NELCO

Sweet Chocolate

SUN BOOK INDUSTRIES
Ph: 223820
KUNNAMKULAM.

my FAVOURITE

soorajss1729@gmail.com
+91-9400635788

INDEX

Appendix : 2-(1)
Group theory

Name SOORAJ.S. Sub.

Std Div. Roll No.

S. No	Topic	Page No	Date	Grade/Marks	Signature
	QUANTUM COMPUTATION & QUANTUM INFORMATION				
	- Nielsen & Chuang				

a group (G, ✶) satisfies following axioms:

1. Closure: $\ast : G \times G \to G$
2. Associativity: (a ✶ b) ✶ c = a ✶ (b ✶ c), for any a, b, c ∈ G.
3. Identity: There exists an element e in G, such that for all a ∈ G, a ✶ e = e ✶ a = a.
4. Inverse: For any a ∈ G, there exist a unique a' such that a ✶ a' = a' ✶ a = e.

Examples:

(1) $\mathbb{Z}/n\mathbb{Z}$, fancy notation for the integers mod n under addition

(2) $(\mathbb{Z}/n\mathbb{Z})^\times$, more fancy notation for the integers mod n under multiplication. IMPORTANT: the elements of this set are NOT all integers mod n, but rather all integers RELATIVELY PRIME to n. See if you can show how these relatively prime elements

(3) $\mathbb{Z}$, the integers under addition. Groups don't have to be finite. Also note that you can't make the integers into a group under multiplication, since elements like 2 don't have a multiplicative inverse (i.e. an element y such that $2y = 1$, since $1/2$ isn't in the integers). But in Math 152, we mainly only care about examples of the type

$n\mathbb{Z}$ is the set of integers that are multiples of n

$\mathbb{Z}/n\mathbb{Z}$ is the "Quotient group."

It is the set of remainders when we choose an integer and subtract members of $n\mathbb{Z}$

You might know it as integers mod n.

And you might also see it as $\mathbb{Z}_n$. If nothing is said about the group operation, assume it is addition. But it really is better to be explicit about those things. $\mathbb{Z}_n^+$

$\mathbb{Z}/n\mathbb{Z}^\times$ or $\mathbb{Z}_n^\times$ would be a group of integers mod n with the operation of multiplication.

$\mathbb{Z}/4\mathbb{Z} = \{0, 1, 2, 3\}$ form a group with respect to addition $(\mathbb{Z}/4\mathbb{Z}, +)$

To form a group with multiplication, with the same set, we need to throw out some elements. $2 \in \mathbb{Z}/4\mathbb{Z}$ is bad, because it has no inverse, also 0 has no inverse. We're left with $\{1, 3\}$, so $(\mathbb{Z}/4\mathbb{Z})^\times = (\{1, 3\}, \times)$.

A ring (R, +, ×) satisfies the following axioms:

1. (R, +) is a **commutative group**

2. Associativity: $(a \times b) \times c = a \times (b \times c)$, for any $a, b, c \in R$.

3. Distributivity: $(a + b) \times c = a \times c + b \times c$.

Examples:

(1) Both the examples $\mathbb{Z}/n\mathbb{Z}$ and $\mathbb{Z}$ from before are also RINGS. Note that we don't require multiplicative inverses.

(2) $\mathbb{Z}[x]$, fancy notation for all polynomials with integer coefficients. Multiplication and addition is the usual multiplication and addition of polynomials.

A field (F, +, ×) satisfies the following axioms:

1. (F, ×) is a **commutative ring.**
2. Identity: There exists a multiplicative identity 1 in F such that a × 1= 1 × a = a, for all a ∈ F.
3. Inverse: For any a ∈ F - {0}, there exists a unique multiplicative inverse 1/a such that a × 1/a = 1/a × a = 1.

Definition 3. *A* **FIELD** *is a set F which is closed under two operations $+$ and $\times$ such that*

(1) *F is an abelian group under $+$ and*
(2) *$F - \{0\}$ (the set F without the additive identity 0) is an abelian group under $\times$.*

Examples: $\mathbb{Z}/p\mathbb{Z}$ is a field, since $\mathbb{Z}/p\mathbb{Z}$ is an additive group and $(\mathbb{Z}/p\mathbb{Z}) - \{0\} = (\mathbb{Z}/p\mathbb{Z})^\times$ is a group under multiplication. Sometimes when we (or Cox) want to emphasize that $\mathbb{Z}/p\mathbb{Z}$ is a field, we use the notation $\mathbb{F}_p$. Other examples: $\mathbb{R}$, the set of real numbers, and $\mathbb{C}$, the set of complex numbers are both infinite fields. So is $\mathbb{Q}$, the set of rational numbers, but not $\mathbb{Z}$, the integers. (What fails?)

Definition. Given a field F, a **vector space** V over F is an additive Abelian group endowed with an action of F called **scalar multiplication** or **scaling**.

An **action** of F on V is an operation that takes elements $\lambda \in F$ and $v \in V$ and gives an element, denoted λv, of V.

The scalar multiplication is to satisfy the following axioms:

(V1) for all $v \in V$ and $\lambda \in F$, λv is an element of V;
(V2) $\lambda(\mu v) = (\lambda\mu)v$ for all $v \in V$ and $\lambda, \mu \in F$;
(V3) $1v = v$ for all $v \in V$;
(V4) $(\lambda + \mu)v = \lambda v + \mu v$ for all $v \in V$ and $\lambda, \mu \in F$;
(V5) $\lambda(v + w) = \lambda v + \lambda w$ for all $v, w \in V$ and $\lambda \in F$.

Appendix 2 : Group Theory

A group $(G, \cdot)$ is a non-empty set G with a binary group multiplication operation '$\cdot$', with the following properties :

(i) Closure : $g_1 \cdot g_2 \in G$ for all $g_1, g_2 \in G$

(ii) Associativity : $(g_1 \cdot g_2) \cdot g_3 = g_1 \cdot (g_2 \cdot g_3)$ for all $g_1, g_2, g_3 \in G$

(iii) Identity : there exists $e \in G$ such that $\forall g \in G$, $g \cdot e = e \cdot g = g$

(iv) Inverses : For all $g \in G$, there exists $g^{-1} \in G$ such that $g \cdot g^{-1} = e$ and $g^{-1} \cdot g = e$

Note : We often write $g_1 \cdot g_2$ as $g_1 g_2$, and refer to the group G without referring explicitly to its multiplication operation, but it must be defined.

- A group G is finite if the # of elements in G is finite.

- The order of a finite group G is the # of elements it contains, denoted as $|G|$ (or) $o(G)$.

- A group G is said to be Abelian/Commutative if $g_1 \cdot g_2 = g_2 \cdot g_1$ for all $g_1, g_2 \in G$.

i.e., '$\cdot$' is a commutative binary operation.

Ex: additive group $\mathbb{Z}_n$ of integers modulo n, with 'multiplication' operation, the operation of modular addition.

$$\boxed{\begin{aligned} \mathbb{Z}_n = \mathbb{Z}_n^+ = \mathbb{Z}/n\mathbb{Z} &= (\mathbb{Z}/n\mathbb{Z})^+ \\ &= (\mathbb{Z}/n\mathbb{Z}, +) = (\{0,1,\ldots,n-1\}, +) \end{aligned}}$$

There is an identity element, 0, since

$x + 0 = x \pmod n$ for all x

Every $x \in G$ has an inverse, $n-x$, since

$x + (n-x) = 0 \pmod n$

- The order of an element $g \in G$ is the smallest +ve integer r such that g^r (g multiplied with itself r times) equals the identity element e, ie. denoted as $|g|$ such that $g^{|g|} = e$

- **Ex: A2.1** For any element g of a finite group, there always exist a +ve integer r such that $g^r = e$.

  i.e., every element of such a group has an order.

Proof

Suppose G is a finite group, and let $g \in G$.

