(#) cyclic subgroup generated by a group element

You may not have a cyclic group $(G, *)$ but we can derive a cyclic subgroup $(H, *)$ from G

→ Let $(G, *)$ be a group

$x \in G$, such that $order(x) = m$

$H = \{ x^0 = e, x^1 = x, x^2 \ldots\ldots x^{m-1} \}$

(e: identity)

$H \subseteq G$ & all elements of H are distinct

Then H is a cyclic group subgroup of order m generated by x

$$H = \langle x \rangle$$

We have to prove group axioms satisfied for H.
To do that we have to show only S_1 & S_2 satisfied

S_1 : for any $x^i, x^j \in H$ we have

$$x^i * x^j = x^{i+j} = x^{(i+j) \bmod m} \in H$$

$x^{i+j} = x^{(i+j) \bmod m}$ $\because$ $x^m = 1$ (identity)

$(i+j) \bmod m \Rightarrow$ gives remainder from 0 to $m-1$

$\therefore$ any power of x from m 0 to $m-1$ is part of H

$\therefore$ closure property satisfied.

S_2 : consider any arbitrary $x^i \in H$, where $i > 0$

$\because$ if $i = 0$ $x^0 = e$ identity

we need to check for non identity elements

$$x^i \cdot x^{m-i} = x^m = 1 \quad 0 < i \leq m-1$$

$$x^{m-i} \in H$$

since $x^{m-1} \in H$ the inverse of x^1 is x^{m-1}

Left and Right coset

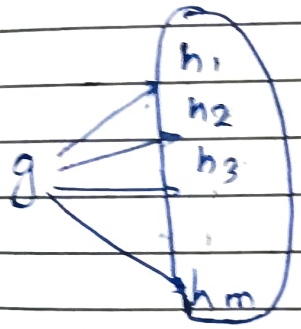
Let $(G, *)$ be a group and $(H, *)$ be a subgroup of G, and let $g \in G$

i) Left coset of H w.r.t g →

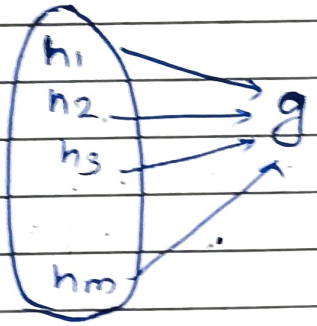
$$gH = \{g * h \mid h \in H\}$$

ii) Right coset of H w.r.t g

$$Hg = \{h * g \mid h \in H\}$$



Left coset



Right coset

- Proof: If H is a finite subgroup, then for any $g \in G$, we have $|gH| = |Hg| = |H|$

- Let $H = \{h_1, h_2 \dots h_n\}$

$$gH = \{g*h_1, g*h_2 \dots g*h_n\}$$

From ~~Left~~ cancellation rule, all these elements are distinct.

$\therefore gh_i = gh_j \Rightarrow h_i = h_j$

$\therefore$ all elements are distinct as

all

eg consider a subgroup $H = \{1, 10\}$

$G = Z_{11}^* = \{1, 2, \ldots\ldots 10\} \Rightarrow$ +ve Integers coprime to

The operation is $\times_{11}$

$1 \times_{11} H = \{1, 10\}$ $\quad$ $6 \times_{11} H = \{6, 5\}$

$2 *_{11} H = \{2, 9\}$ $\quad$ $7 \times_{11} H = \{7, 4\}$

$3 \times_{11} H = \{3, 8\}$ $\quad$ $8 \times_{11} H = \{8, 3\}$

$4 \times_{11} H = \{4, 7\}$ $\quad$ $9 \times_{11} H = \{9, 2\}$

$5 \times_{11} H = \{5, 6\}$ $\quad$ $10 \times_{11} H = \{10, 11\}$

Note that, Left cosets can be identical or disjoi

eg $1 \times_{11} H = 10 \times_{11} H$

$2 \times_{11} H = 9 \times_{11} H$

- Proof : Let $(G, *)$ be a group, $(H, *)$ be a subgroup of G and let $g_1, g_2 \in G$. Then either $g_1 * H = g_2 * H$ or $g_1 * H \cap g_2 * H = \phi$

Lets recap terms:

1) Equivalance class
2) Partition

1) Equivalance class

+ A relation said to be equivalant if it satisfies reflexive, symmery and transitive property

+ Let R be an equivalance relation on a set A. The set of all elements that are related to an element 'a' with respect to 'R' is denoted by $[a]_R$ is called as equivalance class of 'a'.

$[a]_R = \{ (a,s) \mid s \in R \}$

$\{ s \mid (a,s) \in R \}$

Any element $b \in [a]_R$ called as representative of the equivalance class.

eg Let R be the relation on set of integers, such that aRb iff $a = b$ or $a = -b$.

- In this case $[a] = \{a, -a\}$

$[7] = \{7, -7\}$

$[0] = \{0\}$

2) Partitions :-

- Let A be the set of students at your school who are majoring in exactly one subject.
- R is a relation defined over A

$R = \{(x,y) \mid x \text{ and } y \text{ are students with same major}\}$

- Here R is an equivalance relation.
- R splits A into disjoint sets (subsets), where each subset contains students with specified major.
- These subsets are equivalance classes of R

Theorem 1: Let R be the equivalance relation on set A then equivalance classes of two elements of A either identical or disjoint

[illegible]

Let R be an equivalance relation on set A. These statements for elements a and b of A are equivalant

i) aRb ii) $[a] = [b]$ iii) $[a] \cap [b] \neq \phi$

Proof: Lets understand first the terms

i) aRb - a is related to b where $a, b \in A$

ii) $[a] = [b] \Rightarrow$ Equivalance class of a and equivalance class of b are equal.

$$[a] = \{s \mid (a, s) \in R\}$$
$$[b] = \{s \mid (b, s) \in R\}$$

iii) $[a] \cap [b] \neq \phi$

Interseection of $[a]$ and $[b]$ cannot be Null

We first show i) implies ii) Then ii) implies iii) and finally iii) implies i)

① i) implies ii)

$aRb \rightarrow [a] = [b]$

→ Assume aRb

we will prove $[a] = [b]$ by $[a] \subseteq [b]$ & $[b] \subseteq [a]$

Suppose $c \in [a]$,

Then we have aRc

We know that aRb & R is symmetric

$\Rightarrow$ bRa is present in R

Also R is transitive

$\therefore bRa \rightarrow aRc \Rightarrow bRc$

This implies $c \in [b]$

This proves $[a] \subseteq [b]$

similarly we can prove $[b] \subseteq [a]$

② $[a] = [b] \rightarrow [a] \cap [b] \neq \phi$

Assume $[a] = [b]$, This follows

$[a] \cap [b] \neq \phi$

because [a] is non empty on R is reflexive
$a \in [a]$

③ $[a] \cap [b] \neq \phi \rightarrow aRb$

Let $[a] \cap [b] \neq \phi$

Then there is an element 'c' with $c \in [a]$ and $c \in [b]$.

In otherwords we have, aRc and bRc, by symmetric property we also have cRb

$\therefore aRc, cRb \rightarrow aRb$ proved!

- Let R be the equivalance relation on set A. The union of the equivalance classes of R is all of A.

$$\bigcup_{a \in A} [a]_R = A$$

This follows

$[a]_R \cap [b]_R = \phi$ (If disjoint)

$[a]_R \cap [b]_R \neq \phi$ (If identical)

eg $S = \{1, 2, 3, 4, 5, 6\}$, The collection of sets $A_1 = \{1, 2, 3\}$ $A_2 = \{4, 5\}$ and $A_3 = \{6\}$ forms a partition on 'S' because these sets are disjoint & forms 'S' on union.

If R be the relation on set 'S' Then equivalance classes of R form a partition of 'S'.

eg List all the ordered pairs in the equivalance relation 'R' produced by the partition $A_1 = \{1, 2, 3\}$ $A_2 = \{4, 5\}$ $A_3 = \{6\}$. of $S = \{1, 2, 3, 4, 5, 6\}$

1) From $A_1 = \{1, 2, 3\}$

pairs = $\{(1,1), (2,2), (3,3), (1,2), (2,1), (1,3), (3,2), (2,3)\} \in R$

2) From $A_2 = \{4, 5\}$

pairs - $\{(4,4), (5,5), (4,5), (5,4)\} \in R$

3) From $A_3 = \{6\}$

pairs = $\{(6,6)\} \in R$

* Now lets go back to our proof on cosets

Let $(G, *)$ & $(H, *)$ be a group & subgroup respectively. & let $g_1, g_2 \in G$. then either

$$g_1 * H = g_2 * H$$

OR

$$g_1 * H \cap g_2 * H = \phi$$

→ This is the condition similar to equivalance class that creates partitions as discussed in previous topic

That is we have to prove cosets are identical or disjoint.

