} * H * (x^{-1})^{-1} \subseteq H \;\; \Rightarrow \; x^{-1} * H * x \subseteq H$

$\Rightarrow \; x * x^{-1} * H * x * x^{-1} \subseteq x * H * x^{-1}$

$\Rightarrow e * H * e \subseteq x * H * x^{-1}$

$\Rightarrow H \subseteq x * H * x^{-1}$ ....(2)

From (1) and (2), we get $x * h * x^{-1} = H \;\; \forall \, x \in G$ and $h \in H$

Theorem : *The intersection of any two normal subgroups of a group is a normal subgroup of a group.*

(or)

If H and K are normal subgroups of a group G then H ∩ K is also a normal subgroup of a group G.

Proof: Let (H, $*$) and (K, $*$) be two normal subgroups of a group (G, $*$).

Given H and K are normal subgroups

$\Rightarrow$ H and K are subgroups of G.

By theorem, the intersection of any two subgroups is also a subgroup.

Therefore, H ∩ K is a subgroup of G.

To Prove: H ∩ K is a normal subgroup of G.

Let $x \in G$ and $h \in \mathrm{H} \cap \mathrm{K}$

i.e., $x \in G$ and [$h \in \mathrm{H}$ & $h \in \mathrm{K}$]

$\Rightarrow$ $x \in G$, $h \in H$ and $\in G$, $h \in K$

$\Rightarrow x * h * x^{-1} \in H$ and $x * h * x^{-1} \in K$ (since H and K are normal subgroup of G)

$\Rightarrow x * h * x^{-1} \in \mathrm{H} \cap \mathrm{K}$

$\Rightarrow$ H ∩ K is a normal subgroup of G.

Theorem : *Every subgroup of an abelian group is a normal subgroup.*

Proof:

Let G be an abelian group and H be a subgroup of G.

To Prove: H is a Normal subgroup of G

Consider $x * H * x^{-1} = x * (H * x^{-1})$

$$= x * (x^{-1} * H) \ \ (\text{G is an abelian})$$

$$= (x * x^{-1}) * H$$

$$= e * H$$

$$x * H * x^{-1} = H$$

$\Rightarrow$ $x * H * x^{-1} = H$ for all $x \in G, h \in H$

Hence, H is a normal subgroup of G

6.HOMOMORPHISM

Group Homomorphism:

Let (G, $*$) and (H, Δ) be any two groups. A mapping $f : G \longrightarrow H$ is called group homomorphism if $f(a * b) = f(a)\, \Delta\, f(b)$ for all $a,b \in G$.

(or) Let (G, $*$) and (G′, $*$) be two groups. A mapping $f : G \longrightarrow G'$ is called group homomorphism if $f(a * b) = f(a) * f(b)$ for all $a,b \in G$.

Isomorphism:

Let (G, $*$) and (H, Δ) be any two groups. A mapping $f : G \longrightarrow H$ is called an isomorphism if

(i) f is homomorphism *i.e.,* $f(a * b) = f(a)\, \Delta\, f(b)$ for all $a,b \in G$.
(ii) *f is ono to one (injective)*
(iii) *f is onto (surjective).*

In otherwords, a bijective homomorphism is said to be an isomorphism.

Another definition of Isomorphism:

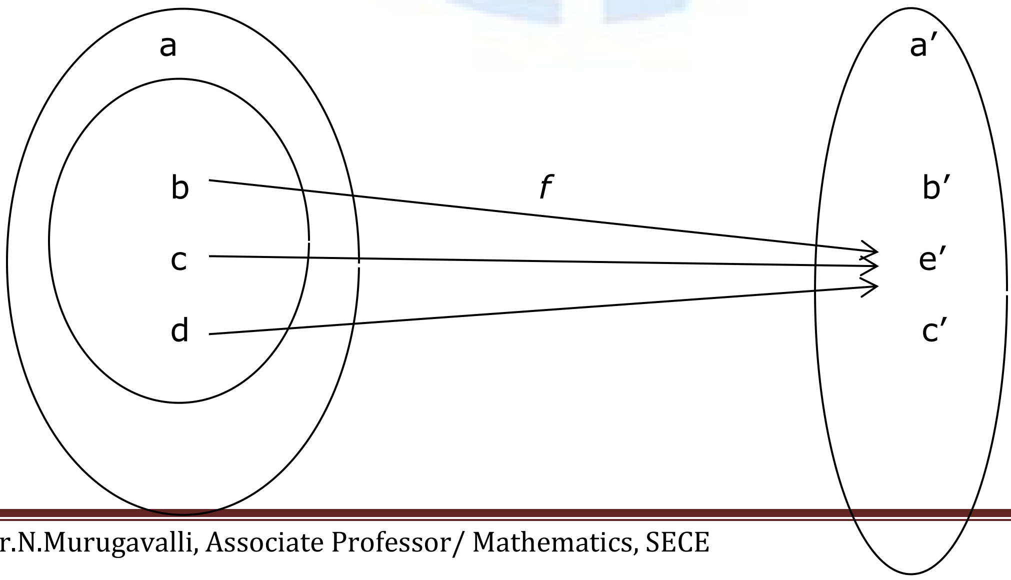
Let (G, $*$) and (G′, $*$) be any two groups. A homomorphism $f : G \longrightarrow G'$ is called an isomorphism if f is one to one and onto.