Consider all positive integral powers of g

i.e., $g, g^2, g^3, \ldots\ldots$

Every one of these powers must be an element of G, by closure axiom.

Since G has a finite # of elements, all these integral powers of g cannot be distinct elements of G.

Therefore suppose that, $g^s = g^r$, $s > r$

$$g^s = g^r \Longrightarrow g^s g^{-r} = g^r g^{-r}$$

$$\Longrightarrow g^{s-r} = e$$

$$\Longrightarrow g^m = e \quad \text{where } m = s-r$$

Since $s > r$,

$t = s-r$ is a positive integer.

$\therefore$ There exists a positive integer t such that, $g^t = e$

Every set of +ve integers has a least number.

$\therefore$ The set of all those +ve integer t such that $g^t = e$ has a least member, say m.

Thus,
there exists a least positive integer m such that $a^m = e$, showing that the order of every element of a finite group is finite.

- The order of an element of a group is the same as that of its inverse.

$$\boxed{|g| = |g^{-1}|}$$

Proof

Let n and m be the orders of g and g^{-1} respectively, i.e., $g^n = e$ and $(g^{-1})^m = e$

$$g^n = e \longrightarrow (g^n)^{-1} = e^{-1}$$
$$\longrightarrow (g^{-1})^n = e$$
$$\Rightarrow |g^{-1}| \leq n \Rightarrow m \leq n$$

$$(g^{-1})^m = e \Rightarrow (g^m)^{-1} = e \Rightarrow g^m = e^{-1} = e$$
$$\Rightarrow |g| \leq m \Rightarrow n \leq m$$

$$\therefore \underline{m = n}$$

If the order of g is infinite, then the order of a^{-1} cannot be finite.

Proof

If $|g^{-1}| = m \Rightarrow |g| \leq m$

$\Rightarrow |g|$ is finite.

i.e., if the order of g is infinite, then the order of g^{-1} must also be infinite

- The order of any integral power of an element g cannot exceed the order of g. $\boxed{|g^k| \leq |g|}$

Proof: Let g^k be any integral power of g. & let $|g| = n$

$|g| = n \longrightarrow g^n = e$

$\longrightarrow (g^n)^k = e^k$

$\Rightarrow g^{nk} = e \longrightarrow (g^k)^n = e$

$\Rightarrow \underline{\underline{|g^k| \leq n}}$

- If an element g of a group G is order n, then $g^m = e$ iff n is a divisor of m $\boxed{g^m = e \Rightarrow m = t|g|}$

Proof $|g| = m \Rightarrow g^m = e$

$$\begin{array}{r|l} & t \\ \hline n & m \\ & \overline{r} \end{array}$$

By the division algorithm : $m = tn + r$ where $0 \leq r < n$

$e = g^m = g^{tn+r} = g^{tn} \cdot g^r = (g^n)^t g^r = e^t g^r$

$= eg^r = g^r$

$\Rightarrow g^r = e$, but n is the smallest +ve integer such that $g^n = e$ and $r < n$,

$\therefore r = 0$

$\therefore \quad m = tn + 0$

$= tn$

$g^m = e$ iff

$\Rightarrow n \mid m$ (or) $|g|$ divides m

Example : Groups

$\boxed{Ex:}$ $(\mathbb{Z}, +)$ is a group, but $(\mathbb{Z}, \cdot)$ is not

Ans:

$+$ is an associative binary operation on $\mathbb{Z}$.

The identity element w.r.t $+$ is 0.

The inverse of any $n \in \mathbb{Z}$ is $-n$.

$\Longrightarrow (\mathbb{Z}, +)$ is a group.

Multiplication in $\mathbb{Z}$ is associative

$1 \in \mathbb{Z}$. is the multiplicative identity

Not every element in $\mathbb{Z}$ have multiplicative inverse.

$\Longrightarrow (\mathbb{Z}, \cdot)$ is not a group.

$\boxed{\text{Ex:}}$ $(\mathbb{Q}, +)$ and $(\mathbb{R}, +)$ are groups.

$\boxed{\text{Ex:}}$ Let $G = \{\pm 1, \pm i\}$ and the binary operation be multiplication. Then $(G, \cdot)$ is a group.

Ans: The table of the operation is:

$\cdot$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

$a \cdot 1 = a \quad \forall\, a \in G \Rightarrow 1$ is the identity element

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

$\boxed{\text{Ex:}}$ Let G be the set of all 2×2 matrices with non-zero determinant. i.e.,

$$G = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \,\middle|\, a,b,c,d \in \mathbb{R},\ ad-bc \neq 0 \right\}.$$

Consider G with matrix multiplication, i.e., for $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ and $P = \begin{bmatrix} p & q \\ r & s \end{bmatrix}$ in G.

$$AP = \begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} p & q \\ r & s \end{bmatrix} = \begin{bmatrix} ap+br & aq+bs \\ cp+dr & cq+ds \end{bmatrix}$$

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

Ans

$A, P \in G \Longrightarrow A\cdot P \in G$: '$\cdot$' is a binary operation.

$\det(A\cdot P) = \det(A)\cdot\det(P) \neq 0$, since $\det A \neq 0$ & $\det(P) \neq 0$

$\therefore$ $A\cdot P \in G$ for all $A, P \in G$.

The matrix multiplication is associative &

$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ is the multiplicative identity.

For $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in G$, the matrix

$$B = \begin{bmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{bmatrix}$$ is such that $\det(B) = \frac{1}{ad-bc} \neq 0$.

and $AB = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$. Thus, $B = A^{-1}$.

$\Longrightarrow$ The set of all 2×2 matrices over $\mathbb{R}$ with non-zero determinant forms a group under multiplication.

$AB \neq BA$: matrix multiplication is not commutative.

$\therefore$ This group is not commutative or non-abelian.

The set of all 2×2 matrices over $\mathbb{R}$ with non-zero determinant forms a non-abelian/non-commutative group under matrix multiplication, is called the general linear group of order 2 over $\mathbb{R}$, denoted by $GL_2(\mathbb{R})$.

Ex: Consider the set of all translations of $\mathbb{R}^2$.

$$T = \left\{ f_{a,b} : \mathbb{R}^2 \to \mathbb{R}^2 \;\middle|\; f_{a,b}(x,y) = (x+a,\, y+b) \text{ for some fixed } a,b \in \mathbb{R} \right\}$$

Each element $f_{a,b}$ in T is represented by a point (a,b) in $\mathbb{R}^2$.

$(T, \circ)$ is a group, where '$\circ$' denotes the composition of functions.

Ans:

$$f_{a,b} \circ f_{c,d}(x,y) = f_{a,b}(x+c,\, y+d) = (x+c+a,\, y+d+b)$$

$$= f_{a+c,\, b+d}(x,y) \quad \text{for any } (x,y) \in \mathbb{R}^2$$

$$\therefore f_{a,b} \circ f_{c,d} = f_{a+c,\, b+d} \in T$$

$\therefore$ '$\circ$' is a binary operation on T

$$f_{a,b} \circ f_{0,0} = f_{a,b} \quad \forall\, f_{a,b} \in T$$

$\therefore f_{0,0}$ is the identity element

$$f_{a,b} \circ f_{-a,-b} = f_{0,0} \quad \forall\, f_{a,b} \in T$$

$\therefore f_{-a,-b}$ is the inverse of $f_{a,b} \in T$

$f_{a,b} \circ f_{c,d} = f_{c,d} \circ f_{a,b} \quad \forall \; f_{a,b}, f_{c,d} \in T$

$\therefore$ $(T, \circ)$ is an abelian/commutative group.

Binary Operations

- Let S be a non-zero set. Any function $* : S \times S \to S$ is called a binary operation on S.

i.e., a binary operation associates a unique element of S to every ordered pair of elements of S.

For a binary operation $*$ on S and $(a,b) \in S \times S$, we denote $*(a,b)$ by $a*b$.