If we can prove the the relation R, where

$$xRy \Rightarrow y \in xH$$ (i.e. y belongs to coset) is an equivalance relation.

① Relation R is reflexive

$x = x * e \Rightarrow x \in xH$

$\therefore e \in H$ & $x * e = x$

$\therefore$ we have a relation $xRx \Rightarrow$ reflexive relation

② Relation R is symmetric

Let: xRy

$y = x * h_1$ for some $h_1 \in H$ —①

multiply both sides by $(h_1)^{-1}$

$x = y * (h_1)^{-1}$

We know that $h_1 \in H$ then $(h^{-1}) \in H$ ∵

∴ H is a sub group.

∴ $x \in yH \Rightarrow yRx$

∴ we have xRy & $yRx \Rightarrow$ symmetric

③ Relation R is transitive

let xRy & yRz

$y = x * h_1$ for some $h_1 \in H$ —①

$z = y * h_2$ for some $h_2 \in H$ —②

$z = (x * h_1) * h_2 = x * (h_1 * h_2) \in xH$

∴ $h_1 * h_2 \in H \Rightarrow h_1$

∴ $x * (h_1 * h_2) \in xH$.

∴ This is a transitive relation.

∴ R creates a partition of G, with cosets constituting the equivalance classes

Lagrange's Theorem

+ Let 'G' be the finite group of order 'n' and H be a subgroup of order 'm'. Then m divides n.

→ • Size of each coset = m

we have proved that $|xH| = |Hx| = |H|$

∴ Size of coset = m

• We have also proved that any cosets are either disjoint or same

• The set of distinct cosets constitutes partition of G.

Lets say we have 'k' distinct cosets

The union of all cosets ⇒ G

$k \cdot m = n \Rightarrow$

m divides n

$k * |xH| = |G|$

Lets revisit whatever we have discussed so far about subgroups

1) subgroup = subset + Group

$H \leq G$ - Notation

Two standard / trivial subgroups

① G

② $\{e\}$

As per Lagrange's theorem, If $H \leq G$, then order of H divides the order of G.

order of $G = |G|$

If $H \leq G \rightarrow |H|$ divides $|G|$

That means subgroups cannot be of any size there is strong restriction on possible subgroup size.

eg Let G be the group with $|G| = 323$

The divisors of $323 = 1, 17, 19, 323$

Then possible subgroups orders: $1, 17, 19, 323$

We know two trivial subgroup

① $G \rightarrow |G| = 323$

② $\{e\} \rightarrow |\{e\}| = 1$

Any other possible subgroup has order 17 or 19

Q $|G| = 323$ (17×19)

Does Lagrange's theorem say there are subgroups of order 17 and 19?

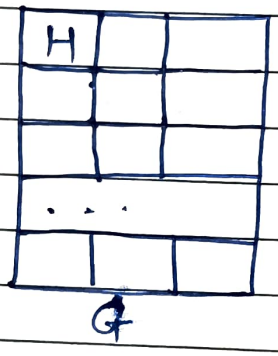
- NO!

According to Lagrange's theorem

If $H \leq G$ THEN $|H|$ divides $|G|$

* This doesn't mean if $|H|$ divides $|G|$ then $H \leq G$

G is partitioned into cosets



$|G| = n$

$|H| = d$

If # cosets $= K$

$\therefore k \cdot d = n$

$\rightarrow$ 'd' divides 'n'

Remember that G is partitioned into coset & only 'H' is subgroup of G as only H contains identity element

Normal subgroup & factor (quotient)

Lets take a motivating example

Z $\rightarrow$ set of integers

operation - Integers mod 5

The operation divides Z into 5 sets according to remainder

$r = 0$: {---15, -10, -5, 0, 5, 10, 15---}

$r = 1$ {--- -14, -9, -4, 0, 6, 11, 16--}

$r = 2$ {--- -13, -8, -3 0, 7, 12, 17--}

$r = 3$ {--- -12, -7, -2, 0, 8, 13, 18--}

$r = 4$ {--- -11, -6, -1, 0, 9, 14, 19--}

Critical observation

① If you take any number from $r=0$ & add to $r=2$ you will get always a number from set $r=3$

To generalize take any number from set 1 and add to any number from any set 2 then output will be from one of the 5 sets

These 5 sets are called as congruent classes

$\bar{0} = \{\ldots -15, -10, -5, 0, 5, 10, 15 \ldots\}$
$\bar{1} = \{\ldots -14, -9, -4, 1, 6, 11, 16 \ldots\}$
$\bar{2} = \{\ldots -13, -8, -3, 2, 7, 12, 17 \ldots\}$
$\bar{3} = \{\ldots -12, -7, -2, 3, 8, 13, 18 \ldots\}$
$\bar{4} = \{\ldots -11, -6, -1, 4, 9, 14, 19 \ldots\}$

If we treat these 5 sets as numbers then we create a set Z with these 5 elements

$$Z = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$$

Now we can have a group Z_5
These meta numbers indeed forms a group under addition.

1) closure property satisfied $\bar{0} + \bar{1} \in Z$

$\bar{3} + \bar{2} = \bar{0} \in Z$

2) Associative - addition operation itself is associative

3) Identity - $\bar{0}$

4) Inverse $\bar{0} \to \bar{0}$
$\bar{1} \to \bar{4}$
$\bar{2} \to \bar{3}$
$\bar{3} \to \bar{2}$
$\bar{4} \to \bar{1}$

306
2034

When two integers are in same congruence class then we write

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

a is congruent to b mod n

That means 'a' & 'b' have same remainder when divided by 'n'.

- Now Lets consider a group $(Z, +)$.

We have subgroups as

$$Z, 2Z, 3Z, 4Z, 5Z, 6Z \ldots\ldots$$

All these sets satisfies group axioms. & they are subsets of Z.

Lets take 5Z subgroup

$5Z = \{\ldots -15, -10, -5, 0, 5, 10, \ldots\}$ - subgroup

$5Z+1 = \{\ldots -14, -9, -4, 1, 6, 11, \ldots\}$

$5Z+2 = \{\ldots -13, -8, -3, 2, 7, 12, \ldots\}$

$5Z+3 = \{\ldots -12, -7, -2, 3, 8, 13 \ldots\}$

$5Z+4 = \{\ldots -11, -6, -1, 4, 9, 14 \ldots\}$

} cosets

Z

group Z

The ~~set~~ is divided into 5 distinct cosets formed using 5Z subgroup

This creates a partition.

Note that only 5Z satisfies group axioms

5Z+1	closure ✗
5Z+2	inverse ✗
5Z+3	identity ✗
5Z+4	

We used subgroup $5\mathbb{Z}$ to partition to group $\mathbb{Z}$ into cosets, and because the cosets form the group we call $5\mathbb{Z}$ as normal subgroup and group of ~~quotient~~ cosets is called quotient group.

Here quotient group is denoted as $\mathbb{Z}/5\mathbb{Z}$
we are using subgroup $5\mathbb{Z}$ to divide the group $\mathbb{Z}$ into quotient group

- Note that, cosets are → $0+5\mathbb{Z}, 1+5\mathbb{Z}, 2+5\mathbb{Z}, 3+5\mathbb{Z}, 4+5\mathbb{Z}$.
  Now we can consider these cosets as elements in a new group called as coset group
- Note that it is not necessary the cosets always form a group; If cosets do not form a group then we do not call 'N' as normal subgroup, and we cannot make a quotient group

Cosets problems

Defn :- Let H be a subgroup of G and $a \in G$. then the set

$aH = \{ah \mid h \in H\}$ is called left coset of H in G

$Ha = \{ha \mid h \in H\}$ is called right coset of H in G

By defn it is clear that corresponding to every element of G, we have a left coset & right coset of H in G.

$$aH \subset G, \quad Ha \subset G \quad \forall a \in G$$

Furthermore note that, $eH = H = He$

left & right cosets of H corresponding to the identity 'e' coincides with H.

