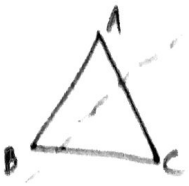
3-1-17

Group Theory

Symmetry of Rotation of an eq. Δ:



Axis.

120° clockwise : R (A occupies C's original ...)

120° again : R^2

120° again : R^3 (same as original)

(*) R^3 → identity transformation.

F_1: A → A
B → C
C → B

F_2 (Along the median)

F_2 * : B → B
A → C
C → A

Composition of the above operations:
(One after the other)

RF: $A \xrightarrow{R} B \xrightarrow{F_1} C$

B → C → B

C → A → A

FR: $A \xrightarrow{F} A \xrightarrow{R} B$

B → C → A

C → B → C

RF ≠ FR ; R doesnot commute with F.

1. The first property of a group is that composition of any 2 elements of the group, we get back a member of the group.
2. It should have an identity element.
3. Assosiativity. 4. Existence of inverse.

A group G is a non empty set of elements if there is defined a binary operation called product & denoted by $*$ or $\cdot$ (can be any operation) such that:

1. Closure: $A, B \in G \Rightarrow A \cdot B \in G$

2. $A, B, C \in G \Rightarrow A \cdot (B \cdot C) = (A \cdot B) \cdot C$
   Assosiative Law

3. There exists element $e \in G \ni a = a \cdot e$ $\forall a \in G$.
   Existence of the identity element in G:

4. For every $a \in G$ $\exists$ an a^{-1} in G such that
   $a \cdot a^{-1} = a^{-1} \cdot a = e$.
   Existence of the inverse.

If in addition to this $a \cdot b = b \cdot a$ $\forall a, b \in G$.
Then G is called an Abelian group.

Congruence Modulo: mod n:
Op: Addition $(0, 1, 2, \ldots n-1)$

Any number we get, we shd take mod n.

$G = S_3$ Symmetric group is the group of 1-1 mappings of the set $\{x_1 x_2 x_3\}$ onto itself.

eg: -1 : Symmetric group

ϕ : $x_1 \to x_2$, $x_2 \to x_1$, $x_3 \to x_3$

ψ : $x_1 \to x_2$, $x_2 \to x_3$, $x_3 \to x_1$.

$\phi \cdot \psi \Rightarrow$ $x_1 \to x_2 \to x_3$, $x_2 \to x_1 \to x_2$, $x_3 \to x_3 \to x_1$

$\psi \cdot \phi \Rightarrow$ $x_1 \to x_1$, $x_2 \to x_3$, $x_3 \to x_2$

$\psi^2 \Rightarrow$ $x_1 \to x_3$, $x_2 \to x_1$, $x_3 \to x_2$

$\phi^2 \Rightarrow$ $x_1 \to x_1$, $x_2 \to x_2$, $x_3 \to x_3$

~~$\phi^{-1} \Rightarrow$~~

$\psi^3 \Rightarrow$ $x_1 \to x_1$, $x_2 \to x_2$, $x_3 \to x_3$

$\psi^3 = e$

$\psi^2 = \psi^{-1}$

$\psi^{-1}\phi = \phi\psi$

So this is a group with $e = \phi^2$ or ψ^3.

Cyclic group: Let n be any $\neq$ integer.

We consider a group of order n as fall:

$i = 0, 1, 2 \cdots n-1$

where $a^0 = a^n = e$.

$a^i \cdot a^j = a^{i+j}$ if $i + j \leq n$

$a^i \cdot a^j = a^{i+j-n}$ if $i + j > n$.

3. We know $(a^{-1}) \cdot (a^{-1})^{-1} = e = a^{-1} \cdot a$

Left cancellation,

$(a^{-1})^{-1} = a$.

4. $(ab) \cdot (b^{-1}a^{-1}) = a(b \cdot b^{-1}) \cdot a^{-1} = aea^{-1} = a \cdot a^{-1} = e$

$(b^{-1}a^{-1}) \cdot (ab) = b^{-1}b = e$.

