Homomorphism: Let $(G,*)$ (H,o) be two groups. a mapping $f: G \to H$ is said to be a group homomorphism if it is $f(x*y) = f(x) \circ f(y)$ $\forall$ $x,y \in G, H$.

→ If homomorphic mapping is 1-1 fn then it is called monomorphism.

→ If 'f' is onto fn that it is called epimorp-ism.

→ A homomorphic mapping "f" is 1-1 and onto. then it is called isomorphism.

Eg: Let $(G,+)(H,\times)$ be two groups then $f: G \to H$ is group homomorphism by $f(x) = 3^x$

$\therefore f(x+y) = 3^{x+y}$

$= 3^x \cdot 3^y$

$= f(x) f(y)$ $\forall x,y \in G, H$.

$\therefore f: G \to H$ is a homomorphism.

Let $(P,*)(Q,\Delta)(R,\oplus)$ be any three groups $f: P \to Q$ $g: Q \to R$ be group homomorphism. then p.T $gof: P \to R$ is also group.

G.T $(P,*)(Q,\Delta)(R,\oplus)$ are any 3 groups. $f: P \to Q$, $g: Q \to R$ be group homomorphisms. Consider

$$gof(x*y) = g(F(x*y))$$
$$= g(F(x) \Delta F(y))$$
$$= g(F(x)) \oplus g(F(y))$$
$$= gof(x) \oplus gof(y)$$

$\therefore gof : P \to R$ is a group of homomorphism.

Cyclic group: Let $(G, *)$ be a group and if $\exists$ $a \in G$ s.t the elements of G can be expressed as some powers of a, then the group $(G, *)$ is called the cyclic group.

i.e., any element can be expressed in the form a^n. where n is the +ve integer and a is called generators of the cyclic group.

Eg: If $G = \{1, -1, i, -i\}$ $(G, \times)$ is a cyclic group.

with $i^4 = 1$, $i^2 = -1$, $i = i$, $i^3 = -i$

$\therefore (G, \times)$ is a cyclic group with 'i' as generator.

Order of an element: The order of an element in a group 'G' is the smallest +ve integer 'n' such that $a^n = e$. If no such integer exist then we say that 'a' is the infinite order.

Eg: Let $G = (1, -1, i, -i)$

$(G, \times)$ is a cyclic group with $e = 1$

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

$(-1)^2 = 1 \Rightarrow O(-1) = 2$ $\quad (-i)^4 = 1 \Rightarrow O(-i) = 4$

Problem:

1) Find the order of every element of $G=\{1,3,5,7\}$ w.r.t. $\times_8$

Sol:

$\times_8$	1	3	5	7
1	(1)	3	5	7
3	3	(1)	7	5
5	5	7	(1)	3
7	7	5	3	(1)

Every group or Klein group

$|X_8 1| = 1^2 = 1 \Rightarrow o(1) = 2$

$3 \times_8 3 = 1 \Rightarrow 3^2 = 1 \Rightarrow o(3) = 2$

$5 \times_8 5 = 1 \Rightarrow 5^2 = 1 \Rightarrow o(5) = 2$

$7 \times_8 7 = 1 \Rightarrow 7^2 = 1 \Rightarrow o(7) = 2$

Sub group: Let $(G, *)$ is a group and $\phi \neq H$ be a non-empty subset of G such that $(H, *)$ is a group then 'H' is called a sub group of G.

Ex: Let $G = \{1, -1, i, -i\}$ $(G, \times)$ is a group.

Let $H = \{1, -1\}$ $H \subset G$

$\times$	1	-1
1	1	-1
-1	-1	1

$(H, \times)$ is a sub group of the group 'G'.

Thm: The identity element of a sub group 'H' of a

group 'G' is same as the identity element of group.