Hence 'H' itself is a left as well as right coset of H in G.

eg (1)

$G = (\mathbb{Z}, +)$ & $H = 2\mathbb{Z} = \{\cdots -4, -2, 0, +2, 4 \cdots\}$ then right cosets of H in G

$\Rightarrow$

$H+0 = \{\cdots -4, -2, 0, 2, 4 \cdots\}$

$H+1 = \{\cdots -3, -1, 1, 3, 5 \cdots\}$

$H+2 = \{\cdots -2, 0, 2, 4, 6 \cdots\} = H$

$H+3 = \{\cdots -3, -1, 1, 3, 5, \cdots\} = H+1$

Here $H+1 = H+3 = H+5 = \cdots$

$H = H+2 = H+4 = \cdots$

$\therefore G = H \cup (H+1)$

Here 'G' has only two distinct cosets $(H, H+1)$

eg 2. Find all cosets of $3\mathbb{Z}$ in the group $(\mathbb{Z}, +)$

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

$H+0 = \{\ldots -9, -6, -3, 0, 3, 6, 9, \ldots\}$
$H+1 = \{\ldots -8, -5, -2, 1, 4, 7, 10 \ldots\}$
$H+2 = \{\ldots -7, -4, -1, 2, 5, 8, 11 \ldots\}$
$H+3 = \{\ldots -6, -3, 0, 3, 6, 9, \ldots\} = H+0$
$H+4 = \{\ldots -5, -2, 1, 4, 7, 10 \ldots\} = H+1$

cosets are $H, H+1, H+2$

$G = H \cup H+1 \cup H+2$

Remark: There are 'n' cosets of $n\mathbb{Z}$ in $(\mathbb{Z}, +)$.

Q.3) Find all the cosets of $H = \{0, 4\}$ in the group $(\mathbb{Z}_8, +_8)$

$\Rightarrow$ $G = \{0, 1, 2, 3, 4, 5, 6, 7\}$ $+_8$
$H = \{0, 4\}$

$H+0 = \{0, 4\}$
$H+1 = \{0+_8 1, 4+_8 1\} = \{1, 5\}$
$H+2 = \{0+_8 2, 4+_8 2\} = \{2, 6\}$
$H+3 = \{0+_8 3, 4+_8 3\} = \{3, 7\}$
$H+4 = \{0+_8 4, 4+_8 4\} = \{4, 0\} = H$
$H+5 = \{0+_8 5, 4+_8 5\} = \{5, 1\} = H+1$

There are 4 distinct cosets $\Rightarrow H, H+1, H+2, H+3$.

- If H is subgroup of G & $g \in G$, then prove

a) $gHg^{-1} = \{ghg^{-1} \mid h \in H\}$ is a subgroup of G
b) If H is finite, then $O(H) = O(gHg^{-1})$

→ a) Let $x = gh_1g^{-1} \in gHg^{-1}$
$y = gh_2g^{-1} \in gHg^{-1}$

where $h_1, h_2 \in H$

then
$$xy^{-1} = (gh_1g^{-1})(gh_2g^{-1})^{-1}$$
$$= (gh_1g^{-1})((g^{-1})^{-1} \cdot h_2 \cdot g^{-1})$$
$$= (gh_1g^{-1})(g \cdot h_2^{-1}g^{-1})$$
$$= gh_1(g^{-1} \cdot g) \cdot h_2^{-1}g^{-1}$$
$$= gh_1(e) \cdot h_2^{-1}g^{-1}$$
$$= gh_1h_2^{-1} \cdot g^{-1}$$
$$= gh_1h_2^{-1}g^{-1} \in gHg^{-1}$$

$\therefore h_1h_2^{-1} \in H$

only one cond^n is enough to check subgroup - inverse cond^n

$\because a, b \in G$ then $(ab)^{-1} = b^{-1}a^{-1}$

Proof $(ab)^{-1} = b^{-1}a^{-1}$?

$(ab)^{-1}(ab) = e$ - identity
$(ab)^{-1}(ab)b^{-1} = e \cdot b^{-1}$ - multiply by b^{-1}
$(ab)^{-1}(a \cdot b \cdot b^{-1}) = eb^{-1}$
$(ab)^{-1}(a) = b^{-1}$
$(ab)^{-1} \cdot a \cdot a^{-1} = b^{-1}a^{-1}$ - multiply by a^{-1}
$ab^{-1} \cdot e = b^{-1}a^{-1}$
$\Rightarrow (ab)^{-1} = b^{-1}a^{-1}$

• **Theorem**: If H is subgroup of a group G and $a \in G$ then

$a \in aH$ and $a \in Ha$

Proof: Let e be identity of G so also of H.

$a \in G, \; e \in H, \rightarrow ae = a \in aH$

$e \in H \rightarrow ea = a \in Ha$

$\Rightarrow aH \neq \phi \;\&\; Ha \neq \phi$

Ⓐ **cosets**: Left coset & right coset are subset of G.

$(G, *)$ - group $\quad (H, *)$ - subgroup

let $g \in G$

Left coset $\Rightarrow g \cdot H$

We know that, $\forall h \in H, \; h \in G$ also as $H \subseteq G$.

and G satisfies closure property

$\therefore g * h \in G$

$\therefore$ left coset is subset of G

similarly we can prove for right coset

• **Theorem**: If H is a subgroup then for $h \in H$

$h * H = H = H * h$

Here $(H, *)$ is a subgroup of $(G, *)$ & $h \in H$.

$\Rightarrow$ ~~We will first try to prove $hH = H$~~

To prove $h*H = H$ we need to prove two conditions

i) $h*H \subseteq H$ ii) $H \subseteq hH$

① $h*H \subseteq H$, we know $h \in H$

Let $h' \in H$, then

multiply by h

$h'*h \in H*h$ —①

we know that $h' \in H$ & $h \in H$ then by closure property

$h'*h \in H$ —②

∴ we can say that $Hh \subseteq H$

⇒ We will first try to prove $Hh = H$, To prove this we need to prove two conditions

1) $H*h \in H$ 2) $H \subseteq H*h$

1) $H*h \subseteq H$, we know $h \in H$

Let $h' \in H$, multiply by h

⇒ $h'*h \in H*h'$ —①

as both h' & $h \in H$, by closure property

$h'*h \in H$ —②

∴ from ① & ②

$H*h \subseteq H$

2) $H \subseteq H*h$

let $h_1 \in H$, we know $h \in H$

by inverse property, $h^{-1} \in H$.

$h_1 \in H$ —①

$h^{-1} \in H$

by closure property

$h_1 * h^{-1} \in H$ — (II)

multiply by h to eqn (II)

$h_1 * h^{-1} * h \in H * h$

$h_1 * e \in H * h$

$h_1 \in H * h$ — (III)

from (I) & (III)

$H \subseteq H * h$.

Group 'G' is union of all Left or right cosets.

⇒ proof: If $H \leq G$, then G is union of all right cosets of H in G

Let S = union of all right cosets in G

$S = H \cup Ha_1 \cup Ha_2 \cdots Ha_n$

where $a_i \in G$, $i \neq 1$ to n

We need to prove that S is a group G i.e.

$S = G$

To prove this we need to prove 2 conditions

i) $S \subseteq G$ ii) $G \subseteq S$

① $S \subseteq G$

let $x \in S$,

so x can be either belongs to H, or Ha_1 or $Ha_2 \cdots$

We have already proved that cosets are subsets of G

$\therefore Ha_i \subseteq G$

$\therefore$ x can belong to any coset & the coset itself is subset of G.

$\therefore x \in G$

$\therefore S \subseteq G$

2) similarly we need to prove $G \subseteq S$

let $a_1 \in G$, we need to prove $a \in S$

$$a_1 = e * a_1 \quad -(1)$$

we know that $e \in H$

$\therefore$ I can write $a_1 \in Ha$

$\because (e \in H \rightarrow e * a = a)$

If $a \in Ha$ then $a_1 \in S$

$\because S = H \cup Ha_1 \cup Ha_2 \cup a_3 \cdots$

$\Rightarrow a \in S \Rightarrow G \subseteq S$

same we can prove for left cosets

Normal subgroup:

so for we discussed about group, subgroups & cosets created from subgroup

Now lets define a normal subgroup,

It is a type of subgroup

Let G be the group & $H \leq G$

let $x \in G$, then

left coset $\Rightarrow xH$

Right coset $\Rightarrow Hx$

We know if group is abelian group then

$$xH = Hx \quad \forall x \in G$$

But if G is not an Abelian group, it is not necessary to satisfy left coset = right coset.

