Symmetric difference group :

Let X be a non-empty set and $P(X)$ be the set of all subset of X.

On $P(X)$. Define Δ operations

$$A \Delta B = (A \cup B) \setminus (A \cap B)$$

Then $P(X)$ is a group under Δ.

Here ϕ is behave as identity

Proof :

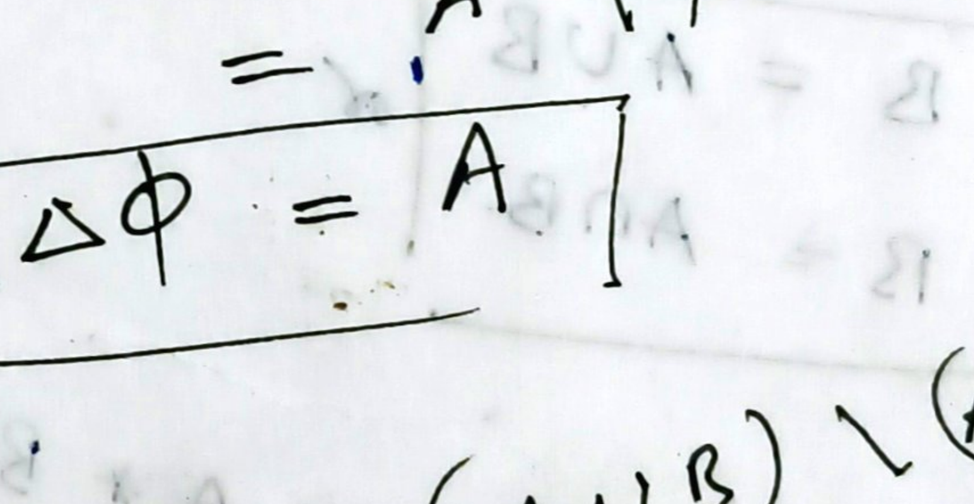
$$A \Delta \phi = (A \cup \phi) \setminus (A \cap \phi)$$

$$= A \setminus \phi$$

$$\boxed{A \Delta \phi = A}$$

$$\textcircled{*} \quad (A \Delta B) \Delta C = (A \cup B) \setminus (A \cap B)$$

$\Rightarrow$



* $A \Delta B = B \Delta A$

Proof:- $A \Delta B = (A \cup B) \cap (A^c \cup B^c)$

$= (B \cup A) \cap (B^c \cup A^c)$

$\boxed{A \Delta B = B \Delta A}$

(*) Let X be a non-empty set and $P(X)$ be the set of all subsets of X.

On $P(X)$, define operation (*)

$$\boxed{\begin{aligned} A * B &= A \cup B \\ A * B &= A \cap B \end{aligned}} \text{ or}$$

$\Rightarrow A * B = A \cup B$ or $A * B = A \cap B$

Take $A = B$:

$A * A = A \cup A = A$

$A * A = A \cap A = A$.

But in group, the only idempotent element is identity. (identity)

i.e there are no unique identity element

$\therefore \not\Rightarrow (P(X), *)$ is not a group.

Note: The only idempotent element in a group is its identity elements.

Proof:-

Q. find the number of non-zero elements in the field $\mathbb{Z}_p$, where p is an odd prime number which are squares, i.e of the form m^2, $m \in \mathbb{Z}_p$, $m \neq 0$.

Soln: Let $\mathbb{Z}_p^*$ denote the set of non-zero elements of $\mathbb{Z}_p$.

$$f : (\mathbb{Z}_p^*)^2 \longrightarrow (\mathbb{Z}_p^*)^2$$

$$\mathbb{Z}_p^* = \{1, 2, 3, \ldots, p-1\}.$$

$$(\mathbb{Z}_p^*)^2 = \{x^2 \mid x \in \mathbb{Z}_p^*\}.$$

let $f : \mathbb{Z}_p^* \longrightarrow (\mathbb{Z}_p^*)^2$ defined by $f(x) = x^2$ then f is surjective homomorphism.

Take $x, y \in Z_p^*$

Then $f(xy) = (xy)^2 = (xy)(xy)$

$= x \cdot x\, yy$

$= x^2 y^2$

$$\boxed{f(xy) = f(x) f(y)}$$

f is ~~a~~ homomorphism

f is onto because

$$(Z_p^*)^2 = \{x^2 \mid x \in Z_p^*\}.$$

Take $Z_5^* = \{1, 2, 3, 4\}$

$(Z_5^*)^2 = \{1^2, 2^2, 3^2, 4^2) \mid x \in Z_5^*\}$

$= \{1, 4, 4, 1) \mid x \in Z_5^*\}.$

$$(Z_5^*)^2 = \{1, 4\}.$$

~~$f : Z_p^*$~~

$f : Z_5^* \longrightarrow (Z_5^*)^2$ is surjective homomorphism.

