SubGroups

Definition :-

If $(G, *)$ is a group & $H \subseteq G$ is a non empty subset that satisfies the following conditions :

(1) For $a, b \in H$ then $a * b \in H$.

(2) $e \in H$ where e is the identity of $(G, *)$

(3) For any $a \in H$, $a^{-1} \in H$ then $(H, *)$ is called a subgroup of $(G, *)$

Example :- consider $(Z, +)$

(1) $3Z = \{0, \pm 3, \pm 6, \ldots\}$ is a subgroup of $(Z, +)$.

(2) consider $G = (\{1, -1, i, -i\}, \cdot)$

$H = \{1, -1\}$ is a subgroup of G.

If H is a nonempty subset of a group G, then H is a subgroup of G, if H is a group under the same operation as G

H is itself a group $\underline{H \text{ is a}}$ subset of G & H & G use the same binary operation

Theorem :-

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

(ie) A nonempty subset H of a group $(G, *)$ is a subgroup of G iff $a, b \in H \Rightarrow a * b^{-1} \in H$.

Definition :-

$(G, *)$ – group.

H nonempty subset of G, H is a subgroup of G if H itself is a group under the same binary operation $*$.

Proof :-

Necessary part :-

Let $(G, *)$ be a group. H is a non empty subset of G.

Assume H is a subgroup of G.

By definition $(H, *)$ is a group

So $a, b \in H \Rightarrow b^{-1} \in H$ By inverse property

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

$\Rightarrow a * b^{-1} \in H$ By closure property

Sufficient part :

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

H is a nonempty subset of G.

Assume $a, b \in H \Rightarrow a * b^{-1} \in H$ —— (1)

claim : H is a subgroup of G.

i.e $(H, *)$ is a group.

H is a nonempty, so let $a \in H$.

Now $a, a \in H$ by (1) $a * a^{-1} \in H$.

i.e $e \in H$.

identity exists.

$a \in H$, Now by previous step $e \in H$

Now $e, a \in H$ by (1).

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

i.e $a^{-1} \in H$

inverse exists.

$a, b \in H$ by previous step $b^{-1} \in H$.

Now $a, b^{-1} \in H$ by (1).

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

i.e $a * b \in H$

Closure verified.

$a, b, c \in H \quad H \subseteq G \quad a, b, c \in G$

In G, $(a * b) * c = a * (b * c)$

$\therefore$ In H also $(a * b) * c = a * (b * c)$

Associative verified. $(H, *)$ is a group.

ie H is a subgroup of G.

(1) Prove that the intersection of two subgroups of a group is also a subgroup of a group.

(OR)

If H & K are two subgroups of a group $(G, *)$. then $H \cap K$ is also a subgroup.

Soln: Let H_1 & H_2 be any two subgroups of a group G.

To prove that $H_1 \cap H_2$ is also a subgroup of G.

$H_1 \cap H_2$ is a non empty set (i) $H_1 \cap H_2 = \phi$ since atleast the identity element 'e' is common to both H_1 & H_2.

Let $a \in H_1 \cap H_2$ then $a \in H_1$ & $a \in H_2$

$b \in H_1 \cap H_2$ then $b \in H_1$ & $b \in H_2$.

$\therefore H_1$ is a subgroup of G.

$\therefore a * b^{-1} \in H_1$ for $a, b \in H_1$

H_2 is a subgroup of G.

$\therefore a * b^{-1} \in H_2$ for $a, b \in H_2$

$\Rightarrow a * b^{-1} \in H_1 \cap H_2$ when $a, b \in H_1 \cap H_2$

$\therefore H_1 \cap H_2$ is a subgroup of G.

(2) Prove that the union of two subgroups of a group $(G, *)$ need not be a subgroup of G.

Proof :- consider the group $G = (Z, +)$

ie Additive group of integers.

clearly $(2Z, +)$, $(3Z, +)$ are subgroups of $(Z, +)$

ie $H_1 = \{0, \pm 2, \pm 4 \cdots\}$

$H_2 = \{0, \pm 3, \pm 6 \cdots\}$

$H_1 \cup H_2 = \{0, \pm 2, \pm 3, \pm 4, \pm 6 \cdots\}$

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

Since $2 \in H_1 \cup H_2$, $+ 3 \in H_1 \cup H_2$

$2+3 \notin H_1 \cup H_2$

$\therefore H_1 \cup H_2$ is not closed under addition.