$\Rightarrow (ab)^{-1} = b^{-1}a^{-1}$

Eg: Prove whether the sets are groups or not:

1. Integers, $-$ $(\mathbb{Z})$

Assosiativity doesn't hold.
Identity doesn't exist.

2. ~~(N)~~ Whole Nos; $\bullet$ $*$

Inverse doesn't exist.

3. Rational nos, with odd den, $(+)$ ~~$\bullet$~~

4) P.T. if G is an Abelian group, $\Rightarrow (ab)^m = a^m \cdot b^m$ $\forall$ integers m.

Induction: $S(1) \rightarrow$ True.

Suppose $S(K-1)$ is true.

$(ab)^{K-1} = a^{K-1} \cdot b^{K-1}$

$S(K) = (ab)^{K-1} \cdot (ab)$ $\in G$

$\Rightarrow a^{K-1} \cdot (b^{K-1} \cdot a) \cdot b$

$\Rightarrow a^K \cdot b^K$ $\therefore S(K)$ is true

$(ab)(ab)(ab)\cdots(ab)$ (m times)

$\Rightarrow aa\,bb\,aa\,bb\,aa\,bb\cdots$

$a^2b^2a^2b^2a^2b^2\cdots$

$a^2a^2b^2b^2\cdots$

$\Rightarrow$ go on $a^m b^m$

$n = 0 \quad (ab)^0 \Rightarrow e$

$a^0 \cdot b^0 \Rightarrow e \cdot e = e$.

Suppose $n = -m$.

$$(ab)^n = (ab)^{-m} = ((ab)^{-1})^m$$

$$\Rightarrow (b^{-1}a^{-1})^m$$

G is commutative

$$\Rightarrow (a^{-1}b^{-1})^m$$

$$\Rightarrow (pq)^m$$

$$\Rightarrow p^m q^m$$

$$\Rightarrow a^{-m} b^{-m}$$

$$\Rightarrow a^n b^n$$

5. If G is a group such that $(ab)^2 = a^2b^2$, then the group is Abelian.

$$(ab)^2 = a^2 b^2$$

$$\Rightarrow (ab)\cdot(ab) = a \cdot a \cdot b \cdot b$$

$$a(ba)b = a \cdot (ab)b$$

Left, Right cancellation

$$ab = ba$$

6. Suppose the above result is true for consec. int ; P.T grp is Abelian [$(ab)^m = a^m b^m$]

$(ab)^m = a^m \cdot b^m$

$(ab)^{m+1} = a^{m+1} \cdot b^{m+1}$

$(ab)^{m+2} = a^{m+2} \cdot b^{m+2}$

$a^m b^m \cdot (ab)^2 = a^m \cdot a^2 \cdot b^m \cdot b^2$

$(ab)^m \cdot ab$

$a^m \cdot b^m \cdot a \cdot b = a^m \cdot a \cdot b^m \cdot b$

$\Rightarrow \boxed{b^m a = a b^m}$

$b^m \cdot (ab)^2 = a \cdot a \cdot b^m \cdot b^2$ | $b^m a = ab^m$

$b^m \cdot (ab)^2 = a\, b^m (ab^2)$

~~$b^m a = ab^m$~~

$b^m abab = a\, b^m a\, b^2$

$\Rightarrow a b^m bab = a\, b^m a\, b^2$

$bab = a \cdot b \cdot b$

$\Rightarrow \underline{ba = ab}$

Eg: In S_3 find elements such that:

$(xy)^2 \neq x^2 y^2$

S_3: $\{e, \psi, \psi^2, \phi, \phi\psi, \psi\phi\}$

$\phi = x_1 \to x_2$, $x_2 \to x_1$, $x_3 \to x_3$

$\psi = x_1 \to x_2$, $x_2 \to x_3$, $x_3 \to x_1$.

$\boxed{x = \psi \quad y = \phi}$

here

17-1-17

Congruence Modulo

(addition Mod n)

$a \equiv b \bmod n$

iff $n \mid (b-a)$

n divides.

This is an equivalence relation on the set of integers (Prove it).