- If G is not Abelian and still left cosets & right cosets are equal then we call such 'H' as normal subgroup

$xH = Hx \quad \forall x \in G$ even 'G' is not abilian 'H' is a normal subgroup

* That mean if G is Abelian then all its subgroups are normal subgroups

Note that for non Abelian group.

$Hx = xH$ must be satisfied for all $x \in G$

It is denoted by,

$$\boxed{H \trianglelefteq G}$$

Trivial normal subgroups / Improper Normal subgroup

1) $H = \{e\}$
2) $H = G$

Non trivial or proper normal subgroups

$H \subsetneq G$ & $x \in H$ $x \neq e$

$$\boxed{H \trianglelefteq G}$$

- Simple group :- A group for which no proper normal subgroup exists.

eg let G be a group of order 3

- By lagranges theorem we know that, order of subgroup is multiple of 3

∴ It can be either 1 or 3 i.e.

it can be either $\{e\}$ or G it self.

∴ it is a simple group

* H is a normal subgroup iff $xHx^{-1} = H$

i.e

$$H \trianglelefteq G \leftrightarrow xHx^{-1} = H$$

$$\downarrow$$

$$xH(x^{-1} \cdot x) = Hx$$

$$xHe = Hx$$

$$xH = Hx \rightarrow \text{Normal subgroup}$$

G

H	xH
	Hy

$yH = Hx$

Theorem: If $H \trianglelefteq G$ then each left coset of H in G is a right coset of H in G.

Note here we are not restricting

$xH = Hx$ by

but it is also true for $y \in G$

$xH = Hy$.

→ We know $xHx^{-1} = H$ & $xH = Hx$

$$xH = Hx \quad \text{—(i)}$$

we have also proved that two cosets of a group are either disjoint or identical i.e.

let $x, y \in G$

xH & yH are two cosets

$\therefore$ 1) $xH = yH$ or

2) $xH \cap yH = \phi$

$\therefore$ If I consider these are ~~disjoint~~ identical then eq^n (1) becomes

$yH = Hx$ → Hence proved.

Similarly we can prove converse

i.e. given $xH = Hy$ - prove $H \trianglelefteq G$

$x, y \in G$.

→ $x \in xH$ is possible ? yes $\because e \in H$

$\therefore x \in x \cdot e \Rightarrow x \in xH$

$x \in xH$ —(1) left cosets

we know that $xH = Hy$

$\therefore x \in Hy$ — (2)

can $x \in Hx \Rightarrow$? Right coset yes!

$\therefore e \in H, \quad x \in Hx$ — (3)

$x \in Hy$ from (2) $\quad x \in Hx$ from (3)

We know that two cosets are distinct or identical

$\therefore Hy = Hx$ — (4)

We have given $xH = Hy$

$\therefore xH = Hx \Rightarrow$ Normal subgroup condn

$\therefore H \trianglelefteq G$

- **Theorem** → if $H \trianglelefteq G$ then product of two right coset is again a right coset.

(i) lets prove first implication

$H \trianglelefteq G \longrightarrow Hx * Hy = H * z, \forall x, y, z \in G$

let x, y be any two elemen of G

take product of right cosets

$(Hx)(Hy)$ — (1)

we know it satisfies associativity property

$\therefore = H(xH)y$ — (2)

We know $H \trianglelefteq G \quad \therefore xH = Hx$

$\therefore = H(Hx)y$ — (3)

Again consider associativity

$(HH)xy$ — (4)

As $HH = H$ ($\because$ closure property)

$= Hxy$ Now. we considered $x, y \in G$

$\therefore xy \in G$ let $xy = z$

$= \underline{\underline{Hz}}$ Rigu coset.

ii) Now we will prove converse

$(Hx)(Hy) = Hz$ then $H \trianglelefteq G$

lets take an inverse of x as x^{-1}

$\therefore (Hx)(Hx^{-1}) \Rightarrow$ is also a rigu coset — ①

Now we know

$e \in H$

$\therefore (ex)(ex^{-1}) \in (Hx)(Hx^{-1})$

$\Rightarrow$

$x x^{-1} \in (Hx)(Hx^{-1})$

$e \in (Hx)(Hx^{-1})$

$e \in$ rigu coset from eqn ①

Now we also know $e \in H$

and we can also say that $e \in He$

$\therefore He = \underline{H}$ — ②

i.e rigu coset generated by identity e

We have two rigu cosets Now

① He ② $(Hx)(Hx^{-1})$

These rigu cosets can be identical or distinct

but $e \in He$ & $e \in (Hx)(Hx^{-1})$

these rigu cosets are identical.

$(Hx)(Hx^{-1}) = H$ — ③

Let $h, h' \in H$

$(hx)(h'x^{-1}) \in (Hx)(Hx^{-1})$

$\therefore$ from eqn (3)

$(hx)(h'x^{-1}) \in H$ — (4)

multiply by h^{-1} both sides:

$h^{-1}(hx)(h'x^{-1}) \in h^{-1}H$

e

$xh'x^{-1} \in H$

$\because hH = H$ (proved already)

$\therefore xh'x^{-1} \in H$

This is the normality condn ie.

If $xh'x^{-1} \in H \Rightarrow H$ is a normal subgroup

Quotient group / Factor group

Group → subgroup → cosets → Normal subgroup

↓

quotient group

- Quotient group - collection of all cosets H in G where H is normal subgroup
- collection of all cosets of normal subgroup

It is denoted by G/N where N is normal subgroup

G/H " H " "

$G/H = \{Ha \mid a \in G\}$

Here we are taking only right coset of H

is a normal subgroup & $Ha = aH$

Why it is called as group?
- As all cosets collectively forms a group.

- Properties of quotient group

① If G is Abelian then G/H is also abelian.
let $a, b \in G$

$Ha, Hb \in G/H$
Take operation on $Ha * Hb$

$$(Ha)(Hb) = Hab \quad -①$$
- Right cosets operated to get right

$$(Ha)(Hb) = Hba$$
$\because ab = ba$ as group is abel

$\Rightarrow (Ha)(Hb) = (Hb)(Ha)$
$\Rightarrow$ cosets are also ~~Abelian~~ commutative
$\therefore$ quotient group is commutative
$\rightarrow$ It is Abelian group

* Note that here we are considering cosets as element of quotient group

② If G is cyclic, G/H also cyclic

$\Rightarrow$ $G = \langle a \rangle$ with 'a' as generator
so all elements of G are generated by a^n

$\therefore a^n \in G$

Derive a coset from $a^n \Rightarrow Ha^n$

$\Rightarrow H(a \cdot a \cdot a \cdots a)$

$\Rightarrow Ha\,Ha\,Ha \cdots Ha$

$(\because HaHb = Hab)$

$\Rightarrow (Ha)^n$

$Ha^n = (Ha)^n$

That mean if I take any element of G/H, it can be represented as $(Ha)^n$

$\Rightarrow$ cyclic group with generator Ha

$G/H = \langle Ha \rangle$

③ Let $a \in G$, & $O(a) = n$

$Ha \in G$ & $O(Ha) = m$

Then m divides n.