$\therefore H_1 \cup H_2$ is not a subgroup of G.

(OR)

Let $H_1 = \{0, 3\}$ & $H_2 = \{0, 2, 4\}$ be a subgroup of G.

$G = \{0, 1, 2, 3, 4, 5, +_6\}$ addition modulo 6.

$H_1 \cup H_2 = \{(0, 2, 3, 4), +_6\}$

$2 +_6 3 = 5 \notin H_1 \cup H_2$

Hence $H_1 \cup H_2$ is not a group.

(3) If G is an abelian group with identity e. prove that all elements x of G satisfying the equation $x^2 = e$ form a subgroup H of G.

Soln Let $H = \{x \in G \mid x^2 = e\}$

(1) As the identity element $e \in G$ satisfies the equation $x^2 = e$ we have

$e^2 = e$ $\because$ $e \in H$ is the identity element of H.

Let $a, b \in H$. $a^2 = e$ & $b^2 = e$.

To prove that

$(a * b^{-1})^2 = e$ i.e $a * b^{-1} \in H$

i.e H is a subgroup of G.

$\because$ G is an abelian

$$(a * b^{-1})^2 = (a * b^{-1}) * (a * b^{-1})$$
$$= a^2 * b^{-12}$$
$$= a^2 * (b^2)^{-1}$$
$$= e * e^{-1} = e$$

$\therefore$ $a * b^{-1} \in H$ & H is a subgroup of G.

cyclic group :-

A group $(G, *)$ is said to be cyclic, if there exists an element $a \in G$, such that every element x of G can be expressed as $x = a^n$ for some integer n.

all elements of G are power of a

$a^n = a.a.\cdots.a$ (n times)

In other words

Let $(G, *)$ be a group then G is called a cyclic group if $\exists$ an element $a \in G$ such that

$$G = \{ a^n \quad n \in Z \}.$$

We say that G is generated by 'a' & we denote $G = (a) = \langle a \rangle$

a is called the generator of G.

Ex :- Multiplicative group $G = \{1, -1, i, -i\}$ is cyclic.

$i^1 = i$	$(-i)^1 = -i$
$i^2 = -1$	$(-i)^2 = -1$
$i^3 = -i$	$(-i)^3 = +i$
$i^4 = 1$	$(-i)^4 = 1$

G is generated by element i & $(-i)$

2. Multiplicative group $G = \{1, \omega, \omega^2\}$ is cyclic.

$\omega^1 = \omega$
$\omega^2 = \omega^2$
$\omega^3 = 1$

$(\omega^2)^1 = \omega^2$
$(\omega^2)^2 = \omega^4 = \omega$
$(\omega^2)^3 = \omega^6 = (\omega^3)^2 = 1$.

$\therefore \omega$ & ω^2 are generators of G.

3. The group $G = \{0, 1, 2, 3, 4, 5, +_6\}$ is cyclic.

$1^1 = 1$
$1^2 = 1 +_6 1 = 2$
$1^3 = 1+1 +_6 1 = 3$
$1^4 = 1 +_6 1^3 = 4$
$1^5 = 1+1+1+\cdots = 5$
$1^6 = 1+1+1+\cdots+1 = 0$

$+_6$	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

$2^1 = 2$
$2^2 = 2 +_6 2 = 4$
$2^3 = 2+2 +_6 2 = 0$
$2^4 = 2+2+2 +_6 2 = 2$

$\langle 2 \rangle = (2, 4, 0)$

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

$3^1 = 3$

$3^2 = 3 +_6 3 = 0$

$\langle 3 \rangle = (3, 0)$

$\langle 4 \rangle = \langle 4, 2, 0 \rangle$

$\langle 5 \rangle = (5, 4, 3, 2, 1, 0)$

$\therefore G = \langle 1 \rangle$ generator by 1

$\because$ 5 is the inverse of 1

$\therefore$ 1 & 5 are generators of G.

order of a group :-

The number of elements of a group (finite or infinite) is called its order.