Therefore, it partitions the set properly into equivalence classes.

Subgroup: H is a subgroup if $H \leq G$ and H is a group by itself.

Result-1 H is a subgroup of G iff

① $a, b \in H \Rightarrow a \cdot b \in H$.

② $a^{-1} \in H$.

I) $\because H$ is a group, ①, ② imply.

II) Given these properties, we need to prove H is a group.

(a) Closure: Given

(b) Associative: if $a, b, c \in H$

$a, b, c \in G$.

$\therefore (a \cdot b) \cdot c = a \cdot (b \cdot c)$

(c) Inverse exists and is present in H.

(d) $a \cdot a^{-1} = e \in H$

$a^{-1} \cdot a = e \in H$

as H is closed. ∎

Result-2 In case H is a finite subset of G, then H is a subgroup if $a \cdot b \in H$ where $a, b \in H$.

Proof: Let $a \in H$.

$\Rightarrow a^2 \in H$ (By closure property).

$\Rightarrow a^3, a^4 \ldots \in H$

but H is finite. So there are repetitions:

$$a^r = a^s \quad r > s > 0.$$

since $a^r, a^s \in H \Rightarrow \in G$.

$\Rightarrow \underbrace{a \cdot a \cdot a \cdots}_{r \text{ times}} = \underbrace{a \cdot a \cdot a \cdots}_{s \text{ times}}$

Apply Cancellation on G.

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

$a^{r-s} \in H \quad \therefore e \in H$.

(Any power of $a \in H$)

$r > s > 0$

$\Rightarrow \boxed{r - s - 1 \geq 0}$

$\Rightarrow a^{r-s-1} \in H$.

(closure).

$a^{r-s} = e$

$a^{-1} \cdot a^{r-s} = e \cdot a^{-1}$

$\Rightarrow a^{r-s-1} = a^{-1}$

$\Rightarrow a^{-1} \in H$.

Eg (a) Let G be grp of Int under '+'.

H is a subset consisting multiples of 5.

$\Rightarrow$ Yes.

(b). $H_n \rightarrow$ multiples of n. [subgrp of G].

$H_m \rightarrow$ " " m

$m = 6 \quad n = 9$.

$H_6 \cap H_9 \Rightarrow H_{18} \rightarrow$ subgroup.

Eg: if H, K are subgrps of G, P.T. $H \cap K$ is a subgroup of G.

We need to show Closure property, Inverse property.

① Closure: $a, b \in H \cap K$

$\Rightarrow a, b \in H$, $a, b \in K$

$\Rightarrow a \cdot b \in H$, $a \cdot b \in K$

$\Rightarrow a \cdot b \in H \cap K$

② Inverse: $a \in H \cap K$

$a \in H$, $a \in K$

$\Rightarrow a^{-1} \in H$, $a^{-1} \in K$

$\Rightarrow a^{-1} \in H \cap K$.

Note: $H \cup K$ may not be a subgroup.

Cyclic Subgroup

G is any group

$a \in G$.

$(a) = \{ a^i \mid i = 0, \pm 1, \pm 2, \cdots \}$

is the cyclic subgrp. generated by a.

Let G be a group. H be a subgroup of G.

For $a, b \in G$, we say that $a \equiv b \bmod H$ if $ab^{-1} \in H$.

Result: Congruence Modulo is an equivalence relation.

Reflexive: $a \cdot a^{-1}$

$\Rightarrow e \in H$

$\rightarrow$ holds.

Symmetric: Let $ab^{-1} \in H$.

To prove: $ba^{-1} \in H$

if $(ab^{-1})^{-1} \in H$

$\Rightarrow (ab^{-1})^{-1} \in H$

$\Rightarrow ba^{-1} \in H$.

transitive: Let $ab^{-1} \in H \quad bc^{-1} \in H$

$\Rightarrow (ab^{-1}) \cdot (bc^{-1}) \in H$

$\Rightarrow ac^{-1} \in H$.

Def: If H is a subgroup of G,

$H \cdot a = \{ h \cdot a \mid h \in H \}$

is called the coset of H in G.