Then we say that G and G′ are isomorphic and it can be written as G≅G′.

Kernel of a homomorphism: Definition:

Let f : G $\longrightarrow$ G′ be a group homomorphism. The set of elements of G which are mapped into e′ (i.e., e′ is an identity element of G′) is called the kernel of f and it is denoted by ***ker(f)*** .i.e., *ker(f)* $= \{ x \in G \,/\, f(x) = e' \}$

for example,



e d'

G G'

Here *ker(f)* = {b,c,d}.

Quotient group or Factor group:

Let (H, $*$) be a normal subgroup of a group (G, $*$) and G/H denotes the set of all left (or right) cosets of H in G. i.e., G/H = $\{a * H : \forall\, a \in G\}$. Then an algebraic structure (G/H, $\oplus$) is said to be a quotient group if $(a * H) \oplus (b * h) = (a * b) * H \;\forall\, a,b \in G$.

Natural Homomorphism:

Let (H, $*$) be a normal subgroup of a group (G, $*$). A mapping *f : G* $\longrightarrow$ *G/H such that* $f(x) = H * x$, $\forall\, x \in G$ is called a natural homomorphism of the group G onto the quotient group G/H.

Theorem 6.1: Homomorphism preserves identities,inverses and subgroup.

Proof: Let f : (G, $*$) $\longrightarrow$ (G′, $*$) be a homomorphism

To prove: Homomorphism preserves identities

Let $a \in G$. Clearly $f(a) \in G'$.

Now $f(a) * e' = f(a)$ (since e′ is the identity element of G′)

$= f(a * e)$ (since e is the identity element of G)

$f(a) * e' = f(a) * f(e)$ (since f is homomorphism)

$\Rightarrow f(e) = e'$.

Therefore, f preserves identities

To prove: Homomorphism preserves inverses

Let $a \in G$. Since G is group, $a^{-1} \in G$

Now $f(e) = e'$

$f(a * a^{-1}) = e'$ [$a * a^{-1} = a^{-1} * \mathrm{a} = \mathrm{e}$]

$f(a) * f(a^{-1}) = e'$

Therefore $f(a^{-1})$ is the inverse of $f(a)$

$i.e., [f(a)]^{-1} = f(a^{-1}),$

Therefore, f preserves inverses.

To prove: Homomorphism preserves subgroup

Let H be a subgroup of G. Then $f(H) = \{f(h) / h \in H\}$

Since H is non empty, e $\in H$.

If $h,k \in H$ then $h * k^{-1} \in H$ [since H is a subgroup]

Let $h * k^{-1} = m$

Now we have to prove that f(H) is a subgroup of G'.

i.e., $h',k' \in f(H) \Rightarrow h' * (k')^{-1} \in f(H)$

Let $h',k' \in f(H)$. [$since\ f(h) = h'\ and\ f(k) = k'$]

Consider $h' * (k')^{-1} = f(h) * (f(k))^{-1}$

$= f(h) * (f(k^{-1})$

$= f(h * k^{-1})$

$= f(m) \in f(H)$

$h',k' \in f(H) \Rightarrow h' * (k')^{-1} \in f(H)$

Therefore , f(H) is a subgroup of G'.

Hence, f preserves subgroup

Thereom 6.2: If f : (G, $*$) $\longrightarrow$ (G', $*$) is a homomorphism then the Ker(f) is a normal subgroup of G

Proof: WKT, *ker(f)* = { $x \in G$ / *f(x)* = e' } , $e' \in G'$

To Prove: **Ker(f) is a normal subgroup of G**

i.e., we have to prove the following

(i) ker*(f)* is non-empty

(ii) *ker(f)* is a subgroup of G

(iii) *ker(f)* is a normal subgroup of G

Proof of (i): *ker(f)* is non-empty

Since f(e) = e' is always true.