$|G|$ ⟶ order of the group G.

order of an element :-

If the element $a \in G$ where G is a group with identity element e then the least positive integer m for which $a^m = e$ is called the order of the element a & is denoted by $O(a)$. If there is no such m, then the order of a is infinite

If no such integer exists then a is of infinity order.

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

$O(i) = 4.$

$O(-i) = 4.$

$O(-1) = 2$

$(-1)^1 = -1$

$(-1)^2 = 1$

$i^2 = -1$

$i^3 = -i$

$i^4 = 1$

$i^5 = (i^2)^2 i = i$

$i^6 = (i^2)^3 = -1$

$i^7 = i(i^2)^3 = -i$

$i^8 = (i^2)^4 = 1$

least +ve integer

4, 8 ....

(2) Additive integer is a group

$G = \{0, \pm 1, \pm 2, \dots\}$

$O(G) = \infty$

$O(1) = \infty.$

Properties of a cyclic group :-

(1) Every cyclic group is abelian but abelian group is not cyclic

proof :- Let G be a cyclic group & let a be a generator of G.

Then $G = \langle a \rangle = \{a^n \mid n \in z\}$.

Let $g_1 + g_2$ be any two elements of G.

Then $g_1 = a^m$ & $g_2 = a^k$ for some integers m & k

So $g_1 * g_2 = a^m * a^k$

$= a^{m+k}$

$= a^k * a^m$

$= g_2 * g_1$

Thus G is an abelian group.

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

Proof :- If a is a generator of $(G, *)$ then a^{-1} is also a generator.

Let $b \in G$. Then $b = a^m$ for some $m \in \mathbb{Z}$

$b = a^m = (a^{-1})^{-m} = (a^{-1})^n$ where $n = -m \in \mathbb{Z}$

$\therefore$ a^{-1} is also a generator.

③ If G is a finite group of order n generated by an element $a \in G$ i.e $G = \langle a \rangle$ then (i) $a^n = e$ (ii) $G = \{e, a, a^2, \ldots a^{n-1}\}$ Also n is the least positive integer for which $a^n = e$.

Proof :- If possible, let there exist an $m \in \mathbb{Z}$ such that $a^m = e$ $m < n$.

Since G is cyclic, any element of G can be expressed as a^k for some $k \in \mathbb{Z}$. Let $k = mq + r$ $0 \le r < m$.

$$a^k = a^{mq+r} = a^{mq} \cdot a^r = (a^m)^q \cdot a^r$$

$$= e^q \cdot a^r = a^r.$$

$\therefore a^k = a^r \Rightarrow a^{k-r} = e$.

Thus any element of G can be expressed as a^r; $0 \le r < m$. This means G has only $m < n$ elements which is a contradiction as $o(G) = n$ (given)

$\therefore$

∴ n is the least positive integer such that $a^n = e$.

Hence $G = \{e, a, a^2, \ldots, a^{n-1}\}$

claim : The elements $a, a^2, \ldots, a^{n-1}$ are distinct.

Suppose ~~that~~ not

Let $a^i = a^j \quad i \neq j \quad i < j \leq n$

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

$e = a^{j-i}$, $j - i < n$ a contradiction as n is the least positive integer for which $a^n = e$.

(4) prove that subgroup of a cyclic group is cyclic. Any element a repeatedly multiply we get all the elements in G.

proof :- Let $(G, *)$ be a cyclic group.

Then G has a generator a such that any $b \in G$ is written in the form $b = a^n$ for some $n \in Z$

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

claim :- H is cyclic that is H has a generator

Since $H \subseteq G$ all elements of H are in the form of a^n for some $n \in Z$.

$$H = \{ a^l, a^k, a^m, a^r, a^s \dots \}$$

choose $m = \min \{ \text{all powers of } a \mid a^n \in H \text{ & } n \in Z^+ \}$

i.e. if $r < m$ then $a^r \notin H$ or $r = 0$

claim a^m is generator for H.

Let $b \in H$ $\quad H \subseteq G \quad b \in G$

$\therefore b = a^n$ for some $n \in G$.