Now by using first theorem of isomorphism,

$(Z_5^*)^2$ is isomorphic to $\frac{Z_5^*}{\ker f}$.

i/e $(Z_p^*)^2$ is isomorphic to $\frac{Z_p^*}{\ker f}$

$\ker f = \{x \mid x^2 = 1\}$.

$= \{-1, 1\}$

$|\ker f| = 2$

Therefore $|(Z_p^*)^2| = \frac{p-1}{2}$

Q. Let H and K be subgroup of G of order 3 and 5 respectively. Then $H \cap K = \{e\}$, where e is the identity element of G.

Proof:

Since $\gcd(3,5) = 1$.

By Bezout's theorem, we can write

$1 = 3x + 5y$ for some integer x and y

Let $g \in H \cap K$, then

$g = g^1 = g^{3x+5y}$

$= g^{3x} \cdot g^{5y}$

$= (g^3)^x (g^5)^y$.

$= e \cdot e \cdot$

Since $g^3 = e = g^5$. i.e $g \in H$

$g \in K$.

$\boxed{g = e} \Rightarrow \boxed{H \cap K = \{e\}}$

Q. If G is an abelian group of odd order, then $\phi(x) = x^2$ is an automorphism of G.

Sol:

$$\phi(xy) = \phi(x)\,\phi(y)$$

$$(xy)^2 = x^2 \cdot y^2$$

Since G is abelian:

$\Rightarrow \phi$ is homomorphism.

To show ϕ is injective:-

Since G is an abelian group of odd order

i.e $|G| = 2n-1$.

Suppose $x^2 = y^2$

Then, $x = x \cdot x^{2n-1}$

$= (x^2)^n$

$= (y^2)^n = y \cdot y^{2n-2}$.

$= y$.

$\Rightarrow$ i.e $\boxed{x = y}$

$$\phi(x) = \phi(y)$$

$$\Rightarrow x^2 = y^2$$

$$\Rightarrow x = y$$

Therefore ϕ is injective.

To show ϕ is surjective :-

$|G| = 2n-1$. . let $g \in G$.

$$\Rightarrow g^k \in G.$$

$$\phi : G \longrightarrow G.$$

$$\phi(g^k) = (g^k)^2$$

$$= g^{2k}$$

$$= g\,(g^{2k-1})$$

$$\boxed{\phi(g^k) = g}$$

Therefore ϕ is onto

Hence $\phi(x) = x^2$ is automorphism

If G is an abelian group of even order, then $\phi(x) = x^2$ is not an automorphism.

Soln:

Let $x \in G$. $\Rightarrow x^n \in G$.

$$\text{order}(x) = 2n > 0.$$

$$x^{2n} = 1.$$

$$\Rightarrow x^n \neq 1.$$

~~$f(x) =$~~

$$f(x^n) = (x^n)^2$$

$$= (x^n)^2$$

$$= x^{2n}$$

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

Similarly $f(y^n) = 1$

but $x^n \neq y^n$.

ϕ is not injective.

$\Rightarrow$ ϕ is not an automorphism.

Theorem :- If G has exactly one-element of order 2, then this element belongs to the Centre of G.

Soln: Take an element $x \in G$.

$$x = a^{-1} b a \quad \text{where } b \in G,$$

and b has order 2.

$$x^2 = (a^{-1} b a)^2$$

$$x^2 = (a^{-1} b a)(a^{-1} b a)$$

$$x^2 = e = a^{-1} b b a$$

$$= a^{-1} a$$

$$\boxed{x^2 = e}$$

Also, $b^2 = e$

$$\Rightarrow x^2 = b^2 = e$$

$$\Rightarrow \boxed{x = b}$$

$$a^{-1}ba = x = b$$

$$a^{-1}ba = b$$

$$\boxed{ba = ab}$$

Thus implies $b \in Z(G)$

b is in the centre of G.

Note : Number of group homomorphism from

$$Z_n \text{ to } Z_m = \gcd(n, m)$$

(#) find a generator of F_7^*, the multiplicative group of non-zero elements of F_7.