$\Rightarrow$ Let $a^n = e$ ($\because$ defn of order)

$Ha^n = H(a \cdot a \cdot a \cdots a)$

$= Ha\,Ha\,Ha \cdots Ha$

$Ha^n = (Ha)^n$

but $a^n = e$

$\Rightarrow He = (Ha)^n$

$\Rightarrow H = (Ha)^n$

$\Rightarrow (Ha)^n = H$ which is identity of G/H

we already proved $a^n = e$ & $O(a) = m$

then m divides n

$\Rightarrow m \mid n$

Q Find quotient group G/H when
$G = (\{1, -1, i, -i\}, \times)$ & $H = (\{1, -1\}, \times)$

⇒
Here G is a commutative group, so every subgroup of G is a normal subgroup.
Consiqeently G/H exists & having following cosets

$H \times 1 = \{1 \times 1, -1 \times 1\} = \{1, -1\} = H$
$H \times -1 = \{-1 \times 1, -1 \times -1\} = \{1, -1\} = H$
$H \times i = \{i, -i\} = i \cdot H$
$H \times -i = \{-i, i\} = iH$

$\therefore G/H = \{H, iH\}$

Composition table of G/H is

	H	Hi
H	H	Hi
Hi	Hi	H

✓

Q2 Find the quotient group G/H when
$G = (Z, +)$, $H = (4Z, +)$

→ $(4Z, +) \trianglelefteq Z$ ∴ G/Z exists
The cosets of H in G as follows

$0 + H = H + 0 = \{-\infty \cdots -8, -4, 0, 4, 8 \cdots\}$
$1 + H = H + 1 = \{-\infty \cdots -7, -3, 1, 5, 9 \cdots\}$
$2 + H = H + 2 = \{-\infty \cdots -6, -2, 2, 6, 10 \cdots\}$
$3 + H = H + 3 = \{-\infty \cdots -5, -1, 3, 7, 11 \cdots\}$

Further

$H = H+4 = H+8 \cdots = H+(-4) = H+(-8) \cdots$

$H+1 = H+5 = H+9 \cdots = H+(-3) = H+(-7) \cdots$

$H+2 = H+6 = H+10 \cdots = H+(-2) = H+(-6) \cdots$

$H+3 = H+7 = H+11 = \cdots = H+(-1) = H+(-5) \cdots$

Thus the distinct cosets are

$G/H = \{H, H+1, H+2, H+3\}$

Composition table

+	H	H+1	H+2	H+3
H	H	H+1	H+2	H+3
H+1	H+1	H+2	H+3	H
H+2	H+2	H+3	H	H+1
H+3	H+3	H	H+1	H+2

Identity = H

Inverse of $H = H$, $H+1 \Rightarrow H+3$

$H+2 \Rightarrow H+2$

$H+3 \Rightarrow H+1$

Permutation group

- **Functions** :: A function or mapping, defined as $(f : X \to Y)$ is a relationship from elements of one set X to elements of another set Y. (X and Y are non empty sets)

  X → Domain / pre-image
  Y → codomain / image

A function 'f' is a relation on X and Y such that for each $x \in X$, there exists a unique $y \in Y$ such that $(x, y) \in R$.

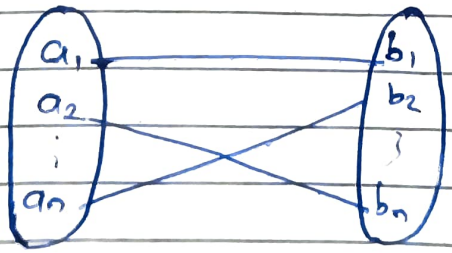
* A function can be one-to-one, or many-to-one but not one to many

① Injective / one-to-one

- A function is said to injective or one-to-one function for every element in codomain there exists atmost one element in domain.

$f : A \to B \quad \forall\, b \in B$, atmost one $a \in A$

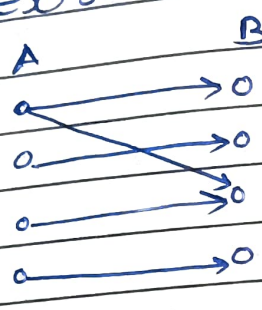
i.e. if $a_1 \neq a_2$ implies $f(a_1) \neq f(a_2)$



one-to-one

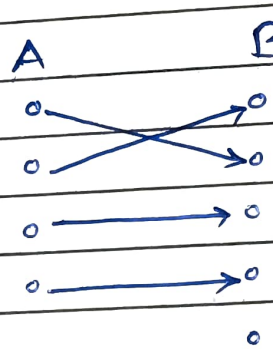
② Surjective / on-to

A function $f: A \to B$ is surjective (onto) if for every $b \in B$, there exists some $a \in A$, such that $f(a) = b$. This means for any y in B, there exists some x in A, $y = f(x)$.

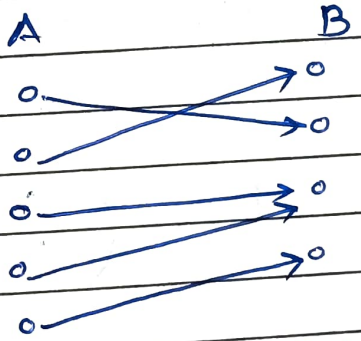


Not a function
(one-to-many)
A has many B

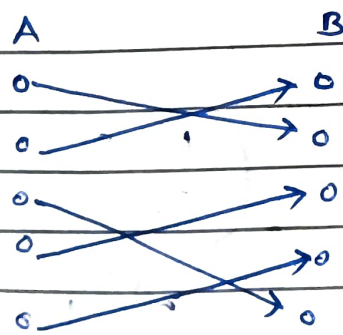
General function
B has many A



Injective (Not surjective)
B can't have many A



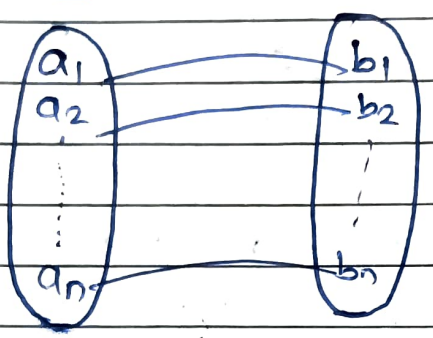
Surjective (Not Injective)
Every B has some A.



Bijective
(Injective & surjective)
A to B perfectly.

Suppose 'S' is a finite set having 'n' distinct elements. The one-one mapping of 'S' onto itself is called permutation of degree 'n'

$f : S \to S$ with one-to-one mapping & onto.



Such function with number of elements is called as permutation with degree 'n'.

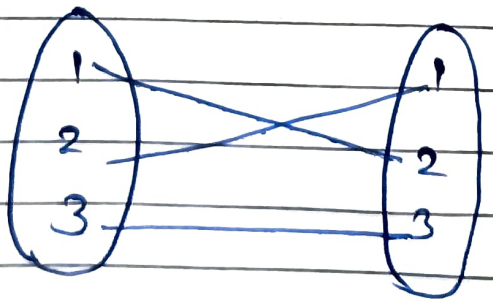
The other way of representing permutation is as follows

$$f = \begin{pmatrix} a_1 & a_2 & a_3 & \cdots & a_n \\ b_1 & b_2 & b_3 & \cdots & b_n \end{pmatrix}$$

a_1 image is b_1

a_2 " " b_2

eg



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

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

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

- **Equality of two permutations**

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

$f = g$ if $f(a) = g(a)$ $\forall a \in S$

Product or composition of two permutations

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

1) $fog = f(g(x))$

$f(1) = 2$	$g(1) = 4$
$f(2) = 3$	$g(2) = 3$
$f(3) = 4$	$g(3) = 2$
$f(4) = 1$	$g(4) = 1$

① $fog(1) = f(g(1)) = f(4) = 1$

$fog(2) = f(g(2)) = f(3) = 4$

$= f(g(3)) = f(2) = 3$

$f(g(4)) = f(1) = 2$

② $gof \Rightarrow g(f(1)) = g(2) = 3$

$g(f(2)) = g(3) = 2$

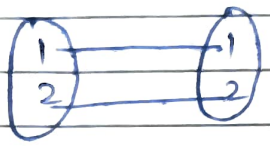
$g(f(3)) = g(4) = 1$

$g(f(4)) = g(1) = 4$

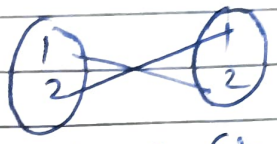
$fog \neq gof \Rightarrow$ Some cases it may be in general it is not commutative

- Let $S = \{1, 2\}$ $\quad f: S \to S$

How many possible permutations (one-one ...