Apply division Algorithm for the two integers n, m

$$m \overline{)\, n \,}\ q \qquad r$$

$n = mq + r$ where $0 \le r < m$

$$a^n = a^{mq+r} = a^{mq} * a^r$$

$$a^n = (a^m)^q * a^r$$

$$a^r = a^n * [(a^m)^q]^{-1}$$

$a^m \in H$ By closure $(a^m)^q \in H$

By inverse $\left[(a^m)^q\right]^{-1} \in H$

$a^n \in H$, By closure

$$a^n * \left[(a^m)^q\right]^{-1} \in H$$

i.e. $a^r \in H$.

By the choice of m, we have $r \geq 0$

$\therefore a^n = (a^m)^q$ $\quad a^0 = e$

i.e. $b = (a^m)^q$ for some $q \in \mathbb{Z}$

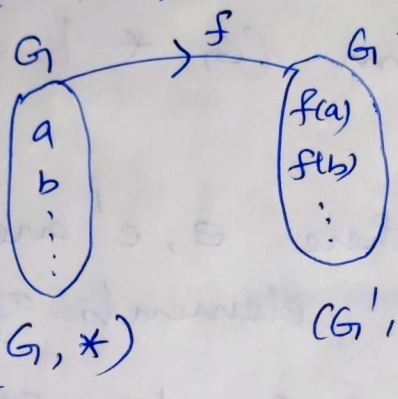
$\therefore$ a^m is a generator for H

i.e. H is a cyclic subgroup of G.

Group Homomorphism :-

If $(G, *)$ & (G', Δ) are two groups, then a mapping $f : G \to G'$ is called a group homomorphism if

$$f(a * b) = f(a) \Delta f(b) \quad \forall a, b \in G \text{ & } f(a), f(b) \in G'$$



Eg :- $(G, +)$ – G - set of all real nos.

$(G', \times)$ – G' – set of non zero real numbers.

$f(x) = 2^x \quad \forall x \in G$.

Let $a, b \in G$ then $f(a) = 2^a$, $f(b) = 2^b$.

$$f(a+b) = 2^{a+b}$$
$$= 2^a \cdot 2^b$$
$$= f(a) \cdot f(b) \quad \forall a, b \in G.$$

Note :- A group homomorphism f is called group isomorphism if f is 1-1 & onto.

Properties :-

If $f : G \to G'$ is a group homomorphism from $(G, *)$ to (G', Δ) then

(i) $f(e) = e'$ where e, e' are identity elements of G & G'

(ii) for any $a \in G$, $f(a^{-1}) = [f(a)]^{-1}$

(iii) If H is a subgroup of G, then $f(H)$ is a subgroup of G' i.e. $f(H) = \{f(h) \mid h \in H\}$

Proof :-

Let $x \in G$, i.e. $f(x) \in G'$

Since f is a homomorphism.

$\therefore x * e = x$

$e' \Delta f(x) = f(x)$

$= f(e * x)$

$= f(e) \Delta f(x)$ $\because f$ is a homomorphism

By using Right cancellation law

$e' = f(e)$.

(ii) To prove $f(x^{-1}) = [f(x)]^{-1} \quad \forall x \in G$.

Let $x \in G \Rightarrow x^{-1} \in G$.

ie $f(x) \in G' \& f(x^{-1}) \in G'$.

Now f is a homomorphism

$f(x) \Delta f(x^{-1}) = f(x * x^{-1}) \quad \because a * a^{-1} = e$

$= f(e)$

$= e'$

ie $f(x^{-1}) = [f(x)]^{-1}$.

(iii) Let $h_1, h_2 \in H \& h_1', h_2' \in f(H)$

ie $h_1' = f(h_1) \& h_2' = f(h_2)$.

$h_1' \Delta (h_2')^{-1} = f(h_1) \Delta [f(h_2)]^{-1}$

$= f(h_1) \Delta f(h_2^{-1})$ by property (ii)

$= f(h_1 * h_2^{-1})$ ∵ f is a homomorphism

$\in f(H)$ ∵ H is a subgroup

i.e. $h_1' \Delta (h_2')^{-1} \in f(H)$ $a, b \in H \Rightarrow a * b^{-1} \in H$

for $h_1', h_2' \in f(H)$.

Thus $h_1', h_2' \in f(H)$

$\Rightarrow h_1' \Delta (h_2')^{-1} \in f(H)$.

∴ $f(H)$ is a subgroup of G'.

Kernel of a homomorphism :-

If $f : G \to G'$ is a homomorphism then the kernel of homomorphism f is denoted by $\ker f$ or K and defined as.