Proof: Let (G, ·) is a group, H' is subset of 'G'. (H, *) is a subgroup of 'G'.

on contradiction let us assume that e and e' are the two identity of G and H respectively.

let 'a' ∈ G, H

∴ 'e' is an element of 'G'.

$$a \cdot e = e \cdot a = a \quad \text{---} (1)$$

also e' is the identity element of H'.

$$a \cdot e' = e' \cdot a = a \quad \text{---} (2)$$

Finally from (1) & (2) ⇒ $a \cdot e = a \cdot e'$

$$e = e' \text{ [LCL]}$$

∴ The identity element of G & H are unique.

Eg: $G = \{1, -1, i, -i\}$ (G, ×) is a group.

$H = \{1, -1\}$ (H, ×) is a sub group.

'1' is the identity element which is same for both G and H.

Coset: Let (G, *) be a group and (H, *) be a sub group of a group 'G', then its left coset and right coset are defined as for any element $a \in G$ & H.

~~H*G~~ $H * a = \{h * a / h \in H\}$ (Right coset)

$a * H = \{a * h / h \in H\}$ (left coset)

~~Note~~:

Order of Cosets: If H is a subgroup of G no. of distinct right coset of G is called index of G. it is denoted by $I(H)$.

Eg: Let G be the set of integers & H is the subgroup of G defined by multiply each element by 3. Find index of H with it.

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

$$H = \{\ldots -9, -6, -3, 0, 3, 6, 9 \ldots\}$$

$$H+1 = \{\ldots -8, -5, -2, 1, 4, 7, 10 \ldots\}$$

$$H+2 = \{\ldots -7, -4, -1, 2, 5, \ldots\}$$

$$H+3 = \{\ldots -9, -6, -3, 0, 3, 6, 9, \ldots\}$$

$\therefore H = H+3$

$H+1 = H+4$

$H+2 = H+5 \ldots$

$\therefore$ The total index $= 3$

$\therefore$ The union of all right coset of H in G is G.

Right Coset decomposition: From the def of left and Right cosets and their properties we note that

1) Left (or) Right coset are the subsets of group.
2) No left (or) Right Cosets of H in G is empty.

3. Any two left (or) right cosets of H in G are either identical or disjoint.

4. The union of all left (or) right cosets of H in G is equal to G.

5. set of all left/right cosets of H in G gives as a partition of G. This partition is called left coset decomposition.

Legranges Theorem:-

If 'G' is a finite group of and H is the subgroup of G. then $O(H) | O(G)$

Proof:- Let 'G' is finite group and 'H' is subgroup of 'G' with binary operation multiplication.

no. of cosets of 'H' in 'G' is ~~binary~~ finite

Let $(Ha_1, Ha_2, \ldots Ha_n)$ are 'n' disjoint coset of H in G.

Then by right coset decomposition the union of all right cosets = element of group 'G'.

$\therefore G = Ha_1 \cup Ha_2 \cup \ldots \cup Ha_n$

where $Ha_1 \cap Ha_2 \cap \ldots \cap Ha_n = \emptyset$

$$O(G) = O(Ha_1 \cup Ha_2 \ldots \cup Ha_n)$$
$$= O(Ha_1) + O(Ha_2) + \ldots + O(Ha_n)$$
$$= O(H) + O(H) + \ldots + O(H)$$

~~Let~~ $O(G) = nO(H)$

$O(H) | O(G)$.

Eg:- $G = \{1, -1, i, -i\}$ $(G, \times)$ is a group

Let $H = \{1, -1\}$ $(H, \times)$ is a subgroup

$O(G) = 4$

$O(H) = 2$

$2 | 4$

$\Rightarrow O(H) | O(G)$.