Sol: 3 or 5

$$\langle 3 \rangle = \{3, 3^2, 3^3, 3^4, 3^5, 3^6\}$$

$$= \{3, 2, 6, 4, 5, 1\}$$

$$\langle 5 \rangle = \{5, 5^2, 5^3, 5^4, 5^5, 5^6\}$$

$$= \{5, 4, 6, 2, 3, 1\}$$

(#) The highest power of a prime p dividing $n!$ is given by

$$\left[\frac{n!}{p}\right] + \left[\frac{n!}{p^2}\right] + \left[\frac{n!}{p^3}\right] + \cdots$$

(#) Number of trailing zeroes in $n!$

= highest power of 5 in $n!$

~~Example~~

Example : 61 !!

$$\left\lfloor \frac{61}{5} \right\rfloor + \left\lfloor \frac{61}{5^2} \right\rfloor = 12 + 2 = 14$$

i,e there 14 zero's at the end of 61!.

Q. Let H be the subgroup generated by (12) in S_3. Compute the normalizer, $N(H)$, of H.

Sol. The normalizer $N(H)$ of a subgroup H of a group G can be defined to be the

Set $N(H) = \{ g \in G \mid gHg^{-1} = H \}$

$gH = Hg$.

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

Here $H = \langle (12) \rangle = \{ I, (12) \}$,

$N\langle (12) \rangle$?

$\Rightarrow I(12) = (12)$

$(12)(12) = (12)(12)$

$(12)(23) \neq (23)(12)$

$(12)(13) \neq (13)(12)$

$(12)(123) \neq (123)(12)$

$(12)(132) \neq (132)(12)$

Therefore $N(H) = H$

$N\{\langle (12) \rangle\} = \{ I, (12) \}$

$= \{ I, (12) \}. \quad \langle (12) \rangle$

Q

Number of distinct r-cycle in S_n

$$= \frac{n!}{r(n-r)!}$$

Find the number of conjugates of a r-cycle

$$\sigma = (123\ldots r) \in S_n$$

Soln The conjugate class of σ is

$$C(\sigma) = \{\theta\sigma\theta^{-1} : \theta \in S_n\}$$

$$= \{\theta(123\ldots r)\theta^{-1} : \theta \in S_n\}$$

$$= \{(\theta(1)\theta(2)\ldots\theta(r) : \theta \in S_n\}.$$

Thus $C(\sigma)$ consist of all distinct r-cycles in S_n

$$\therefore |C(\sigma)| = \frac{n!}{r(n-r)!}$$

$\Rightarrow$ The number of conjugates of the

n-cycle $(1\,2\,3 \ldots, n)$ in S_n

$= (n-1)!$

$$\therefore o[C(\sigma)] = \frac{n!}{n(n-n)!}$$

$$= \frac{n(n-1)!}{n}$$

$$\boxed{\therefore o[C(\sigma)] = (n-1)!}$$

Note :- For each cycle $(i_1\, i_2, \ldots\, i_k)$ in S_n

and each $\sigma \in S_n$

$$\boxed{\sigma(i_1\, i_2 \cdots i_k)\sigma^{-1} = (\sigma(i_1)\,\sigma(i_2) \cdots \sigma(i_k))}$$

Example:- S_5, take $\sigma = (13)\cdot(254)$.

$(i_1, i_2, i_3, i_4) = (1\,4\,3\,2)$

$\sigma(1432)\sigma^{-1} = (13)(254)(1432)(245)(13)$

$= (1\,5\,3\,2)$

whole $(\sigma(1)\ \sigma(4)\ \sigma(3)\ \sigma(2))$

$= (3215)$

Since $\sigma(1) = 3$, $\sigma(4) = 2$, $\sigma(3) = 1$

and $\sigma(2) = 5$

clearly $(1532) = (3215)$

$(1532) = (3215)$

Therefore,

$$\sigma(1432)\,\sigma^{-1} = (\sigma(1), \sigma(4), \sigma(3), \sigma(2))$$

Q. $\mathbb{R}^\times = \mathbb{R} - \{0\}$ = multiplicative group of real number

$\mathbb{C}^\times = \mathbb{R} - \{0\}$ = Multiplicative group of Complex number.