The set of those elements of G which are mapped to the identity element of G' under mapping f.

$$\ker f \text{ or } K = \{ x : x \in G \mid f(x) = e' \}$$

$e' \to$ identity element of G'

Eg :-

(1) $(G, +)$ — Additive group — set of Real numbers

$(G', \times)$ → set of non zero Real numbers.

$f(x) = 2^x \quad \forall x \in G.$

$a, b \in G, \quad f(a) = 2^a$

$f(b) = 2^b.$

$f(a+b) = 2^{a+b}$

$= 2^a \cdot 2^b$

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

$\therefore$ f is a homomorphism.

$f(x) = e^1 = 1$

$2^x = 1$

$\boxed{x = 0}$

$\text{Ker } f = \{0\}$

$\text{Ker } f \in G.$

(2) $(G, +)$ — set of integer.

$G' = \{1, -1\} \quad (G', \times).$

$f(x) = (-1)^x \quad \forall x \in G.$

Let $a, b \in G$.

$$f(a+b) = (-1)^{a+b}$$
$$= (-1)^a \cdot (-1)^b$$
$$= f(a) \cdot f(b)$$

$\therefore$ f is a homomorphism.

$$f(x) = e' = 1$$
$$(-1)^x = 1$$
$$x = 0, \pm 2, \pm 4, \pm 8 - - - -$$

$$\ker f = \{0, \pm 2, \pm 4, \pm 8 - - - -\}$$

(3) $f : G \longrightarrow G'$.

$G = \mathbb{Z}$ $\quad G' = \mathbb{Z}_4$ (Addition modulo 4.

$a = 2, \ b = 5$

$f(2+5) = f(7) = \bar{7} = 3$

$\therefore$ f is a group homomorphism.

$$\ker f = \{ x \in G \mid f(x) = e' \ \ e' \in G' \}$$
$$\text{ie } m \in \mathbb{Z} \mid f(m) = 0 = e'$$

2
5

$f(2) = \bar{2} = 2$
$f(5) = \bar{5} =$

$f(2) +_4 f(5)$
$2 +_4 1$
$= 3.$

$f(0) = \bar{0} = 0$

$f(1) = \bar{1} = 1 \neq 0.$

$f(-1) = (\bar{-1}) = -1+4 = 3 \neq 0.$

$f(4) = \bar{4} = 0$

$f(-4) = -\bar{4} = -4+4 = 0.$

$= \{0, \pm 4, \pm 8 \cdots\}$

$= k \cdot 4 \quad k \in Z$

(4) Consider the groups $(R^+, \cdot)$ & $(R, +)$

Let $f : R^+ \to R$ be defined by $f(x) = \log_{10} x$ check f is a homomorphism or not.

Soln For $x, y \in R^+$

$f(x \cdot y) = \log_{10}(xy)$

$= \log_{10} x + \log_{10} y$

$= f(x) + f(y)$

ie $f(x \cdot y) = f(x) + f(y)$

f preserves the operation.

$\therefore$ f is a homomorphism.

(5) If R & C are additive groups of real & complex no resp & if the mapping $f : C \to R$ is defined by $f(x+iy) = x$. Show that f is a homomorphism & find $\ker f$.

Soln $a+ib, c+id \in C$.

$$f(a+ib+(c+id)) = f(a+c+i(b+d)) = a+c.$$

$$= f(a+ib) + f(c+id).$$

$\therefore$ f preserves operation.

$\therefore$ f is a homomorphism.

$\ker f = \{ x \in C \mid f(x) = 0 \}$

$\because 0$ is the identity element of $(R, +)$

$f(x) = f(a+ib) = 0$

$a = 0$.

$\therefore \ker(f) = \{$ All purely imaginary no $\}$.

(b) If G is the set of all ordered pairs (a,b) of real nos & $*$ is the binary operation defined by

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

G' is the additive group of real nos & $f : G \to G'$ is defined by $f(a,b) = a$ $\forall$ $(a,b) \in G$. check f is homomorphism.

Soln $(a,b), (c,d) \in G$.

$$f((a,b) * (c,d)) = f(a+c, b+d)$$

$$= a + c$$

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

$\therefore$ f preserves operation.

f is homomorphism.