Identity mapping (I)
1-1, 2-2



1 - 2 (f_1)
2 - 1

If $n = 2$ then 2 permutations are possible

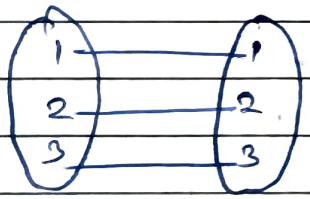
This is denoted by S_2

$S_2 = \{f : f$ is permutation of degree 2$\}$

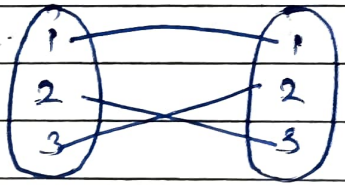
$S_2 = \{I, f_1\}$

- Let $S = \{1, 2, 3\}$ $\quad f: S \to S$

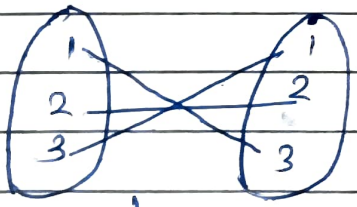
How many possible permutations?



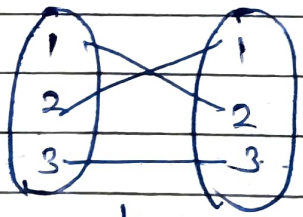
Identity (I)



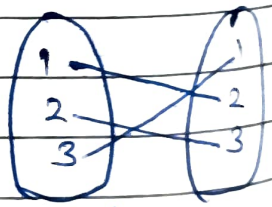
f_1



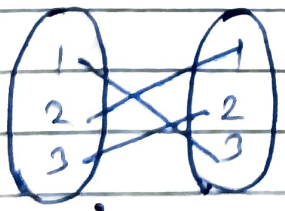
f_2



f_3



f_4



f_5

No other possibilities

This is denoted by S_3

$S_3 = \{f : f$ is a permutation of

order(S_3) = 6

- similarly $O(S_n) = n!$
  $\therefore O(S_4) = 4 \times 3 \times 2 \times 1 = 24$

Symmetric group

$S_n = \{\sigma : \sigma \text{ is permutation of degree } n\}$

Binary operation ($\bullet$) composition of permutation

$(S_n, \bullet) \Rightarrow$ is a group.

① closure property - composition of two permutation is also permutation.

let $\sigma, g \in S_n \rightarrow \sigma \circ g \in S_n$

$\because g \in S_n$ & $\sigma \in S_n$

$\downarrow$ $\sigma \circ g \in S_n$

②

Associative property

$\forall\ \sigma, g, h \in S_n$

$(\sigma \circ g) \circ h = \sigma \circ (g \circ h)$

③ Identity :- $\forall \sigma \in S_n$ $I \in S_n$ such that

$\sigma \circ I = I \circ \sigma = \sigma$

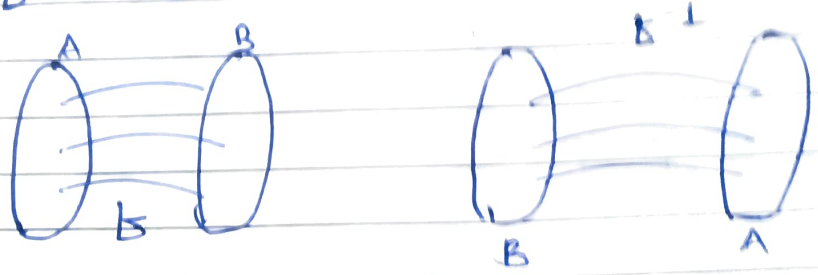
eg $\sigma = \begin{pmatrix} a_1 & a_2 & a_3 & \cdots & a_n \\ b_1 & b_2 & b_3 & \cdots & b_n \end{pmatrix}$

$I = \begin{pmatrix} a_1 & a_2 & a_3 & \cdots & a_n \\ a_1 & a_2 & a_3 & \cdots & b_n \end{pmatrix}$

$\sigma \circ I = \begin{pmatrix} a_1 & a_2 & a_3 & \cdots & a_n \\ b_1 & b_2 & b_3 & & b_n \end{pmatrix} = \sigma$

④ Inverse — Here inverse of a function calculated by changing domain & codomain

$f : A \to B \Rightarrow f^{-1} : B \to A$



As function is one to one & onto the inverse exists

$$f = \begin{pmatrix} a_1 & a_2 & a_3 & \cdots & a_n \\ b_1 & b_2 & b_3 & & b_n \end{pmatrix}$$

$$f^{-1} = \begin{pmatrix} b_1 & b_2 & b_3 & \cdots & b_n \\ a_1 & a_2 & a_3 & & a_n \end{pmatrix}$$

$$f^{-1} \circ f = \begin{pmatrix} a_1 & a_2 & a_3 & \cdots & a_n \\ a_1 & a_2 & a_3 & \cdots & a_n \end{pmatrix} = I$$

⑤ commutative — Not satisfied.

$$fog \neq gof$$

- cyclic permutation:

permutation group can be represented as below

Eg

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 1 & 3 & 5 & 6 \end{pmatrix}$$

(1 2 3 4) (

(1 2 4 3) (5) (6) $\Rightarrow$ (1 2 4 3)

we can get back to complete permutation

as follows

Permutation group of order 6 & cyclic permutation (1243) = ?

$$b = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 1 & 3 & 5 & 6 \end{pmatrix}$$

Now lets focus on S_3

$$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}$$

$S_3 = \{ I, (23), (13), (12), (123), (132) \}$

Reduced form.

$S_3 = \{ I, (12), (13), (23), (123), (132) \}$

Now lets check if S_3 satisfies closure property

① Closure

$(12) \circ (13) = ?$

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

$= (132) \in S_3$

$(13)(23) = (321)$

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

$= I$

② Associative property - satisfied

④ Inverse

$(12)(12) \Rightarrow (1)(2)(3) = I$

inverse of (12) is (12)

$(13)(13) \Rightarrow (1)(3)(2) = I$

in general $(ab)^{-1} = (ba)$

$(abc)^{-1} = (aba)$

Note that $abc = bca = cab$

cycles are same

$(13) = (31)$ & $(12) = (21)$

$abc \neq bac$

What is the difference between permutation & symmetric group?

– symmetric group is set of all permutations of degree n

eg $S_3 = \{I, (13), (12)(23), (123)(132)\}$

Permutation group is a subgroup of symmetric group

eg $H = \{I, (132), (123)\}$ is a permutation group which is subgroup of symmetric group S_3

But H is not a symmetric group

• caley graph / table

S_3 = { I , (12), (13), (23), (123), (132) }

	I	(12)	(13)	(23)	(123)	(132)
I	I	(12)	(13)	(23)	(123)	(132)
(12)	(12)	I	(132)	(123)	(23)	(13)
(13)	(13)	(123)	I	(132)	(12)	(23)
(23)	(23)	(132)	(123)	I	(13)	(12)
(123)	(123)	(13)	(23)	(12)	(132)	I
(132)	(132)	(23)	(12)	(13)	I	(123)

(12)(12) ⇒ (11)(22)(33) ⇒ (1)(2)(3) = I

(12)(13) ⇒ (132)

(12)(23) ⇒ (231)

(12)(123) ⇒ (1)(23)

(12)(132) ⇒ (31) = (13)

(13)(12) ⇒ (123)

(13)(13) ⇒ (1)(3)(2) ⇒ I

(13)(23) ⇒ (213) ⇒ (132)

caley table

As this group is not symmetric → this is non abelian group

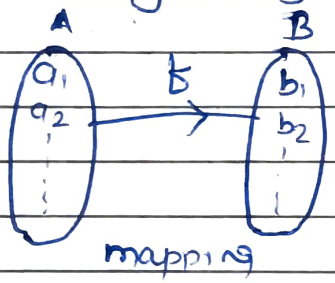
Homomorphism of group

Homo — same — same Algebric structure (Group)

morphism — mapping — mapping between two groups. mapping which preserve structure

- Mapping between two algebric structure which preserves property of algebraic structure

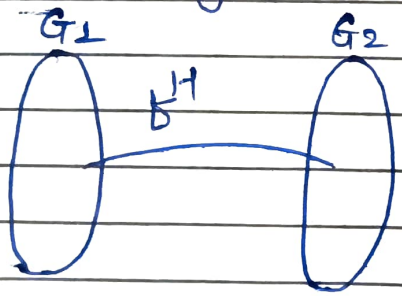
Mapping is generally defined by a function



$f(a_1) = b_1$

$f(a_2) = b_2$

same thing will follow in groups.