Q. $\mathbb{R}^\times$ and $\mathbb{C}^\times$ are not isomorphics.

proof:- Suppose there is a group isomorphism

$$\therefore \phi : \mathbb{C}^\times \longrightarrow \mathbb{R}^\times$$

Since ϕ is a group homomorphism

$$\phi(1) = 1$$

$$\phi(1) = \phi((-1)(-1))$$

$$= \phi(-1)\,\phi(-1)$$

$$= \phi(-1)^2 = 1.$$

$$\phi(-1)^2 = 1$$

$$\phi(-1) = \pm 1.$$

Since ϕ is injective so $\phi(-1) = -1$

$$\phi(1) = 1.$$

Now we have

~~$\phi(-1) =$~~

Since $i \in \mathbb{C}^\times$ and $\phi : \mathbb{C}^\times \longrightarrow \mathbb{R}^\times$

& ~~$\phi : \mathbb{C}^\times$~~ $i^2 \in \mathbb{C}^\times$

$$\phi(i^2) = \phi(-1) = -1.$$

$$\phi(i \cdot i) = \phi(i) \cdot \phi(i) = -1$$

$$\Rightarrow \phi(i)^2 = -1.$$

$$\Rightarrow \phi(i) = \sqrt{-1}$$

$$\phi(i) = i$$

Since Co-domain is $\mathbb{R}^\times$ so $\phi(i) \in \mathbb{R}^\times$

$\Rightarrow \phi(i)^2$ must be +ve number

But $\phi(i)^2 = -1$, this lead to the

Contradiction.

Therefore there is no isomorphism between

$\mathbb{R}^\times$ and $\mathbb{C}^\times$.

Also, we can say that $-i$ has order 4 in $\mathbb{C}^\times$ i.e $(-i)^4 = (-i)^2 \cdot (-i)^2$

$= 1.$

but if x is real with $x^4 = 1$

then $x = \pm 1$

Here $\text{order}(x) = 2 \neq 4$

Contradiction.

Therefore there is no isomorphism between

$\mathbb{R}^\times$ and $\mathbb{C}^\times$

Note:- $\mathbb{C}^+$ and $\mathbb{R}^+$ are isomorphic

$\phi : \mathbb{C}^+ \longrightarrow \mathbb{R}^+$ defined by.

$\phi(a+ib) = a$

Q. Given any group G of order 12, and any n that divides 12, there exists a subgroup H of G of order n.

True / False:

Soln. False

Take $G = A_4$

$O(G) = 12$.

Take $n = 6$ and $n \mid 12$

But here A_4 has no subgroup of order 6.

2+2
1/2

Unit group of the field of real number $\mathbb{R}$ is $\mathbb{R} - \{0\}$

Let $n \geq 2$. An element 'a' $\in \mathbb{Z}_n$ is said to be a unit if there is an element 'b' $\in \mathbb{Z}_n$ such that $ab = 1$.

Example: In $\mathbb{Z}_5$, 2 is a unit

$2 \cdot 3 = 1 \Rightarrow 2^{-1} = 3$

2 and 3 are inverse of each other.

$U(n)$ denote the group of unit of $\mathbb{Z}_n$

~~$U[n]$~~:

For $n \geq 2$, $U(n) = \{a \in \mathbb{Z}_n : \gcd(a, n) = 1\}$

$U(2) = \{1\} = \mathbb{Z}_1$

$U(2^2) \simeq \mathbb{Z}_2$

$U(2^r)_{r \geq 2} \simeq \mathbb{Z}_2 \times \mathbb{Z}_{2^{r-2}}$

$$U(p^r)_{p\neq 2} \cong \mathbb{Z}_{p^r - p^{r-1}} .$$

$$U(m\cdot n) \cong U(m) \times U(n) \quad \text{if } \gcd(m,n) = 1.$$

Q. let F_3 be a finite field of order 3. let V be a 3-dimensional vector space over F_3. How many 2-dimensional subspaces are contained in V?

Soln. let F be a finite field of size q and V and n-dimensional vectorspace over F.

the number of k-dimensional subspaces of V

$$= \frac{(q^n-1)(q^n-q)\cdots(q^n-q^{k-1})}{(q^k-1)(q^k-q)\cdots(q^k-q^{k-1})}$$

Here $n=3, q=3, k=2$.

$$= \frac{(3^3-1)(3^3-3^{\text{by}})}{(3^2-1)(3^2-3)}$$

$$= \frac{26\cdot 24}{8\cdot 6} = 13$$

#

Number of Subgroup in $\mathbb{Z}_n$

$= \tau(n)$

= Number of divisor of n

Example :- $\mathbb{Z}_{12}$ & $\tau(2^2 \times 3)$

$= \tau(2^2) \times \tau(3)$

$= (2+1)(1+1)$

$= 3 \times 2 = 6$

Number of subgroup of $\mathbb{Z}_{12}$ is 6.