Ex:-

① $+$ and $\times$ are binary operations on $\mathbb{Z}$.
since, $+(a,b) = a+b$ & $\times(a,b) = a\times b$ $\forall\ a,b \in \mathbb{Z}$

② Let $P(S)$ be the set of all subsets of S.
The operations $\cup$ and $\cap$ are binary operations on $P(S)$ since $A \cup B$ and $A \cap B$ are in $P(S)$ for all subset A and B of S

③ Let X be a non-empty set and $F(X)$ be the family of all functions $f : X \to X$. Then the composition of functions is a binary operation on $F(X)$, since $f \circ g \in F(X)$ $\forall\ f, g \in F(X)$.

- Let $*$ be a binary operation on a set S. If there is an element $e \in S$ such that $\forall a \in S$, $a*e = a$ and $e*a = a$, then e is called an identity element for $*$

- For $a \in S$, we say that $b \in S$ is an inverse of a, if $a*b = e$ and $b*a = e$. In this case we usually write $b = a^{-1}$.

• **Theorem**: Let $*$ be a binary operation on a set S. Then

(a) If $*$ has an identity element, it must be unique

(b) If $*$ is associative and $s \in S$ has an inverse w.r.t $*$, it must be unique.

Proof

(a) Suppose e and e' are both identity elements for $*$

Then,

$$e = e * e' \quad \left[\text{since } e' \text{ is an identity element}\right.$$

$$= e' \quad \left[\text{since } e \text{ is an identity element}\right.$$

$\Longrightarrow e = e'$, Hence the identity element is unique.

(6)

Suppose there exists $a, b \in S$ such that $s * a = e = a * s$ and $s * b = e = b * s$ & e being the identity element for $*$.

Then,

$$a = a * e = a * (s * b)$$

($*$ is associative

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

$$= e * b = b$$

ie., $a = b$, Hence the inverse of s is unique.

Properties — Groups

- Let G be a group. Then

$$\boxed{\begin{aligned} (a^{-1})^{-1} &= a \quad \forall\ a \in G \\ (ab)^{-1} &= b^{-1}a^{-1} \quad \forall\ a,b \in G \end{aligned}}$$

Proof

By definition of inverse

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

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

Theorem: If $*$ is associative and $g \in G$ has an inverse, w.r.t $*$, it must be unique.

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

For $a, b \in G$, $ab \in G$

$\therefore (ab)^{-1} \in G$ and is a unique element satisfying $(ab)(ab)^{-1} = e$ and $(ab)^{-1}(ab) = e$.

$$(ab)(b^{-1}a^{-1}) = ((ab)b^{-1})a^{-1}$$
$$= (a(bb^{-1})a^{-1}) = aea^{-1}$$
$$= aa^{-1} = e$$

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

By uniqueness of the inverse, $(ab)^{-1} = b^{-1}a^{-1}$

- For a group G,
  $(ab)^{-1} = a^{-1}b^{-1}$ $\forall\, a, b \in G$ only if G is abelian/commutative.

- For $a, b, c \in G$,

$$\boxed{\begin{aligned} ab = ac &\Rightarrow b = c \quad \text{(left cancellation law)} \\ ba = ca &\Rightarrow b = c \quad \text{(right cancellation law)} \end{aligned}}$$

- If in a group G, there exists an element g such that $gx = g$ for all $x \in G$, then $G = \{e\}$.

Theorem → For elements $a, b \in G$, the equations $ax = b$ and $ya = b$ have unique solutions in G.

For $a, b \in G$,

$$ax = b \Rightarrow x = a^{-1}b$$
$$ya = b \Rightarrow y = ba^{-1}$$

Proof

For $a, b \in G$, $a^{-1}b \in G$

$$a(a^{-1}b) = (aa^{-1})b = eb = b$$

$\therefore$ $a^{-1}b$ satisfies the equation $ax = b$

i.e., $ax = b$ has a solution in G.

Suppose x_1, x_2 are 2 solutions of $ax = b$ in G.

Then, $ax_1 = b = ax_2$

Left cancellation law : $x_1 = x_2$

$\therefore$ $a^{-1}b$ is the unique solution of $ax = b$ in G.

Similarly,

ba^{-1} is the unique solution of $ya = b$ in G.

Ex:- Consider $A = \begin{bmatrix} 2 & 3 \\ 1 & 2 \end{bmatrix}$ and $B = \begin{bmatrix} 1 & 5 \\ 0 & 4 \end{bmatrix}$ in $GL_2(\mathbb{R})$. Find the solution of $AX = B$

Ans: For $A, B \in GL_2(\mathbb{R})$

from theorem, $X = A^{-1}B$.

$$A^{-1} = \begin{bmatrix} 2 & -3 \\ -1 & 2 \end{bmatrix}$$

$$\therefore \quad A^{-1}B = \begin{bmatrix} 2 & -2 \\ -1 & 3 \end{bmatrix} = X$$

Ex:-5 Let S be a non-empty set. Consider $P(S)$ with the binary operation of symmetric difference Δ, given by

$A \Delta B = (A \setminus B) \cup (B \setminus A) \quad \forall \; A, B \in P(S)$

Show that $(P(S), \Delta)$ is an abelian group. What's the unique solution for the equation $Y \Delta A = B$?

Ans: $A \setminus B = A - B = A \cap B^c$, $(A \cap B)^c = A^c \cup B^c$, $(A \cup B)^c = A^c \cap B^c$ and $\cup$ & $\cap$ are commutative & associative.

$\Longrightarrow \Delta$ is an associative binary operation.

$A \Delta B = B \Delta A \quad \forall\ A, B \in P(S)$

$\Longrightarrow \Delta$ is commutative

$A \Delta \phi = (A \setminus \phi) \cup (\phi \setminus A) = A \quad \forall\ A \in P(S)$

$\longrightarrow \phi$ is the identity element

$A \Delta A = (A \setminus A) \cup (A \setminus A) = \phi \quad \forall\ A \in P(S)$

$\Rightarrow$ any element is its own inverse.

$\therefore \ (P(S), \Delta)$ is an abelian group

For $A, B \in (P(S), \Delta)$ we want to solve

$Y \Delta A = B$

A is its own inverse.

Theorem: $Y \Delta A = B \Longrightarrow Y = B \Delta A^{-1}$
$= B \Delta A$ is the unique solution.

Ex:

so

Ans:

The

Ex: For the group $(\mathbb{Z}, -)$, obtain the solution for $a - x = b \;\; \forall\, a, b \in \mathbb{Z}$?

Ans:

$$a - a = 0 \qquad \forall\, a \in \mathbb{Z}$$

$\Rightarrow$ any element is its own inverse.

Theorem: $a - x = b \Longrightarrow x = -(a-b)$ is the unique solution

- Let G be a group. For $a \in G$,

$$\boxed{\begin{array}{lll} \text{(i)} & a^0 = e & \\ \text{(ii)} & a^n = a^{n-1} \cdot a & \text{if } n > 0 \\ \text{(iii)} & a^{-n} = (a^{-1})^n & \text{if } n > 0 \end{array}}$$

Note: n is called the exponent (or index) of the integral power a^n of a.

$\therefore$ By definition $a^1 = a$, $a^2 = a \cdot a$, $a^3 = a \cdot a \cdot a$, and so on.

Note: When the notation used for the binary operation is addition, a^n becomes na.

Ex:- for any $a \in \mathbb{Z}$

$na = 0$ if $n = 0$.

$na = a + a + \cdots + a$ if $n > 0$
(n times)

$na = (-a) + (-a) + \cdots + (-a)$ if $n < 0$.
($-n$ times)

- Let G be a group.

For $a \in G$ and $m, n \in \mathbb{Z}$,

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

(ii) $a^m \cdot a^n = a^{m+n}$

(iii) $(a^m)^n = a^{mn}$

Proof.

(i) If $n=0$, $(a^n)^{-1} = a^{-n} = (a^{-1})^n$

If $n>0$,

$e = e^n = (aa^{-1})^n$

$= (aa^{-1})(aa^{-1}) \cdots (aa^{-1})$ (n times.