G_1 & G_2 are two groups on which we have defined a homomorphism mapping f^H

Defination :- Let G_1 & G_2 be two groups with some binary operations o & $*$ respectively then

$f: G_1 \to G_2$ defined by

$f(a \circ b) = f(a) * f(b)$ $\forall$ $a, b \in G_1$

Then 'f' is called as homomorphism.

G_1 $\quad$ G_2 $\quad$ G_1

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

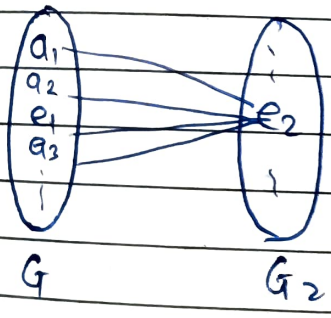
b $\quad$ $\rightarrow$ $\quad$ $f(b)$ $\quad$ $\uparrow\ \uparrow \quad \uparrow\ \uparrow \quad \uparrow$

e $\quad$ $\quad$ $f(e)$ $\quad$ $G_1\ G_1 \quad G_2\ G_2\ G_2$

d

:

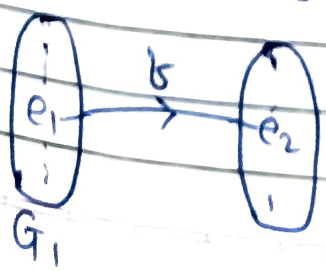
- If a homomorphism is one-to-one then we call it as monomorphism
- If a homomorphism is onto then we call it as epimorphism
- If all elements of G_1 are mapped to identity of G_2 then we call it as trivial homomorphism



- If a homomorphism is both one-to-one & onto we call it as isomorphism.

Theorems on Homomorphism

① If $f: G_1 \rightarrow G_2$ & f is homomorphism then $f(e_1) = e_2$ where e_1 is identity of G_1 & e_2 is identity of G_2



$f(e_1) = e_2$

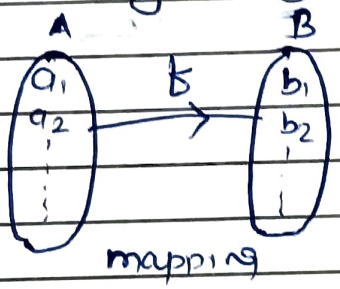
Homomorphism of group

Homo → same → same Algebric structure (Group)

morphism → mapping → mapping between two groups. → mapping which preserve structure

- Mapping between two algebric structure which preserves property of algebraic structure

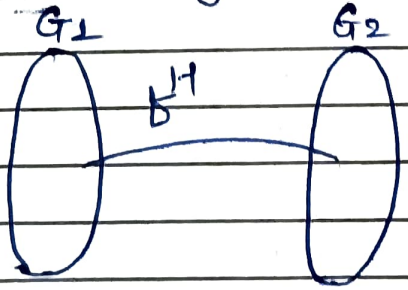
mapping is generally defined by a function



$f(a_1) = b_1$

$f(a_2) = b_2$

same thing will follow in groups.



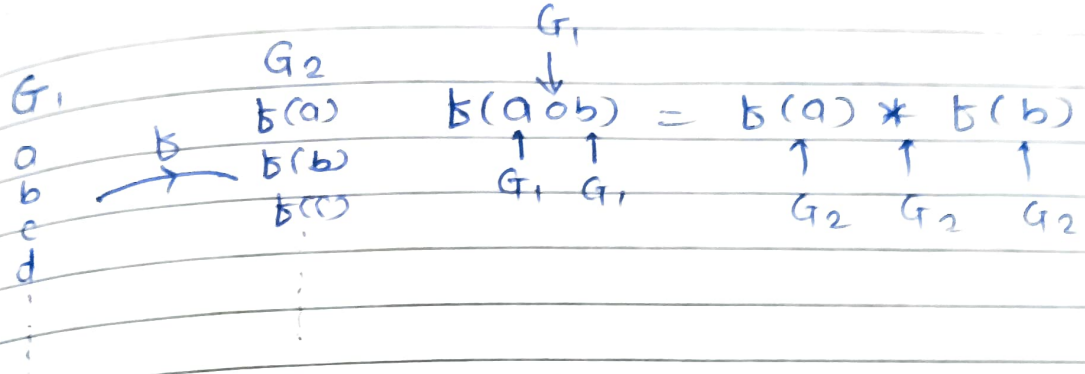
G_1 & G_2 are two groups on which we have defined a homomorphism mapping f^H

Defination :- Let G_1 & G_2 be two groups with some binary operations o & $*$ respectively then

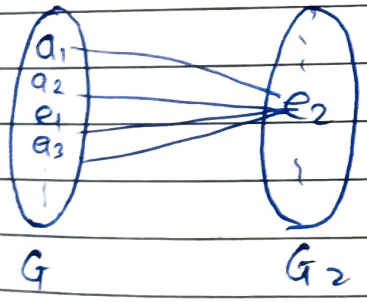
$f: G_1 \to G_2$ defined by

$f(a \, o \, b) = f(a) * f(b) \quad \forall \; a, b \in G_1$

Then 'f' is called as homomorphism.



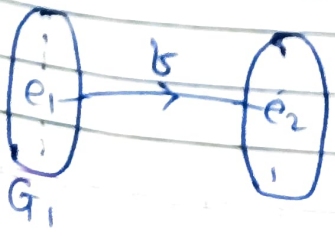
- If a homomorphism is one-to-one then we call it as monomorphism
- If a homomorphism is onto the we call it as epimorphism
- If all elements of G_1 are mapped to identity of G_2 then we call it as trivial homomorphism



- If a homomorphism is both one-to-one & onto we call it as isomorphism.

Theorems on Homomorphism

1. If $f: G_1 \to G_2$ & f is homomorphism then $f(e_1) = e_2$ where e_1 is identity of G_1 & e_2 is identity of G_2



$f(e_1) = e_2$

Identity of G_1 always gets mapped to identity of G_2

Proof :- Let $a \in G_1 \rightarrow f(a) \in G_2$

$$f(a) = f(a) \cdot e_2 \quad -①$$

by multiplying identity of G_2

$$f(a) = f(a \cdot e_1) \quad -②$$

e_1 is identity of G_1 :- $a \cdot e_1 = a$

We know defn of homomorphism

$$f(a \cdot e_1) = f(a) \cdot f(e_1) \quad -③$$

From eqn ① & ③

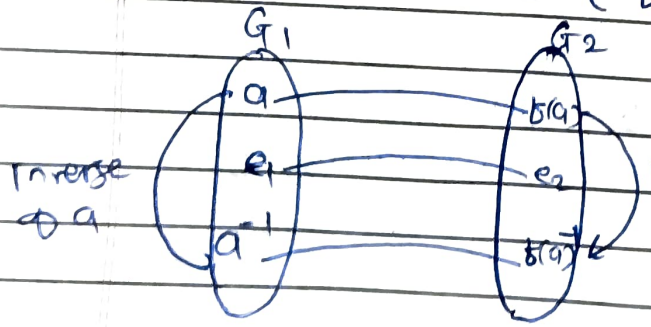
$$f(a) \cdot e_2 = f(a) \cdot f(e_1)$$

By left cancellation rule

$$f(e_1) = e_2$$ Hence proved.