Number of Subgroup of D_n

= Number of divisor of n +

Sum of divisor of n

$= \tau(n) + \sigma(n)$

Number of subgroup in D_3

$$= \tau(3) + \sigma(3)$$

$$= (1+1) + 4$$

$$= 2 + 4$$

$$= 6$$

Ref. where $\sigma(3) = \frac{3^2-1}{3-1} = \frac{8}{2} = 4.$

#

$$\tau(n) = \prod_{1 \le i \le r} (k_i + 1)$$

Example : $\tau(2^2 \times 3) = \tau(2^2) \times \tau(3)$

where $k_1 = 2$, $k_2 = 1$

$$= (2+1)(1+1)$$

$$= 3 \times 2$$

$$= 6$$

$$\# \quad \sigma(n) = \prod_{1 \le i \le r} \frac{p_i^{k_i+1} - 1}{p_i - 1}$$

Example : $180 = 2^2 \cdot 3^2 \cdot 5$

$$\tau(180) = (2+1)(2+1)(1+1) = 18$$

$$\sigma(180) = \left(\frac{2^3-1}{2-1}\right) \times \left(\frac{3^3-1}{3-1}\right) \times \frac{(5^2-1)}{(5-1)}$$

$$= 7 \times 13 \times 6$$

~~Exercise~~.

Note: In S_n, the number of elements which are own inverse ~~equal~~ ~~equal~~

= Number of elements of order 2 in S_n + identity element in S_n.

Q. Find all subgroup of $\mathbb{Z}_2 \times \mathbb{Z}_4$.

Sol $\mathbb{Z}_2 \longrightarrow 1, 2$

$\mathbb{Z}_4 \longrightarrow 1, 2, 4$

So $\mathbb{Z}_2 \times \mathbb{Z}_4$ has subgroup of order 1, 2, 4.

① If subgroup has order 1.

$\mathbb{Z}_2 \times \mathbb{Z}_4$

$1 \quad 1 \quad = \phi(1) \times \phi(1) = 1.$

② If subgroup has order 2

$\mathbb{Z}_2 \times \mathbb{Z}_4$

1 2	$\phi(1) \times \phi(2) = 1$
2 1	$\phi(2) \times \phi(1) = 1$
2 2	$\phi(2) \times \phi(2) = 1$
	Total $= 3$

Now using the formula

Number of subgroup of order d in $\mathbb{Z}_2 \times \mathbb{Z}_4$

=

Number of subgroup of order d

$$= \text{Number of element of order } d \over \phi(d)$$

Number of subgroup of order 2

$$= \frac{3}{\phi(2)} = 3$$

(3) If Subgroup has order 4

$Z_2 \times Z_4$

1 4 $\Rightarrow \phi(1) \times \phi(4) = 2$

2 4 $\Rightarrow \phi(2) \times \phi(4) = 2$

total $= 4$

Number of Subgroup of order 4 $= \frac{4}{\phi(4)}$

$= \frac{4}{2}$

$= 2.$

~~Therefore, total number of subgroup in $Z_2 \times Z_4$~~

~~$\Rightarrow 2+3+1 = 6$~~

Hence the total number of subgroup of

$$\mathbb{Z}_2 \times \mathbb{Z}_6 = 1+2+3$$
$$= 6$$

#. Total number of subgroup of $\mathbb{Z}_3 \times \mathbb{Z}_{13}$

let $G = \mathbb{Z}_{13} \times \mathbb{Z}_{13}$

$o(G) = 13^2$

possible order of $= 1, 13, 13^2$

Here the subgroup containing just the identity is the only group of order 1.

and the only subgroup of order 13^2 order 13^2 must be the whole group.

And Subgroup of order 13 /

$\mathbb{Z}_{13} \times \mathbb{Z}_{13}$

$1 \quad 13 \Rightarrow \phi(1) \cdot \phi(13)$

$13 \quad 1 \Rightarrow \phi(1) \cdot \phi(13)$

$\mathbb{Z}_{13} \times \mathbb{Z}_{13}$

1	13	$\phi(1) \times \phi(13)$	$= 12$
13	1	$\phi(13) \times \phi(1)$	$= 12$
13	13	$\phi(13) \times \phi(13)$	$= 12 \times 12$
			$144 + 24$

~~order~~ Number of subgroup of order 13

$$= \frac{24 + 144}{12}$$

$$= \frac{168}{12}$$

$$= 14$$

Subgroup of order $13^2 = 1$.