Therefore, atleast $e \in ker(f)$

Hence, ker(f) is non empty.

Proof of (ii): *ker(f)* is a subgroup of G i.e., it is enough to prove that $a,b \in ker(f) \Rightarrow a * b^{-1} \in \ker(f)$

Let $a,b \in ker(f)$. Then $f(a) = e'$ and $f(b) = e'$

$f(a * b^{-1}) = f(a) * f(b^{-1})$

[since *f* is a group homomorphism, $f(a * b) = f(a) * f(b)$]

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

$\Rightarrow f(a * b^{-1}) = e' * (e')^{-1}$

$\Rightarrow f(a * b^{-1}) = e' * e'$

$\Rightarrow f(a * b^{-1}) = e'$

$\Rightarrow a * b^{-1} \in ker(f)$

Therefore, $a,b \in ker(f) \Rightarrow a * b^{-1} \in \ker(f)$

Hence, *ker(f)* is a subgroup of G

Proof of (iii): *ker(f)* is a normal subgroup of G.
i.e., $x * h * x^{-1} \in ker(f)$ for all $x \in G$, $h \in Ker(f)$

i.e., it is enough to prove that $f(x * h * x^{-1}) = e'\ \forall x \in G \text{ and } h \in ker(f)$

Now $f(x * h * x^{-1}) = f(x) * f(h) * f(x^{-1})$

[since *f* is a group homomorphism, $f(a * b) = f(a) * f(b)$]

$\Rightarrow f(x * h * x^{-1}) = f(x) * e' * f(x^{-1})$ [$h \in Ker(f),\ f(h) = e'$]

$\Rightarrow f(x * h * x^{-1}) = f(x) * f(x^{-1})$

$\Rightarrow f(x * h * x^{-1}) = f(x * x^{-1})$ [$since\ x * x^{-1} = e$]

$\Rightarrow f(x * h * x^{-1}) = f(e)$

$\Rightarrow f(x * h * x^{-1}) = e'$

$\Rightarrow x * h * x^{-1} \in ker(f)$ for all $x \in G$, $h \in Ker(f)$

Hence, *ker(f)* is a normal subgroup of G

Theorem 6.3: Fundamental theorem on homomorphism of groups:

Every homomorphic image of a group G is isomorphic to some quotient group of G

(or)

Let f : (G, $*$) $\longrightarrow$ (G′,$*$) be a onto homomorphism of groups with Kernel K. Then $G/K \cong$ G′.

Proof: Let f : (G, $*$) $\longrightarrow$ (G′,$*$) be a homomorphism of groups .

Let G′ be the homomorphic image of group G.

Then f is a homomorphism of G onto G′.

Let K be the Kernel of this homomorphism

i.e., K = *ker(f)* = { $x \in G$ / *f(x)* = *e′* } , $e' \in G'$.

Clearly K is a normal subgroup of G . (by theorem 1.2)

Define $\emptyset$: G/K $\longrightarrow$ G′ by $\emptyset(K * a) = f(a)$ for all $a \in G$.

To Prove: $G/K \cong$ G′ i.e., G/K is isomorphic to G′.

i.e., $f(a) \in G'$ $for\ all\ a \in G\ and\ K * a \in G/K$

Define $\emptyset$: G/K $\longrightarrow$ G′ by $\emptyset(K * a) = a$ for all $a \in G$.

To prove this, it is enough to prove the following

(i) $\emptyset$ is well defined
(ii) $\emptyset$ is one to one
(iii) $\emptyset$ is onto
(iv) $\emptyset$ is homomorphism

Claim (i): $\emptyset$ is well defined

i.e., We have to prove that $K * a = K * b \Rightarrow \emptyset(K * a) = \emptyset(K * b)$

Now $K * a = K * b$

$\Rightarrow a * b^{-1} \in K$ (since K is a normal subgroup)

$\Rightarrow f(a * b^{-1})$ = e′

$\Rightarrow f(a) * f(b^{-1}) = e'$

$\Rightarrow [f(a) * (f(b))^{-1}] * f(b) = e' * f(b)$

$\Rightarrow f(a) * [(f(b))^{-1} * f(b)] = e' * f(b)$

$\Rightarrow f(a) * e' = e' * f(b)$

$\Rightarrow f(a) = f(b)$

$\Rightarrow \emptyset(K * a) = \emptyset(K * b)$

$K * a = K * b \Rightarrow \emptyset(K * a) = \emptyset(K * b)$

$\emptyset$ is well defined

Claim (ii): $\emptyset$ is one to one

To prove: $\emptyset(K * a) = \emptyset(K * b) \Rightarrow K * a = K * b$

Now $\emptyset(K * a) = \emptyset(K * b) \Rightarrow f(a) = f(b)$

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

$\Rightarrow f(a) * f(b^{-1}) = e'$

$\Rightarrow f(a * b^{-1}) = e'$

$\Rightarrow a * b^{-1} \in K$

$\Rightarrow K * a = K * b$

Therefore, $\emptyset(K * a) = \emptyset(K * b) \Rightarrow K * a = K * b$

$\emptyset$ is one to one.