$= a^n (a^{-1})^n$ [a & a^{-1} commute

$\therefore \underline{\underline{(a^n)^{-1} = (a^{-1})^n}}$

By definition, $(a^{-1})^n = a^{-n}$

$(a^n)^{-1} = (a^{-1})^n = a^{-n}$ when $n > 0$

If $n < 0$, then

$(-n) > 0$ and

$$(a^n)^{-1} = \left(a^{-(-n)}\right)^{-1} \qquad \left[\, n>0,\ a^{-n} = (a^n)^{-1} \right.$$

$$= \left[(a^{-n})^{-1}\right]^{-1}$$

$$= a^{-n} \qquad \left[\, (a^m)^n = a^{mn} \right.$$

$$(a^{-1})^n = (a^{-1})^{-(-n)} \qquad \left[\, n>0,\ a^{-n} = (a^n)^{-1} \right.$$

$$= \left[(a^{-1})^{-1}\right]^{-n}$$

$$= a^{-n}$$

$$\Longrightarrow (a^n)^{-1} = (a^{-1})^n = a^{-n} \text{ when } n < 0.$$

(ii) If $m=0$ or $n=0$, then $a^{m+n} = a^m \cdot a^n$

Suppose $m \neq 0$ and $n \neq 0$.

case 1: $m>0$ & $n>0$

If $n=1$, then $a^m \cdot a = a^{m+1}$ By definition.

Assume, $a^m \cdot a^{n-1} = a^{m+n-1}$

Then, $a^m \cdot a^n = a^m \cdot (a^{n-1} \cdot a) = a^{m+n-1} \cdot a = a^{m+n}$.

By principle of induction: $a^{m+n} = a^m \cdot a^n$ for $m>0, n>0$

case 2: $m<0$ & $n<0$

then $(-m)>0$ and $(-n)>0$

case 1 $\rightarrow$ $a^{-n} \cdot a^{-m} = a^{-(n+m)} = a^{-n-m}$

Taking inverses, $(a^{-(n+m)})^{-1} = a^{m+n} = (a^{-n} \cdot a^{-m})^{-1} = (a^{-m})^{-1} (a^{-n})^{-1}$

$= a^m a^n$.

Case 3: $m>0$ and $n<0$ $\forall$ $m+n \geq 0$

By case 1, $a^{m+n} \cdot a^{-n} = a^m$

Xing by $a^n = (a^{-n})^{-1}$ on the right,

$$a^{m+n} = a^m a^n$$

Case 4: $m>0$, $n<0$ $\forall$ $m+n<0$.

By case 2, $a^{-m} a^{m+n} = a^n$

Xing both sides by $a^m = (a^{-m})^{-1}$ on the left

$$a^{m+n} = a^m \cdot a^n$$

Similarly, cases 5 & 6 for which $m<0, n>0$.

$\Rightarrow$ $\forall$ $a \in G$ and $m, n \in \mathbb{Z}$,

$$\underline{\underline{a^{m+n} = a^m \cdot a^n}}$$

(iii) Proof by induction $n>0$ & $n<0$.

<u>Case 1:</u> $n>0$

$P(1): (a^m)^1 = a^m = a^{m \cdot 1}$

Assume $(a^m)^{(n-1)} = a^{m(n-1)}$

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

$$= a^{mn-m} \cdot a^m = a^{mn-m+m} = a^{mn}.$$

$\Longrightarrow (a^m)^n = a^{mn}$ when $n>0$

<u>Case 2:</u> $n<0$

$-n>0 \Rightarrow (a^m)^{-n} = a^{m(-n)} = a^{-mn}$

> 0.

3 GROUPS

A Integers Modulo n

Consider the set of integers $\mathbb{Z}$, and $n \in \mathbb{Z}$.

Define the relation of congruence on $\mathbb{Z}$

by : a is congruent to b modulo n

if n divides $a-b$.

$$a \equiv b \pmod{n}$$

Ex :- $4 \equiv 1 \pmod{3}$ since $3 \mid (4-1)$

Note: $\equiv$ is an equivalence relation, and hence partitions $\mathbb{Z}$ into disjoint equivalence classes called congruence classes modulo n.

We denote the class containing r by $\bar{r}$

i.e.,

$$\bar{r} = \{ m \in \mathbb{Z} \mid m \equiv r \pmod{n} \}$$

$\therefore$ An integer m belongs to $\bar{r}$ for some r, $0 \leq r < n$ iff $n \mid r-m$, i.e., $r-m = kn$ for some $k \in \mathbb{Z}$

$$\therefore \quad \bar{r} = \{ r+kn \mid k \in \mathbb{Z} \}$$

Now, if $m \geq n$, then the division algorithm says that $m = nq + r$ for some $q, r \in \mathbb{Z}$, $0 \leq r < n$

i.e., $m \equiv r \pmod{n}$ for some $r = 0, 1, \ldots, n-1$.

Therefore,

The set of all the congruence classes modulo n is:

$$\mathbb{Z}_n = \{ \bar{0}, \bar{1}, \bar{2}, \ldots, \overline{n-1} \} = \{ [0], [1], [2], \ldots, [n-1] \}$$

- $\mathbb{Z}_n$ is read "Z mod n"
- The individual elements of $\mathbb{Z}_n$ are not integers, but rather infinite set of integers, e.g.,

$$[2] = \{ \ldots, 2-3n, 2-2n, 2-n, 2, 2+n, 2+2n, 2+3n, \ldots \}$$

- Let $a, b, n \in \mathbb{Z}$ with $n > 0$. Then 'a' is congruent to b modulo n;

i.e., $a \equiv b \pmod{n}$ provided that

n divides $a - b$.

- Let a and n be integers with $n > 0$. The congruence class of a modulo n, denoted $[a]_n$, is the set of all integers that are congruent to a modulo n; i.e.,

$$[a]_n = \{z \in \mathbb{Z} \mid a - z = kn \text{ for some } k \in \mathbb{Z}\}$$

Define the operation $+$ on $\mathbb{Z}_n$ by

$\bar{a} + \bar{b} = \overline{a+b}$;

where, $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1}\} = \{[0], [1], [2], \dots, [n-1]\}$

If $\bar{a} = \bar{b}$ and $\bar{c} = \bar{d}$ in $\mathbb{Z}_n$.

$a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$

Hence, there exists integers k_1 and k_2 such that $a - b = k_1 n$ and $c - d = k_2 n$

$(a+c) - (b+d) = (k_1 + k_2) n$

$\therefore \overline{a+c} = \overline{b+d}$

Thus, $+$ is a binary operation on $\mathbb{Z}_n$

Ex:-

$\bar{2} + \bar{2} = \bar{0}$ in $\mathbb{Z}_4$ since $2 + 2 = 4$ and $4 \equiv 0 \pmod{4}$

Operation table for $+$ on $\mathbb{Z}_4$

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	0	1	2	3
$\bar{1}$	1	2	3	1
$\bar{2}$	2	3	1	2
$\bar{3}$	3	1	2	3

- The additive group of integers modulo n is denoted as, $(\mathbb{Z}_n, +)$ (or) $\mathbb{Z}/n\mathbb{Z}$ or just $\mathbb{Z}_n$.

- $(Z_n, +)$ is a commutative group.
(or) abelian group

<u>Proof</u>

(i) $\bar{a}+\bar{b} = \overline{a+b} = \overline{b+a} = \bar{b}+\bar{a} \quad \forall\ \bar{a}, \bar{b} \in Z_n$

$\Longrightarrow$ addition is commutative in Z_n.

(ii) $\bar{a}+(\bar{b}+\bar{c}) = \bar{a}+(\overline{b+c}) = \overline{a+(b+c)}$

$= \overline{(a+b)+c} = (\overline{a+b})+\bar{c}$

$= (\bar{a}+\bar{b})+\bar{c} \quad \forall\ \bar{a}, \bar{b}, \bar{c} \in Z_n$

$\longrightarrow$ addition is associative in Z_n.