Therefore, total number of subgroup in

$$\mathbb{Z}_{13} \times \mathbb{Z}_{13} = 1 + 1 + 14$$

$$= 16 \text{ Ans.}$$

Note :- The number of non-isomorphic abelian group of order $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ is

$$p(\alpha_1) \cdots p(\alpha_k)$$

Q. Let $G = Z_2 \times Z_2 \times Z_2$. find all possible order of element in G.

Soln Number of element of order 1 in G

$= Z_2 \times Z_2 \times Z_2$

$1 \quad 1 \quad 1 \quad \phi(1) \times \phi(1) \times \phi(1)$

$= 1.$

Number of element of order 2 in G

$Z_2 \times Z_2 \times Z_2$

2	1	1	$\phi(2)\ \phi(1)\ \phi(1) = 1.$
1	2	1	$\phi(1)\ \phi(2)\ \phi(1) = 1.$
1	1	2	$\phi(1)\ \phi(1)\ \phi(2) = 1.$
2	2	1.	$\phi(2)\ \phi(2)\ \phi(1) = 1$
2	1	2	$\phi(2)\ \phi(1\ \phi(2) = 1$
1	2	2	$\phi(1)\ \phi(2)\ \phi(2) = 1$
2	2	2	$\phi(2)\ \phi(2)\ \phi(2) = 1.$

Total $= 7.$

Q.

Let G be a finite group. An element $a \in G$ is called a Square if there exist $x \in G$ such that $x^2 = a$.

Suppose that G is cyclic. Then if $a, b \in G$ are not squares, ab is a Square. True / False

Sol: True.

G is cyclic, so G is generated by g and 'a' is not a square, then we can find integer x such that $a = g^{2x+1}$ and b is not a Square, then we can find an integer y such that $b = g^{2y+1}$

$$\text{So } ab = g^{2(x+y+1)}$$

$$= g^{2x+2y+2}$$

$$(ab) = g^{2(x+y+1)}$$

$$\Rightarrow (ab) = g^{2K} \text{ where } K = x+y+1.$$

(ab) is a square.

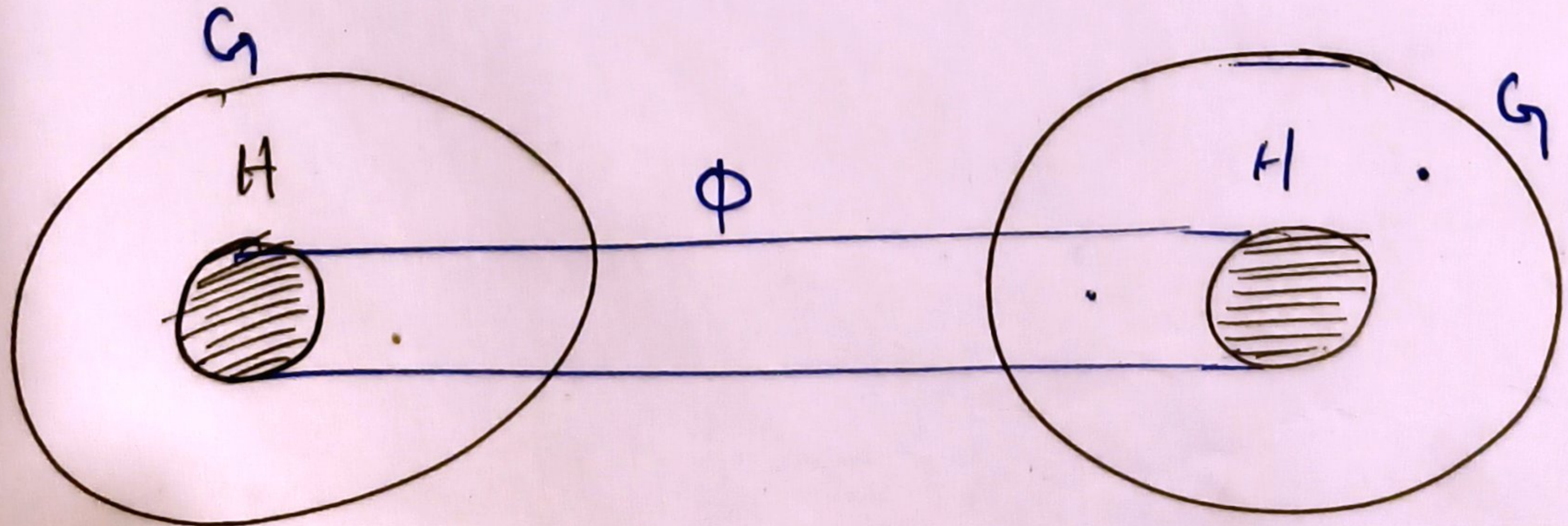
Charact

Characteristic Subgroup :-

A subgroup H of a group G is called characteristic in G if for any $\phi \in Aut(G)$, we have $\phi(H) = H$

Each automorphisms of G maps H to itself.