② If $f : G_1 \rightarrow G_2$ & f is homomorphism then

$$f(a^{-1}) = [f(a)]^{-1}$$



We have to prove

$$[f(a)]^{-1} = f(a^{-1}) \quad \text{— (A)}$$

To show this we can prove

$$f(a) \cdot f(a^{-1}) = e_2$$

↑ identity of G_2

From previous proof we know that

$$e_2 = f(e_1)$$

Let $a \in G$

$$\therefore e_2 = f(a \cdot a^{-1})$$

By def of homomorphism

$$f(a \cdot a^{-1}) = f(a) \cdot f(a^{-1}) = e_2$$

$\therefore$ If $f(a) \cdot f(a^{-1}) = e_2$

This implies inverse of $f(a)$ is $f(a^{-1})$

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

③ $O(f(a))$ divides $O(a)$

order of $f(a)$ divides order of (a)

$\Rightarrow$ $O(f(a)) = m$ $\quad O(a) = n$

$\Rightarrow$ m divides n

→ $a^n = e_1$ – given

$f(a^n) = f(e_1)$

$\Rightarrow f(a \cdot a \cdot a \cdots a) \Rightarrow f(a) \cdot f(a) \cdot f(a) \cdots f(a)$

$\Rightarrow [f(a)]^n = f(e_1)$

$f(e_1) = e_2$ → from previous theorem

$\therefore e_2 = (f(a))^n$ → ①

but order of $f(a)$ is m

we already know from group m divides n

Example

Let $(R, +)$ be the additive group of real numbers and $(R_0, \times)$ be the multiplicative group of non zero real numbers.

mapping $f: (R, +) \to (R_0, \times)$; $f(x) = 2^x \; \forall x \in R$ is a homomorphism of R into R_0 because for any $x_1, x_2 \in R$

$$f(x_1 + x_2) = 2^{x_1 + x_2} = 2^{x_1} \times 2^{x_2}$$
$$= f(x_1) \times f(x_2)$$

Eg2 Let $G = \{1, -1\}$ be a multiplicative group Then map

$$f: (Z, +) \to (G, \times) : f(x) = \begin{cases} 1 & \text{if } x \text{ is even} \\ -1 & \text{if } x \text{ is odd} \end{cases}$$

is an epimorphism from Z to G, because for any $x_1, x_2 \in Z$

i) When x_1, x_2 both are even then,

$$f(x_1 + x_2) = 1 = 1 \cdot 1 = f(x_1) \cdot f(x_2)$$

ii) When x_1, x_2 both are odd

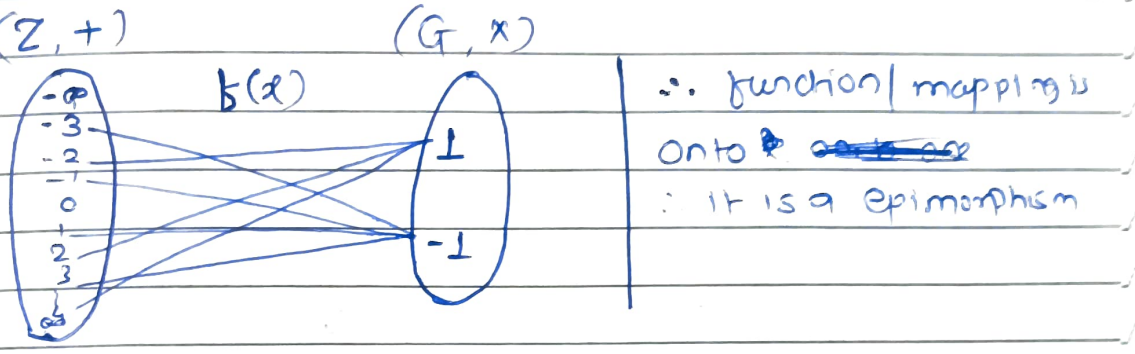
$$f(x_1 + x_2) = +1 = -1 \cdot -1 = f(x_1) \cdot f(x_2)$$

iii) When x_1 is even & x_2 is odd

$f(x_1+x_2) = -1 = +1 \cdot -1 = f(x_1) \cdot f(x_2)$

iv) When x_1 is even x_2 is odd

$f(x_1+x_2) = -1 = +1 \cdot -1 = f(x_1) \cdot f(x_2)$



∴ function/mapping is onto

∴ it is a epimorphism

* The map $f: (Z, +) \to (2Z, +)$; $f(x) = 2x \ \forall x \in Z$ is isomorphism

→ ① $f(x_1+x_2) = 2(x_1+x_2) = 2x_1 + 2x_2$

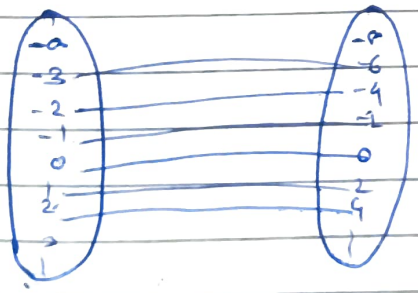
$= f(x_1) + f(x_2)$

∴ it is a homomorphism

If

② $f(x_1) = f(x_2) = 2x_1 + 2x_2 \Rightarrow x_1 = x_2$

If $f(x_1) = f(x_2) \to x_1 = x_2$ then this is a one-to-one mapping



one to one

③ $f(x)$ is onto $f(Z) = 2Z$

$\therefore H \cong 1 \quad Z \cong 2Z$

∴ Z is isomorphic to 2Z

Rings & Fields

① A ring R denoted by $\{R, +, *\}$ is set of elements with two binary operation called addition & multiplication, such that for all $a, b, c \in R$, the following axioms are obeyed

1) Group - G_1 to G_4 (For addition)
2) Abelian group - A_5 (For addition)
3) Associativity - M_2 (For multiplication)
4) Closure - M_1 (For multiplication)
5) Distributive - M_3 - for multiplication

$$a(b+c) = ab + ac$$
$$(a+b)c = ac + bc$$

② Commutative Ring :- A ring is said to be commutative, if it satisfies additional cond? commutative under multiplication.

$$ab = ba$$

③ Integral domain :- An integral domain is a commutative ring that obey,

① multiplicative identity (M_5)

$$a \cdot e = e \cdot a = a$$

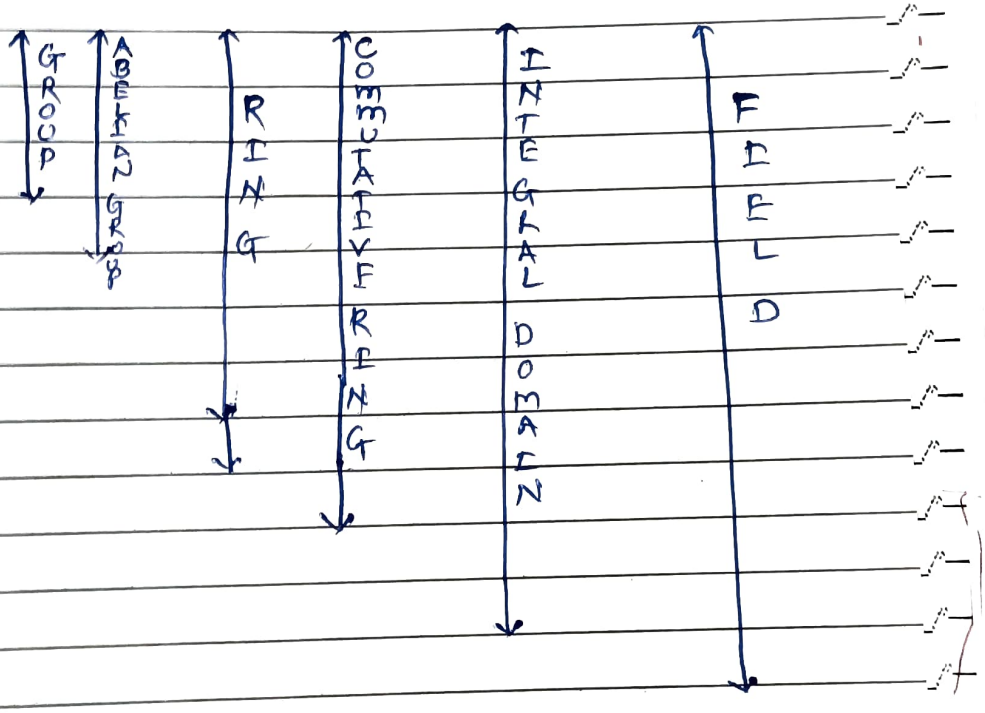
② No zero divisors :-

If $ab = 0$, then either $a = 0$ or $b = 0$

④ Fields :- A field F, sometimes denoted by $\{F, +, *\}$ is a set of elements with two binary operation called addition & multiplication, s.t. for $a, b \in F$ following axioms are obeyed

1) A_1 to A_5 - commutative group under +
2) M_1 to M_6 - for multiplication
3) M_7 - multiplicative inverse exists.

A_1: closure
A_2: Associative
A_3: Identity
A_4: Inverse
A_5: commutative
M_1: closure
M_2: Associative
M_3: Distributive
M_4: commutative
M_5: Identity
M_6: No zero divisors
M_7: Inverse



(5) Finite Fields :- A Field with finite number of elements is called finite field.

- eg set of all $n \times n$ matrices form a ring with identity but it is not a commutative ring

Q.2 Prove that the set $\{0, 1, 2, 3, 4, 5\}$ is a ring with $+_6$ & $\times_6$