(iii) $\bar{a}+\bar{0} = \bar{a} = \bar{0}+\bar{a} \quad \forall\ \bar{a} \in Z_n$

$\Longrightarrow \bar{0}$ is the identity for addition

(iv) For $a \in Z_n$ $\underset{\text{there exists}}{\exists}$ $\overline{n-a} \in Z_n$ such that

$\bar{a}+\overline{n-a} = \overline{a+n-a} = \bar{n} = 0$

$\Longrightarrow$ Every element $\bar{a}$ in Z_n has an inverse with respect to addition.

- $(\mathbb{Z}_n, \cdot)$ is not a group

Proof

We can define multiplication on $\mathbb{Z}_n$ by $\bar{a} \cdot \bar{b} = \overline{ab}$

Then, $\bar{a} \cdot \bar{b} = \bar{b} \cdot \bar{a}$ $\quad \forall\ \bar{a}, \bar{b} \in \mathbb{Z}_n$.

Also, $(\bar{a}\ \bar{b})\bar{c} = \bar{a}\ (\bar{b}\ \bar{c})$ $\quad \forall\ \bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_n$

$\therefore$ multiplication in $\mathbb{Z}_n$ is a commutative and associative binary operation.

$\mathbb{Z}_n$ has a multiplicative identity, $\bar{1}$.

But,

not every element of $\mathbb{Z}_n$, for example $\bar{0}$, does not have a multiplicative inverse.

$\Longrightarrow$ $(\mathbb{Z}_n, \cdot)$ is not a group.

Suppose we consider the non-zero elements of $\mathbb{Z}_n$, i.e., $\mathbb{Z}_n^*$

Is $(\mathbb{Z}_n^*, \cdot)$ a group ?

Ex:- $\mathbb{Z}_4^* = \{\bar{1}, \bar{2}, \bar{3}\}$ is not a group because '$\cdot$' is not even a binary operation on $\mathbb{Z}_4^*$, since $\bar{2} \cdot \bar{2} = \bar{0} \notin \mathbb{Z}_4^*$.

- $(\mathbb{Z}_p^*, \cdot)$ is an abelian group for any prime p.

- The multiplicative group of integers modulo n, may be written as $(\mathbb{Z}, \cdot)$

(or) $(\mathbb{Z}/n\mathbb{Z})^\times$, $(\mathbb{Z}/n\mathbb{Z})^*$, $\mathbb{Z}_n^*$ $\Longleftarrow$

$\boxed{B}$ The Symmetric Group

Let X be a non-empty set.

The composition of functions defines a binary operation on the set $F(X)$ of all functions from X to X.

This binary operation is associative

I_X, the identity map, is the identity in $F(X)$.

Consider the subset $S(X)$ of $F(X)$ given by,

$$S(X) = \{ f \in F(X) \mid f \text{ is bijective} \}$$

$\therefore$ $f \in S(X)$ iff $f^{-1} : X \to X$ exists.

$f \circ f^{-1} = f^{-1} \circ f = I_X$.

$f^{-1} \in S(X)$

For all $f, g \in S(X)$,

$$(g \circ f) \circ (f^{-1} \circ g^{-1}) = I_X = (f^{-1} \circ g^{-1}) \circ (g \circ f)$$

$g \circ f \in S(X)$

$\therefore$ '$\circ$' is a binary operation on $S(X)$

$\circ$ is associative since $(f \circ g) \circ h = f \circ (g \circ h)$ $\forall$ $f, g, h \in S(X)$

I_X is the identity element because

$$f \circ I_X = I_X \circ f \quad \forall f \in S(X)$$

f^{-1} is the inverse of f for any $f \in S(X)$

$\therefore$

$(S(X), \circ)$ is a group & it is called the symmetric group on X.

If the set X is finite, say $X = \{1, 2, \cdots, n\}$ then we denote $S(X)$ by S_n and each $f \in S_n$ is called a permutation on n symbols.

S_n contains $n!$ elements.

Let's represent $f \in S_n$ by

$$\begin{bmatrix} 1 & 2 & \cdots & n \\ f(1) & f(2) & \cdots & f(n) \end{bmatrix}$$

Ex:-

$\begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{bmatrix}$ represents the function

$f : (1,2,3,4) \longrightarrow (1,2,3,4)$

such that $f(1) = 2$, $f(2) = 4$, $f(3) = 3$, $f(4) = 1$

Ex:- Consider S_3, the set of all permutations on 3 symbols. This has, $3! = 6$ symbols.

One such function is,

$$f = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}, \text{ where } f(1) = 2,\ f(2) = 3,\ f(3) = 1$$

$$= (1\ \ 2\ \ 3)$$

Such a permutation is called a cyclic.

- $f \in S_n$ is a cyclic of length r if there are $x_1, \dots, x_r$ in $X = \{1, 2, \dots, n\}$ such that $f(x_i) = x_{i+1}$ for $1 \le i \le r-1$, $f(x_r) = x_1$ and $f(t) = t$ for $t \notin x_1, \dots, x_n$.

In this case f is written as $(x_1, \dots x_r)$

Ex:- $f = (2\ 4\ 5\ 10) \in S_{10}$

$f(2)=4,\ f(4)=5,\ f(5)=10,\ f(10)=2$

and $f(j)=j$ for $i \notin (1,3,6,7,8,9)$

i.e.,
$$f = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 1 & 4 & 3 & 5 & 10 & 6 & 7 & 8 & 9 & 2 \end{bmatrix}$$

Similarly,

the permutation $\begin{pmatrix} 2 & 5 \\ 5 & 3 \end{pmatrix}$ is

the cycle $(1\ 2\ 5\ 3\ 4)$ in S_5

$$\alpha \circ \beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 \end{bmatrix} \circ \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 4 & 1 & 2 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ \alpha\beta(1) & \alpha\beta(2) & \alpha\beta(3) & \alpha\beta(4) & \alpha\beta(5) \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ \alpha(5) & \alpha(3) & \alpha(4) & \alpha(1) & \alpha(2) \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 2 & 5 \end{bmatrix} = (2, 4)$$

C Complex Numbers.

Consider the set $\mathbb{C}$ of all ordered pairs (x,y) of real numbers, i.e., $\mathbb{C} = R \times R$

i.e., $\mathbb{C} = \{(x,y) \mid x,y \in \mathbb{R}\}$

Define addition (+) and multiplication ($\cdot$) in $\mathbb{C}$ as:

$$(x_1,y_1) + (x_2,y_2) = (x_1+x_2,\ y_1+y_2)$$

$$(x_1,y_1) \cdot (x_2,y_2) = (x_1x_2 - y_1y_2,\ x_1y_2 + x_2y_1)$$

for (x_1,y_1) and (x_2,y_2) in $\mathbb{C}$.

$+$ and $\cdot$ are commutative and associative

$(0,0)$ is the additive identity

for (x,y) in $\mathbb{C}$, $(-x,-y)$ is its additive inverse

$(1,0)$ is the multiplicative identity

If $(x,y) \neq (0,0)$ in $\mathbb{C}$, then

either $x^2>0$ or $y^2>0$.

$\therefore x^2+y^2>0$.

Then,

$$(x,y)\cdot\left(\frac{x}{x^2+y^2}, \frac{-y}{x^2+y^2}\right) = \left(x\cdot\frac{x}{x^2+y^2} - y\,\frac{(-y)}{x^2+y^2},\ x\,\frac{(-y)}{x^2+y^2} + y\,\frac{x}{x^2+y^2}\right)$$

$$= (1,0)$$

$\therefore \left(\frac{x}{x^2+y^2}, \frac{-y}{x^2+y^2}\right)$ is the multiplicative inverse of (x,y) in $\mathbb{C}$.

$\longrightarrow$ $(\mathbb{C},+)$ & $(\mathbb{C}^*,\cdot)$ are groups.

where,

$\mathbb{C}^*$: the set of non-zero complex numbers.