ϕ fixes H as a set



$\phi : G \to G$

Normal subgroup :

H is a normal subgroup of G i.e

$H \trianglelefteq G$ if $xHx^{-1} = H$ for all $x \in G$.

If H is characteristic in G, then H is a normal subgroup of G.

For each $g \in G$, define a map $\phi_g : G \longrightarrow G$ define by $\phi_g(x) = gxg^{-1}$. These are

Sometimes $\phi_g(x) = gxg^{-1}$ is an inner automorphism.
This is an automorphism of G with inverse $\phi_{g^{-1}}$

Since H is characteristic, we have

$\phi_g(H) = H$, equivalently we have

$gHg^{-1} = H$

Therefore, H is a normal subgroup of G.

Q Give an example of a normal subgroup that is not characteristic.

Sol Consider the additive group $(\mathbb{Q}, +)$ of rational numbers.

The map $\phi : x \longrightarrow \frac{x}{2}$ is an

The map $\phi : \mathbb{Q} \longrightarrow \mathbb{Q}$ defined by

$\phi(x) = \frac{x}{2}$ is an automorphism.

As $(\mathbb{Q}, +)$ is abelian, all subgroups are normal.

The subgroup $\mathbb{Z}$ is not send into itself by ϕ

because $\phi(1) = 1/2 \notin \mathbb{Z}$

Another example :-

Let G be an abelian group of order 4

Then $G = \{e, a, b, ab \mid a^2 = e = b^2 = (ab)^2$
$ab = ba\}$

Let $H = \{e, a\}$.

Then H is a normal subgroup of G as index of H in G is 2.

Let $\phi : G \longrightarrow G$ defined by

$\phi(a) = b, \quad \phi(b) = a, \quad \phi(ab) = ab$

$\phi(e) = e$

Then $\phi \in Aut(G)$

But $\phi(a) = b \notin H$

$\Rightarrow H$ is not characteristic subgroup of G.

Q: Let $G = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{Z} \right\}$ be the group under matrix addition and H be the subgroup of G consisting of matrices with even entries. Find the order of the quotient group $\frac{G}{H}$.

Soln.

$$O\left(\frac{G}{H}\right) = O\left(\frac{\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}}{2\mathbb{Z} \times 2\mathbb{Z} \times 2\mathbb{Z} \times 2\mathbb{Z}}\right)$$

$$= 2 \times 2 \times 2 \times 2$$

$$= 16 \text{ Ans.}$$

Note :-

Q. Let G be a non-abelian group. Let $\alpha \in G$ have order 4 and let $\beta \in G$ have order 3. Then the order of the element $\alpha\beta$ in G need not be finite. True/False.

Sol. True.

Take $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ $\Rightarrow |A| = 1$.

$$B = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix} \Rightarrow B^3 = I$$

$$\alpha\beta = \begin{pmatrix} -1 & 0 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}$$

$(\alpha\beta)^n = \begin{pmatrix} -1 & 0 \\ 1 & -1 \end{pmatrix}^n$ has infinite order.

Q. find the number of elements in the Set $\{x \in S_3 : x^4 = e\}$

Soln Elements of S_3 are

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

Here | $x^n = e$ if and only if order $(x) \mid n$

$x^4 = e \Rightarrow$ order $x \mid 4$

$\Rightarrow$ ~~order~~ $x =$ ~~order~~ $\Rightarrow$

$\Rightarrow$ order of $x = 1, 2, 4$

S_3 has no element of order 4.

Therefore $|x| = 1$ or 2

$\therefore$ Number of elements of order 2 in S_3

$= \frac{3 \times 2 \times 1}{2^1 \times 1!}$

$= 3$

Number of elements of order 1 in S_3

$$= \frac{3!}{1^3 \cdot 3!}$$

$$= 1$$

∴ Total number of elements in the

Set $\{x \in S_3 : x^4 = e\}$ is $3+1=4$

Q. Find the number of group homomorphisms from the group $\mathbb{Z}_4$ to the group S_3?

Sol:

By using this theorem

(1) let $f: G \longmapsto H$ be a homomorphism

~~from~~ If G is a finite group then ~~Im f~~ Im f is a finite subgroup of H and its order divide that of G.

i.e. if $|G| < \infty \Rightarrow |\text{Im } f| \mid |G|$

$$\boxed{\text{order}(\text{Im } f) \mid \text{order}(G)}$$

(2) if $|H| < \infty \Longrightarrow$ ~~Im f~~ $|\text{Im } f| \mid |G|$

$f: Z_4 \longrightarrow S_3$

$|\text{Im } f| \mid o(G)$ i.e $|\text{Im } f| \mid 4$

~~o f~~ $o(S_3) = 6$

$\Rightarrow |\text{Im } f| = 1 \text{ or } 2$

Case I:-

If $|\text{Im } f| = 2$, then $\text{Im } f$ is a subgroup of order 2 of S_3.

