Sub-Group

Let $(G, *)$ be a group and H, be non-empty subset of G. If $(H, *)$ is itself is a group then $(H, *)$ is called Sub-group of $(G, *)$

eg:- Let $G = \{1, -1, i, -i\}$ and $H = \{1, -1\}$. Here G and H are groups w.r.t. binary operation multiplication and H is a subset of G. Therefore, $(H, \cdot)$ is a subgroup of $(G, \cdot)$.

Ex: Let $H = \{0, 2, 4\} \subseteq Z_6$. Check that $(H, +_6)$ is a subgroup of $(Z_6, +_6)$.

Solⁿ $Z_6 = \{0, 1, 2, 3, 4, 5\}$

$+_6$	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

$\therefore (Z_6, +_6)$ is a group

$H = \{0, 2, 4\}$

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

The following conditions are to be satisfied in order to prove that it is subgroup

(i) Closure : let $a, b \in H \Rightarrow a +_6 b \in H$

$0, 2 \in H \Rightarrow 0 +_6 2 = 2 \in H.$

(ii) Identity Element : The row headed by 0 is exactly same as initial row.

$\therefore 0$ is the identity element.

(iii) Inverse: $0^{-1} = 0$, $2^{-1} = 4$, $4^{-1} = 2$

Inverse exist for each element of $(H, +_6)$

$\therefore$ $(H, +_6)$ is a sub-group of $(Z_6, +_6)$.

Cosets

Let $(H, *)$ be a sub-group $(G, *)$ and $a \in G$

Then the subset:

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

is called a left coset of H in G, and the subset

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

is called a right coset of H in G.

In General, $a * H \neq H * a$, however if G is abelian then $\boxed{a * H = H * a}$ $\forall a \in G$

Ex Let $H = \{1, -1\}$ and $G = \{1, -1, i, -i\}$ there $(H, *)$ is a sub-group $(G, *)$.

Sol^n The various left cosets and right cosets of H in G are given below—

Left cosets of H in G	Right cosets of H in G
$1 \times H = \{1, -1\} = H$	$H \times 1 = \{1, -1\} = H$
$-1 \times H = \{-1, 1\} = H$	$H \times -1 = \{-1, 1\} = H$
$i \times H = \{i, -i\}$	$H \times i = \{i, -i\}$
$-i \times H = \{-i, i\}$	$H \times -1 = \{-i, i\}$

Ex Prove that if $(H, *)$ is a sub-group $(G, *)$, then $a * H = H$ if and only if $a \in H$.

Sol^n Let $a * H = H$

Since $e \in H$ then $a = a * e \in a * H$

Hence $a \in H$

Conversely, let $a \in H$ then $a * H \subseteq H$

$(H, *)$ is a sub-group

$\therefore$ $a \in H, h \in H \Rightarrow a^{-1} * h \in H$.

Now $h \in H$

$\Rightarrow h = a * (a^{-1} * h) \in a * H$

$h \in H \Rightarrow h \in a * H$

$\Rightarrow H \subseteq a * H$

Hence $a * H = H$

Q. Prove that the order of any sub-group of a finite group divides the order of the group.

Sol^n Let $(G, *)$ be a finite group of order n and $(H, *)$ be a Sub-group of G of order m.

Let $a_1 * H$, $a_2 * H$, $a_3 * H$, ... $a_K * H$ denote K distinct Left cosets of H in G such that

$$G = (a_1 * H) \cup (a_2 * H) \cup (a_3 * H) \cup (a_4 * H) \ldots \cup (a_K * H)$$

Where all the K Left coset appearing on right hand side are disjoint.

Therefore,

$$O(G) = O(a_1 * H) + O(a_2 * H) + \cdots + O(a_K * H)$$

$$n = m + m + \ldots + K \text{ terms}$$

$$n = km$$

$$K = n/m = O(G)/O(H)$$

Isomorphism of Group

Let $(G, *)$ and (G', Δ) be two groups.

$$f : G \to G'$$

Satisfying $f(a * b) = f(a) \Delta f(b)$, $\forall a, b \in G$ is called an isomorphism of G to G'.

Ex: Consider the Group $(R, +)$ and $(R^+, \times)$ where R^+ denoted the set of positive real numbers. $f_a : R \to R^+$, $a \in R^+$ is defined by $f_a(x) = a^x$.

Sol^n $f_a(x+y) = a^{x+y} = a^x \times a^y$

$\Rightarrow f_a$ is structure preserving

Also, $f_a(x) = f_a(y)$

$$a^x = a^y$$

$$\frac{a^x}{a^y} = 1$$

$$a^{x-y} = 1$$
$$a^{x-y} = a^0$$
$$\therefore\ x - y = 0$$
$$x = y$$

This shows that f_a is one - one.

From the definition

$y \in R^+ \Rightarrow$ There exists a real number x such that $y = a^x$

$y \in R^+ \Rightarrow y = a^x$ for some $x \in R$.

$\Rightarrow y = f_a(x)$

$\Rightarrow f_a$ is onto function

$\therefore$ Thus $(R, +) \cong (R^+, \times)$

Cyclic Group

Let $(G, *)$ be a group. If there exists an element $a \in G$ such that

$$G = \{a^m : m \text{ is an integer}\}$$

i.e. $(G, *)$ is cyclic, if there exists an element $a \in G$ such that every element of G is a power of a and a is called generator of cyclic group.

eg:- $G = \{1, -1, i, -i\}$ is a group w.r.t. binary operation '$\times$'. $(G, \times)$ is a cyclic group.

i is a generator of G.

Since $(i)^4 = 1$

$(i)^3 = -i$

$i^2 = -1$

$(i)^1 = i$

$G = \{i^4, i^3, i^2, i\}$

$= \langle i \rangle$

Similarly $(-i)$ is a generator

$i, -i$ are only generators of G.

Q. Prove that Every cyclic group is abelian.

Proof: Let $(G, *)$ be a cyclic group Generated by a where $x, y \in G$

$\Rightarrow x = a^m$ and $y = a^n$ for some integers m & n

$$x * y = a^m * a^n$$
$$= a^{m+n}$$
$$= a^{n+m}$$
$$= a^n * a^m$$
$$= y * x.$$

This group have a Commutative property. So Every cyclic group is an abelian group.

Ex. $(G, *)$ is group order 60, find all sub-groups of G.

Sol^n The factors of 60 are:

1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60

Let a be a generator of $(G, *)$ then sub-groups of $(G, *)$ are –

$\{e\}, \langle a \rangle, \langle a^2 \rangle, \langle a^3 \rangle, \langle a^4 \rangle, \langle a^5 \rangle, \langle a^6 \rangle, \langle a^{10} \rangle, \langle a^{12} \rangle, \langle a^{15} \rangle, \langle a^{20} \rangle, \langle a^{30} \rangle, \langle a^{60} \rangle$.