Subgroups

Ex:-
the groups $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$ are contained in the bigger group $(\mathbb{C},+)$ of complex numbers, not just as subsets but as groups.

- Let $(G,*)$ be a group. A non-empty subset H of G is called a subgroup of G if, i.e., $\boxed{H \leq G}$

  (i) $a*b \in H \;\forall\; a,b \in H$

  i.e., $*$ is a binary operation on H

  (ii) $(H,*)$ is itself a group.

Given $H \subseteq G$,

$\cancel{H \leq G} \Longleftrightarrow a,b \in H \Rightarrow ab^{-1} \in H$

Ex:- $(\mathbb{Z},+)$ is a subgroup of $(\mathbb{Q},+)$, $(\mathbb{R},+)$, and $(\mathbb{C},+)$.

- $(H,*)$ is a subgroup of $(G,*)$ if and only if

(i) $e \in H$

(ii) $a,b \in H \Longrightarrow a*b \in H$

(iii) $a \in H \Longrightarrow a^{-1} \in H$

Proof

(i) If h is the identity of $(H,*)$ then for any $a \in H$, $h*a = a*h = a$

~~However~~, $a \in H \subseteq G$

$\therefore a*e = e*a = a$, where e is the identity in G.

$\therefore h*a = e*a$

By right cancellation $\Longrightarrow \underline{h = e}$

(iii)

• If $(H,*)$ is a subgroup of $(G,*)$, we shall just say that H is a subgroup of G, provided that there is no confusion about the binary operations

i.e., $H \leq G$.

Theorem: If H be a non-empty subset of a group G. Then H is a subgroup of G iff $a,b \in H \implies ab^{-1} \in H$

Given $H \subseteq G$, $H \leq G \iff$ $a,b \in H \Downarrow ab^{-1} \in H$

Proof. $H \leq G$

$a,b \in H \implies a, b^{-1} \in H \implies ab^{-1} \in H$

Conversely, Given $a,b \in H \implies ab^{-1} \in H$

Since $H \neq \phi$, $\exists\ a \in H$. Then $aa^{-1} = e \in H$

For any $a \in H$, $ea^{-1} \in H \implies a^{-1} \in H$

If $a,b \in H$, then $a, a^{-1}, b, b^{-1} \in H$. Thus

$a(b^{-1})^{-1} \in H \implies ab \in H$

$\implies H$ is a subgroup.

- A subgroup of an abelian group is abelian.

Ex:1 Consider the group $(\mathbb{C}^*, \cdot)$. Show that $S = \{z \in \mathbb{C} \mid |z| = 1\}$ is a subgroup of $\mathbb{C}^*$.

Ans: $S \neq \phi$ since $1 \in S$.

For any $z_1, z_2 \in S$,

$$|z_1 z_2^{-1}| = |z_1||z_2^{-1}| = |z_1| \frac{1}{|z_2|} = 1$$

$\Longrightarrow z_1 z_2^{-1} \in S$.

$$S \leq \mathbb{C}^*$$

Ex:2 Consider $G = M_{2\times 3}(\mathbb{C})$, the set of all 2×3 matrices over $\mathbb{C}$. Check that $(G, +)$ is an abelian group. Show that $S = \left\{ \begin{bmatrix} 0 & a & b \\ 0 & 0 & c \end{bmatrix} \middle| a, b, c \in \mathbb{C} \right\}$ is a subgroup of G.

Ans: Define addition on G by,

$$\begin{bmatrix} a & b & c \\ d & e & f \end{bmatrix} + \begin{bmatrix} p & q & r \\ s & t & u \end{bmatrix} = \begin{bmatrix} a+p & b+q & c+r \\ d+s & e+t & f+u \end{bmatrix}$$

$\Longrightarrow$ '+' is a binary operation on G.

$0 = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$ is the additive identity.

$\begin{bmatrix} -a & -b & -c \\ -d & -e & -f \end{bmatrix}$ is the inverse of $\begin{bmatrix} a & b & c \\ d & e & f \end{bmatrix} \in G$

$a+b = b+a \ \forall \ a, b \in \mathbb{C}$,

$\Longrightarrow (\mathbb{C}, +)$ is abelian

$\therefore (G, +)$ is an abelian group.

Since $0 \in S$, $S \neq \phi$

For $\begin{bmatrix} 0 & a & b \\ 0 & 0 & c \end{bmatrix}, \begin{bmatrix} 0 & d & e \\ 0 & 0 & f \end{bmatrix} \in S$, we have

$$\begin{bmatrix} 0 & a & b \\ 0 & 0 & c \end{bmatrix} + \begin{bmatrix} 0 & -d & -e \\ 0 & 0 & -f \end{bmatrix} = \begin{bmatrix} 0 & a-d & b-e \\ 0 & 0 & c-f \end{bmatrix} \in S$$

$\therefore S \leq G$

Ex: 3 Consider the set of all invertible 3×3 matrices over $\mathbb{R}$, $GL_3(\mathbb{R})$, i.e., $A \in GL_3(\mathbb{R})$ iff $\det(A) \neq 0$. Show that

$SL_3(\mathbb{R}) = \{A \in GL_3(\mathbb{R}) \mid \det(A) = 1\}$ is a subgroup of $(GL_3(\mathbb{R}), \cdot)$

Ans:

$$I_3 \in SL_3(\mathbb{R}) \Rightarrow SL_3(\mathbb{R}) \neq \phi$$

For $A, B \in SL_3(\mathbb{R})$,

$$\det(AB^{-1}) = \det(A)\det(B^{-1}) = \frac{\det A}{\det B} = 1$$

$$\boxed{\begin{aligned}&\det(BB^{-1}) = \det(B)\det(B^{-1}) = \det I = 1\\ &\Rightarrow \det(B^{-1}) = \frac{1}{\det(B)}\end{aligned}}$$

$\therefore AB^{-1} \in SL_3(\mathbb{R})$.

$\therefore SL_3(\mathbb{R}) \leq GL_3(\mathbb{R})$

Ex: 4 Any non-trivial subgroup of $(\mathbb{Z}, +)$ is of the form $m\mathbb{Z}$ where $m \in \mathbb{N}$ and $m\mathbb{Z} = \{mt \mid t \in \mathbb{Z}\} = \{0, \pm m, \pm 2m, \pm 3m, \dots\}$

Ans:

Part 1

$0 \in m\mathbb{Z} \Rightarrow m\mathbb{Z} \neq \phi$

For $mr, ms \in m\mathbb{Z}$,

$mr + (-ms) = m(r-s) \in m\mathbb{Z}$

$\therefore$ $m\mathbb{Z}$ is a subgroup of $\mathbb{Z}$

Part 2

Let $H \neq \{0\}$ be a subgroup of $\mathbb{Z}$

and $S = \{i \mid i > 0, i \in H\}$.

Q.C.G.T ②

Since $H \neq \{0\}$, there is a non-zero integer k in H. If $k>0$ then $k \in S$. If $k<0$ then $-k \in S$ since $-k \in H$ and $-k > 0$.

(H is a group & each element is invertible)

Hence, $S \neq \phi$

$\Longrightarrow S \subseteq N$

Well-ordering principle

- every non-empty set of +ve integers contain a least element.

$\Rightarrow$ S has a least element, say s

ie, s is the least +ve integer that belongs to H

(a) Consider any element $st \in s\mathbb{Z}$

If $t=0$, then $st = 0 \in H$

If $t>0$, then $st = \underbrace{s+s+\cdots+s}_{(t \text{ times})} \in H$ (s & t ∈ H then s+t ∈ H)

If $t<0$, then $st = \underbrace{-s-s-\cdots-s}_{(|t| \text{ times})} \in H$ (s & t ∈ H ⟹ −s, −t ∈ H then −s−t ∈ H)

$\therefore st \in H \ \forall \ t \in \mathbb{Z}$

i.e., $s\mathbb{Z} \subseteq H$

(b) Let $m \in H$,

Division algorithm : $m = ns + r$ for some $n, r \in \mathbb{Z}$,

$0 \le r < s$

$\therefore \; r = m - ns$

H is a subgroup of $\mathbb{Z}$ and $m, ns \in H$

$\Longrightarrow r \in H$ & $0 \le r < s$.

s is the least +ve integer that belongs to H.