There are exactly 3 of these : $\{e, x_i\}$

for each $i = 1, 2, 3$.

Since f a homomorphism must ~~Aa~~ map the identity to the identity, therefore we have the homomorphisms

$$f_1 : \begin{pmatrix} 0 \\ 1 \\ 2 \\ 3 \end{pmatrix} \longmapsto \begin{pmatrix} e \\ x_1 \\ e \\ x_1 \end{pmatrix} = \text{Im } f_1$$

$\text{Im } f_1$ is a subgroup of order of S_3

$$f_2 : \begin{pmatrix} 0 \\ 1 \\ 2 \\ 3 \end{pmatrix} \longmapsto \begin{pmatrix} e \\ x_2 \\ e \\ x_2 \end{pmatrix} = \text{Im} f_2$$

$$f_3 : \begin{pmatrix} 0 \\ 1 \\ 2 \\ 3 \end{pmatrix} \longmapsto \begin{pmatrix} e \\ x_3 \\ e \\ x_3 \end{pmatrix} = \text{Im} f_3$$

Case II

If $|\text{Im} f| = 1$ then f is the trivial homomorphism $f(x) = e$ for all $x \in \mathbb{Z}_4$.

Therefore, there 4 distinct homomorphism from $\mathbb{Z}_4$ to S_3

Note:- We can also take $f_2(x) = (2\,3)^x$, $x \in \mathbb{Z}_4$

$f_2(x) = (1\,3)^x$

$f_3(x) = (1\,2)^x$

$$f_2 : \begin{pmatrix} 0 \\ 1 \\ 2 \\ 3 \end{pmatrix} \longmapsto \begin{pmatrix} e \\ x_2 \\ e \\ x_2 \end{pmatrix} = \text{Im} f_2$$

$$f_3 : \begin{pmatrix} 0 \\ 1 \\ 2 \\ 3 \end{pmatrix} \longmapsto \begin{pmatrix} e \\ x_3 \\ e \\ x_3 \end{pmatrix} = \text{Im} f_3$$

Case II

If $|\text{Im} f| = 1$ then f is the trivial homomorphism $f(x) = e$ for all $x \in \mathbb{Z}_4$.

Therefore, there 4 distinct homomorphism from $\mathbb{Z}_4$ to S_3

Note:- We can also take $f_2(x) = (2\,3)^x$, $x \in \mathbb{Z}_4$

$f_2(x) = (1\,3)^x$

$f_3(x) = (1\,2)^x$

operation in G	operation in H	Group map definition
$+$	$+$	$f(x+y) = f(x) + f(y)$
$+$	$\cdot$	$f(x+y) = f(x) \cdot f(y)$
$\cdot$	$+$	$f(x \cdot y) = f(x) + f(y)$
$\triangle$	$\star$	$f(x \triangle y) = f(x) \star f(y)$

Q. Let $\alpha = (a_1 a_2 \dots a_k)$ be a k-cycle. Prove that α is odd if and only if K is even.

Soln $\alpha = (a_1 a_k) \dots (a_1 a_3)(a_1 a_2)$ is a product of $k-1$ transpositions.

Therefore, α is odd if and only if $k-1$ is odd if and only if k is even.

Note:-

$$(a_1 a_2 a_3 \dots a_k) = (a_1 a_k) \dots (a_1 a_4)(a_1 a_3)(a_1 a_2)$$

Prove that every subgroup of S_n has either every ~~nen~~ member as even or exactly half the ~~nen~~ members as even permutations.

Soln. Consider the homomorphism

$$f: S_n \longrightarrow \mathbb{Z}_2 \quad \text{defined by}$$

$$f(x) = \begin{cases} 1 & \text{if } x \text{ is even} \\ -1 & \text{if } x \text{ is odd} \end{cases}$$

Let H be a subgroup of S_n

The only subgroup of $\mathbb{Z}_2$ are $\{1\}, \{1,-1\}$

If ~~f(H)~~ If $f(H) = 1$ then H is even

ie H has all permutations to be ~~nen~~ even.

If $f(H) = \{1,-1\}$ then number of

If $f(H) = \{1, -1\}$ then number of even permutations = number of elements of S_n, which are mapped to 1

$= f(H)$ = Half of order of $\mathbb{Z}_2$.