Normal subgroup:- A subgroup H of a group G is said to be a normal subgroup of G.

if $xhx^{-1} \in H \quad \forall \; x \in G$

$h \in H$

Ex:- Let $G = \{1, -1, i, -i\}$ $(G, \times)$ is a group

$H \subset G$ Let $H = \{1, -1\}$ $(H, \times)$ is a subgroup

Let $1 \in G, -1 \in H$ then $xhx^{-1} = 1 \times (-1) \times 1 = -1 \in H$

Let $i \in G, -1 \in H \Rightarrow xhx^{-1} = i \times (-1) \times (-i) = -1 \in H$

All elements of $x \in G, h \in H$ satisfy for $H = \{1, -1\}$

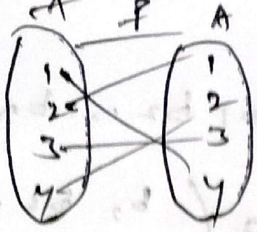
$\therefore$ $(H, \times)$ is a normal subgroup.

Permutation groups:- A permutation is a 1-1 mapping of a non-empty set onto itself. i.e., $f: A \to A$ be a permutation such that $f(a_1) = b_1, f(a_2) = b_2, \ldots f(a_n) = b_n$

$\forall \; a_1, a_2, \ldots a_n \in A$. with this as $f = \begin{pmatrix} a_1 & a_2 & \ldots & a_n \\ b_1 & b_2 & \ldots & b_n \end{pmatrix}$

$b_1, b_2, \ldots b_n$

Ex:- $A = \{1, 2, 3, 4\}$



$$f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}$$

Equal permutation: Let S be a non-empty set & two permutation f & g defined on the non-empty set S are set to be equal if $f(a) = g(a)$ $\forall a \in S$

i.e., Ex:- $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$, $g = \begin{pmatrix} 3 & 2 & 1 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}$

Identity permutation: Let S be a finite non-empty set an identity permutation on S denoted by I, and defined as $I(a) = a$ $\forall a \in S$

$$I = \begin{pmatrix} a_1 & a_2 \cdots a_n \\ a_1 & a_2 \cdots a_n \end{pmatrix}$$

Inverse permutation: Let $f = \begin{pmatrix} a_1 & a_2 \cdots a_n \\ b_1 & b_2 \cdots b_n \end{pmatrix}$

$$f^{-1} = \begin{pmatrix} b_1 & b_2 \cdots b_n \\ a_1 & a_2 \cdots a_n \end{pmatrix}$$

Theorem: Let S_n be set of all permutation defined on the non-empty sets & G is group of w.r.to Operation Circle $(\circ)$ i.e $(S, \circ)$ is a permut

< ration group.

Proof:- Let $S=\{a_1, a_2 \dots a_n, b_1 b_2 \dots b_n, c_1 c_2 \dots c_n\}$

and $f=\begin{pmatrix} a_1 & a_2 \dots a_n \\ b_1 & b_2 \dots b_n \end{pmatrix}$ $g=\begin{pmatrix} b_1 & b_2 \dots b_n \\ c_1 & c_2 \dots c_n \end{pmatrix}$

closure:- since f & g are two permutations

$$gof=\begin{pmatrix} a_1 & a_2 \dots a_n \\ c_1 & c_2 \dots c_n \end{pmatrix}$$

gof is also a permutation. $\therefore$ o is closed.

associative:- composition matrix o is always associative

i.e., $fo(goh)=(fog)oh$

identity:- let identity permutation $I=\begin{pmatrix} a_1 & a_2 \dots a_n \\ a_1 & a_2 \dots a_n \end{pmatrix}$

$$foI=\begin{pmatrix} a_1 & a_2 \dots a_n \\ b_1 & b_2 \dots b_n \end{pmatrix}=f$$

$\therefore foI=Iof=f$

$\therefore$ o satisfy identity properties.

Inverse:- $f^{-1}=\begin{pmatrix} b_1 & b_2 \dots b_n \\ a_1 & a_2 \dots a_n \end{pmatrix}$

$$ff^{-1}=\begin{pmatrix} b_1 & b_2 \dots b_n \\ b_1 & b_2 \dots b_n \end{pmatrix}=I$$

$\therefore ff^{-1}=f^{-1}of=I$

$\therefore (S,o)$ is a permutation on group.