$\Longrightarrow r = 0$

i.e., $m = ns$

$\therefore \; H \subseteq s\mathbb{Z}$

$\Longrightarrow H = s\mathbb{Z}$

Ex: 5. Show that $U_n \leq (\mathbb{C}^*, \cdot)$ is

where $U_n = \{1, \omega, \omega^2, \dots, \omega^{n-1}\}$ and

$\omega = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n} = e^{i2\pi/n}$

Ans: $U_n \neq \emptyset$

Let $\omega^j, \omega^k \in U_n$ then by the division algorithm, $j+k = qn + r$ for $q, r \in \mathbb{Z}$, $0 \leq r \leq n-1$

$\omega^j \cdot \omega^k = \omega^{j+k} = \omega^{qn+r} = (\omega^n)^q \omega^r = \omega^r \in U_n$

since $\omega^n = 1$

$\Longrightarrow U_n$ is closed under multiplication.

If $\omega^j \in U_n$ then $0 \leq n-j < n-1$ and $\omega^j \omega^{n-j} = \omega^n = 1$, i.e., ω^{n-j} is the inverse of ω^j for all $1 \leq j < n$.

Hence, U_n is a subgroup of $\mathbb{C}^*$

Properties of Subgroups

- For any group G, $\{e\}$ and G are subgroups of G, where $\{e\}$ is called the trivial subgroup.

Theorem: Let G be a group, H be a subgroup of G, and K be a subgroup of H. Then K is a subgroup of G.

$$\boxed{\left.\begin{array}{l} H \leq G \\ K \leq H \end{array}\right\} \quad K \leq G}$$

Ex:6 Subgroup of $\mathbb{Z}$ is of the form $m\mathbb{Z}$ for some $m \in \mathbb{N}$. Let $m\mathbb{Z}$ and $k\mathbb{Z}$ be two subgroups of $\mathbb{Z}$. Show that $m\mathbb{Z}$ is a subgroup of $k\mathbb{Z}$ iff $k|m$.

Ans:

If $m\mathbb{Z} \subseteq k\mathbb{Z}$, then

$$m \in m\mathbb{Z} \subseteq k\mathbb{Z} \Rightarrow m \in k\mathbb{Z}$$

$$\Rightarrow m = kr \text{ for some } r \in \mathbb{Z}$$

$$\Rightarrow k|m$$

Conversely, if $k|m$,

Then $m = kr$ for some $r \in \mathbb{Z}$

Consider $n \in m\mathbb{Z}$ then $n = mt$ for some $t \in \mathbb{Z}$

$$n = mt = (kr)t = k(rt) \in k\mathbb{Z}$$

$$\therefore m\mathbb{Z} \subseteq k\mathbb{Z}$$

$m\mathbb{Z} \leq k\mathbb{Z}$ iff $k|m$

* Theorem : If H and K are a subgroups of a group G, then $H \cap K$ is also a subgroup of G.

$$\boxed{\left.\begin{matrix} H \leq G \\ K \leq G \end{matrix}\right\} H \cap K \leq G}$$

Proof

Since $e \in H$ & $e \in K$, then $e \in H \cap K$

$\Longrightarrow H \cap K \neq \phi$

Let $a, b \in H \cap K$,

$a, b \in H$ and $a, b \in K$

$ab^{-1} \in H$ and $ab^{-1} \in K$

$\therefore ab^{-1} \in H \cap K$

$\therefore H \cap K$ is a subgroup of G.

* **Theorem:** Let A and B be a subgroups of a group G. Then $A \cup B$ is a subgroup of G iff $A \subseteq B$ or $B \subseteq A$.

$$\boxed{\left.\begin{array}{l} A \leq G \\ B \leq G \end{array}\right\} A \cup B \leq G \ \text{ iff } \ A \subseteq B \ \text{ or } \ B \subseteq A}$$

Proof

Suppose $A \nsubseteq B$ and $B \nsubseteq A$,

There exists $a \in A$ that's not in B and $b \in B$ thats not in A

i.e., $a \in A - B$ & $b = B - A$

$(a \in A \setminus B)$ & $(b = B \setminus A)$

$a \in A \cup B$ & $b \in A \cup B$.

Let $A \cup B$ is a group-, & therefore $ab \in A \cup B$.

$a^{-1}, b^{-1} \in A \cup B$.

$ab \in A$ (or) $ab \in B$.

$a^{-1}ab \in A$ (or) $abb^{-1} \in B$

$b \in A$ (or) $a \in B$.

which is a contradiction

i.e., $ab \notin A \cup B$.

$\therefore$ $\underline{\underline{A \cup B \not\leq G}}$

Definition: Let G be a group and A, B be non-empty subsets of G. The product of A and B is the set,

$$AB = \{ab \mid a \in A, b \in B\}$$

Ex:- $(2\mathbb{Z})(3\mathbb{Z}) = \{(2m)(3n) \mid m,n \in \mathbb{Z}\}$

$= \{6mn \mid m,n \in \mathbb{Z}\}$

$= \{6\mathbb{Z}$ $\Longrightarrow$ product of 2 subgroups is a subgroup.

Is this always the case?

Ex:- Consider the group

$S_3 = \{I, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$.

and its subgroups $H = \{I, (1,2)\}$ and $K = \{I, (1,3)\}$.

Ans: $(1\ 2)$ is the permutation $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ and

$(1\ 2\ 3)$ is the permutation $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ & $(1\,3) = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$

& $(1\,2)\circ(1\,3) = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1\,3\,2)$

$(1,3) = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$

$HK = \{I \circ I, I \circ (1,3), (1,2) \circ I, (1,2) \circ (1,3)\} = \{I, (1,3), (1,2), (1\ 3\ 2)\}$

$(1\ 3) \circ (1\ 2) = (1\ 2\ 3) \notin HK$

$\Longrightarrow$ HK is not a subgroup of $G = S_3$.

* Theorem : Let H and K be subgroups of a group G. Then HK is a subgroup of G iff HK = KH.

$$\boxed{\left.\begin{array}{l} H \le G \\ K \le G \end{array}\right\} \; HK \le G \text{ iff } HK = KH \text{ (or) } [H, K] = 0}$$

i.e., If H and K are subgroups of an abelian group G, then HK is a subgroup of G.

Proof

(i) Assume that $HK \le G$.

Let $hk \in HK$. Then

$(hk)^{-1} = k^{-1} h^{-1} \in HK$

$\therefore \; k^{-1} h^{-1} = h_1 k_1$ for some $h_1 \in H$, $k_1 \in K$.

Then, $hk = (k^{-1}h^{-1})^{-1} = (h_1k_1)^{-1} = k_1^{-1}h_1^{-1} \in KH$

$\Longrightarrow HK \subseteq KH$

Let $kh \in KH$, then $(kh)^{-1} = h^{-1}k^{-1} \in HK$.

Since $HK \in G$, we have $((kh)^{-1})^{-1} = kh \in HK$.

$\Rightarrow KH \subseteq HK$.

$\therefore \underline{\underline{HK = KH}}$.

Conversely,

Assume that $HK = KH$

$\left.\begin{array}{l} H \leq G \\ K \leq G \end{array}\right\}$ $e \in H, K$ $\Rightarrow e^2 = e \in HK, KH$

$\Rightarrow HK \neq \emptyset$

Let $a, b \in HK$,

then $a = hk$ and $b = h_1k_1$ for some $h, h_1 \in H$ and $k, k_1 \in K$.