Claim (iii) : $\emptyset$ is onto

Let $y \in G'$ be any element.

Since f is onto, y = f(a) ,$\forall\ a \in G$

$\emptyset(K * a) = f(a) = y.$

$\emptyset\ is\ onto.$

Claim (iv) : $\emptyset$ is homomorphism

Now $\emptyset((K * a) * (K * b)) = \emptyset(K * (a * b))$

$= f(a * b)$

$= f(a) * f(b)$

$\emptyset((K * a) * (K * b)) = \emptyset(K * a) * \emptyset(K * b)$

Therefore, $\emptyset$ is a bijective homomorphism

Hence, $\emptyset$ is an isomomorphism between G/K and G'.

i.e., $G/K \cong$ G'

Permutation Group:

Let S be a non empty set. A bijective function f: $S \to S$ is called permutation . If S has n elements, then the permutation is said to be of degree n.

Note:

1. The set of all permutations on a set of n symbols is denoted by S_n.

2. S_n is a group under composition of functions as operation. The group S_n is called the permutation group on n symbols. It is also known as symmetric group of degree n anf $O(S_n) = n!$.

Theorem 6.4: Cayley's Theorem:

Statement: Every finite group of order n is isomorphic to a permutation group of degree n.

Proof: Let G be a finite group of order n. i.e., O(G) = n.

Step 1: To form a permutation set

Let $a \in G$ be any element. Define a function $f_a : G \longrightarrow G$ by $f_a(x) = a * x$

Claim(i) : f_a is one to one

$f_a(x) = f_a(y) \Rightarrow a * x = a * y \Rightarrow x = y$.

f_a is one to one.

Claim(ii) : f_a is onto

Let $y \in G$. Then $f_a(a^{-1} * y) = a * (a^{-1} * y) = (a * a^{-1}) * y = e * y = y$.

f_a is onto.

Thus $f_a : G \to G$ is one to one and onto function and so, it is permutation set of degree n.

Therefore, permutation set G' = $\{f_a / \in G \}$.

Step 2: G' is a group under composition function operation.

Let G' = $\{f_a / \in G \}$.

Closure property:

Let $f_a , f_b \in G'$.

Now $(f_a \circ f_b)(x) = f_a[f_b(x)]$

$= f_a(b * x]$

$= a * (b * x)$

$= (a * b) * x$

$(f_a \circ f_b)(x) = f_{a*b}(x)$

$\Rightarrow (f_a \circ f_b) = f_{a*b} \in G'$ [since $a,b \in G \Rightarrow a * b \in G$]

$\Rightarrow (f_a \circ f_b) \in G'$.

Hence , G' is closed under composition function operation.

Associative property:

Composition function always satisfies associative property.

Identity and Inverse property:

It is obvious that $f_e \in G'$ is the identity element and $f_{a^{-1}} \in G'$ is the inverse of $f_a \in G'$.

Hence G' is a group under composition function operation.

Step 3: G and G' are isomorphic (or) $\emptyset$ is an isomorphism

Define $\emptyset : G \to G'$ by $\emptyset(a) = f_a \; \forall \; a \in G$.

Claim (a) : $\emptyset$ is one to one

To prove: $\emptyset(a) = \emptyset(b) \Rightarrow f_a = f_b \Rightarrow f_a(x) = f_b(x) \Rightarrow a * x = b * x \Rightarrow a = b$

Therefore, $\emptyset(a) = \emptyset(b) \Rightarrow a = b$.

Hence, $\emptyset$ is one to one

Claim (b) : $\emptyset$ is onto

Since f_a is onto, $\emptyset(a)$ is also onto.

Claim (c) : $\emptyset$ is a homomorphism

Consider for any $\forall \; a , b \in G$,

$\emptyset(a * b) = f_{a*b} = f_a \circ f_b = \emptyset(a) \circ \emptyset(b) \; \forall \; a,b \in G$.

Therefore, $\emptyset$ is a homomorphism.

Hence, G and G' are isomorphic.