$ab^{-1} = hk(h_1k_1)^{-1} = hk\ k_1^{-1}h_1^{-1} = h(kk_1^{-1}h_1^{-1})$

$(k k_1^{-1}) h_1^{-1} \in KH = HK$

$\therefore \quad (k_1 k_1^{-1}) h_1^{-1} = h_2 k_2 \in HK$ for some $h_2 k_2 \in HK$

$\therefore \quad ab^{-1} = h h_2 k_2 = (h h_2) k_2 \in HK$

$\Longrightarrow \underline{\underline{HK \leq G}}$

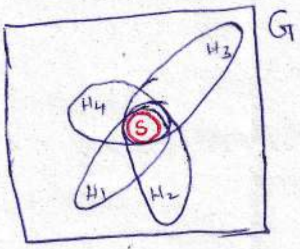
Cyclic groups

Let G be any group and S a subset of G.

Consider the family F of all subgroups of G that contain S, i.e.,

$$F = \{ H \mid H \leq G \text{ and } S \subseteq H \}$$

Theorem $\Rightarrow$ $\bigcap_{H \in F} H$ is a subgroup of G.



Note: (i) $S \subseteq \bigcap_{H \in F} H$

(ii) $\bigcap_{H \in F} H$ is the smallest subgroup of G containing S, i.e., $\min_{H \in F} H = \bigcap_{H \in F} H$

[because, $\bigcap_{H \in F} H$ is a subgroup of G &

$\bigcap_{H \in F} H \subseteq H$ for all $H \in F$

Definition: If S is a subset of a group G, then the smallest subgroup of G containing S is called the subgroup generated by the set S, and is written as $\langle S \rangle$.

$$\langle S \rangle = \bigcap \{H \mid H \leq G,\ S \subseteq H\}$$

(or)

$$\langle S \rangle = \bigcap_{H \in F} H \quad \forall\ F = \{H \mid H \leq G,\ S \subseteq H\}$$

- If $S = \phi$, then $\langle S \rangle = \{e\}$

- If $S = G$, then

G is generated by the set S, and that it S is a set of generators of G.

- If the set S is finite, we say that G is finitely generated.

* Theorem: If S is a non-empty subset of a group G, then

$$\boxed{\langle S\rangle = \left\{ a_1^{n_1} a_2^{n_2} \cdots a_k^{n_k} \,\middle|\, a_i \in S \text{ for } 1 \le i \le k,\ n_1, n_2, \ldots, n_k \in \mathbb{Z} \right\}}$$

Proof

Let $A = \left\{ a_1^{n_1} a_2^{n_2} \cdots a_k^{n_k} \,\middle|\, a_i \in S \text{ for } 1 \le i \le k,\ n_1, n_2, \ldots, n_k \in \mathbb{Z} \right\}$

$\langle S\rangle = \bigcap_{H \in F} H \quad \forall \quad F = \{ H \mid H \le G,\ S \subseteq H \}$

= smallest subgroup of G containing S

$a_1, a_2, \ldots, a_k \in S \subseteq \langle S \rangle$ &

$\langle S \rangle$ is a subgroup of G, i.e.,

$\langle S \rangle \leq G$

$\Rightarrow a_i \in \langle S \rangle \quad \forall \, i = 1, 2, \ldots, k$

$\Rightarrow a_i^{n_i} \in \langle S \rangle \quad \forall \, i = 1, 2, \ldots, k$

$\Rightarrow a_1^{n_1} a_2^{n_2} \ldots a_k^{n_k} \in \langle S \rangle$

$\Rightarrow \underline{\underline{A \subseteq \langle S \rangle}}$

Since any $a \in A$ can be written as $a = a^1$

we have,

$\underline{\underline{S \subseteq A}}$

$S \neq \emptyset \Longrightarrow A \neq \emptyset$ since $S \subseteq A$

Let $x, y \in A$ then

$x = a_1^{n_1} a_2^{n_2} \cdots a_k^{n_k}$ and $y = b_1^{m_1} b_2^{m_2} \cdots b_r^{m_r}$

where, $a_i, b_j \in S$ for $1 \leq i \leq k$, $1 \leq j \leq r$.

Then,

$$xy^{-1} = \left(a_1^{n_1} a_2^{n_2} \cdots a_k^{n_k}\right)\left(b_1^{m_1} b_2^{m_2} \cdots b_r^{m_r}\right)^{-1}$$

$$= a_1^{n_1} a_2^{n_2} \cdots a_k^{n_k} b_r^{-m_r} \cdots b_1^{-m_1} \in A$$

Theorem $\Rightarrow$ A is a subgroup of G.

$S \subseteq A \Rightarrow$ A is a subgroup of G containing S.

$\langle S \rangle$ smallest subgroup of G containing S.

$$\Longrightarrow \langle S \rangle \subseteq A$$

$$\therefore \underline{\langle S \rangle = A}$$

Note: If $(G, +)$ is a group generated by S, S, then any element of G is of the form $n_1 a_1 + n_2 a_2 + \cdots + n_r a_r$ where $a_1, a_2, \ldots, a_r \in S$ and $n_1, n_2, \ldots, n_r \in \mathbb{Z}$.

* A generating group of a group is a subset of the group such that every element of the group can be expressed as a combination (under the group operation) of finitely many elements of the subset and their inverses.

i.e.,

If S is a subset of a group G, then $\langle S \rangle$, the subgroup generated by S, is the smallest subgroup of G containing every element of S, which is equal to the intersection over all subgroups containing the elements of S;

Equivalently,

$\langle S \rangle$ is the subgroup of all elements of G that can be expressed as the finite product of elements in S and their inverses. (Inverse are only needed if the group is infinite, in a finite ~~group~~ group, the inverse of an element can be written as a power of that element).

Ex:-

① Show that $S=\{1\}$ generates $\mathbb{Z}$.

i.e., $\mathbb{Z} = \langle S \rangle$

Ans: For any element $n \in \mathbb{Z}$,

$$n = n.1 \in \langle 1 \rangle$$

$$\therefore \mathbb{Z} = \langle 1 \rangle \quad , \text{ i.e., } \mathbb{Z} = \langle S \rangle$$

$\Longrightarrow S=\{1\}$ generates $\mathbb{Z}$.

② The set $\mathbb{Z}$ of integers is generated by the set $S = \{\pm 1, \pm 3, \pm 5, \ldots\}$ of odd integers.

Ans: For any element $n \in \mathbb{Z}$,

$n = 2^k s$ where $k \geq 0$ & $s \in S$.

$\Rightarrow n \in \langle S \rangle$

$\Rightarrow \langle S \rangle = \mathbb{Z}$

$\Rightarrow \mathbb{Z}$ is generated by the set S of odd integers.

③ Show that a subset S of N generates the group $\mathbb{Z}$ of all integers ~~iff~~ there exist $s_1, \ldots, s_k$ in S and $n_1, \ldots, n_k$ in $\mathbb{Z}$ such that $n_1 s_1 + \cdots + n_k s_k = 1$.

Seen
5/1/2022

Proof.

Given a subset S of N generates the group $\mathbb{Z}$.

$\therefore$

Any $m \in \mathbb{Z}$ can be written as,

$m = m_1 s_1 + \cdots + m_k s_k$ where $s_1, \ldots, s_k \in S$ and $m_1, \ldots, m_k$ are integers.

Since $1 \in \mathbb{Z}$, there must be integers $n_1, \ldots, n_k$ such that

$$1 = n_1 s_1 + \cdots + n_k s_k.$$

④

S

(4) If S generates a group G and $S \subseteq T \subseteq G$, then $\langle T \rangle = G$.

Sweet
Chocolate

Anything is good if it's made of chocolate .

Follow us on

facebook twitter

Type of Ruling:

ruled/unruled

Size: 24 x 18 cm +/- 5 mm
Pages incl.Cover : 152
Max.Ret.Price : ₹ 30/-

9 0123456789

SUN BOOK INDUSTIRES
KUNNAMKULAM-680 503.
PH : 04885-223820