Result $\forall a \in G$, $Ha = \{ x \in G \mid a \equiv x \bmod H \}$

Let $[a] = \{ x \in G \mid a \equiv x \bmod H \}$

$\rightarrow$ (I) $Ha \subseteq [a]$

Let $h \in H$

$\Rightarrow h^{-1} \in H$

$aa^{-1}h^{-1} \in H$

$ax^{-1} \in H$

$\Rightarrow a \equiv x$

$\Rightarrow x \in [a] \Rightarrow (a)(ha)^{-1} \in H$.

$\Rightarrow ha$ is in class of a.

$\therefore Ha \subseteq [a]$

I. $[a] \subseteq Ha$

Let $x \in [a]$

$\Rightarrow ax^{-1} \in H$ or $H^{-1}a \in H$.

$\Rightarrow (ax^{-1})^{-1} \in H$

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

$\Rightarrow xa^{-1}a = ha$

$\Rightarrow x = ha$.

Eg: Prove that $Hh = H$.

$Hh \subseteq H$ & $H \subseteq Hh$

Let $h' \in H$

$hh' \in Hh$ but $h'h \in H$ as H has closure property.

Let $h' \in H$

$h'e \in H$.

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

$(h'h^{-1})h = h_1 h \in Hh$

Put $h'h^{-1} = h_1$

$h'h \in H$

$h'h$ in $Hh \Rightarrow h'h \in H$

$\Rightarrow \boxed{Hh \leq H}$.

Eg: Any two right or left cosets are either disjoint or identical.

Let $c \in Ha \Rightarrow c = h_1 a$

$c \in Hb \Rightarrow c = h_2 b$.

$\Rightarrow h_1 a = h_2 b$

$a = (h_1^{-1} h_2) b$

$\Rightarrow \boxed{a = h_3 b}$

$\Rightarrow Ha = [H h_3] b$

$= Hb$

i.e. $\boxed{Ha = Hb}$

Eg: S.T. One-one correspondance between H and G [Right / Left coset]

Define a mapping $f(aH) = Ha^{-1} \ \forall \ a \in G$.

To verify that this mapping is well defined. Let aH, bH represent the same coset.

$aH = bH$

$H = a^{-1} b H \Rightarrow a^{-1} b \in H$

$Ha^{-1} b = H \Rightarrow Ha^{-1} b b^{-1} = Hb^{-1}$

$Ha^{-1} = Hb^{-1}$.

$\Rightarrow f(aH) = f(bH)$.

one-one

$f(aH) = f(bH)$

$Ha^{-1} = Hb^{-1}$

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

$Ha^{-1}b = H$

$\Rightarrow a^{-1}b \in H \Rightarrow a^{-1}bH = H \Rightarrow aH$

or $bH = aH$.

Onto $f(aH) = Ha^{-1}$

$Ha \rightarrow$ Right Coset

$a^{-1}H \rightarrow$ left Coset

$f(a^{-1}H) = H(a^{-1})^{-1}$

$= Ha$

i.e; ~~both~~ each right coset is an image of a left coset $a^{-1}H$

$\Rightarrow$ H is a subgroup of G_1, G_1 is a finite group $O(H)$ means no. of elements in H. $O(H) \mid O(G_1)$.

$a \mid b \rightarrow$ a divides b.

H is a subgroup of G_1. Enumerate the elements in H; $h_1, h_2 \cdots h_r$;

if all of these form G_1, then $O(H) = r = O(G_1)$ and $O(H) \mid O(G_1)$.

Else

$h_1, h_2, h_3 \cdots h_r \rightarrow (1)$

Let an element $a \notin H$.

$\Rightarrow ah_1, ah_2 \cdots ah_r \rightarrow (2)$

If this is all of G_1,

$O(G) = r + r = 2r$

$O(H) = r$ & $r \mid 2r$

Claim No 2 elements in ①, ② are same.

if not $h_i = h_j a$

$\Rightarrow a = h_j^{-1} h_i$

$\Rightarrow a \in H$

which is false.

Claim No two elements $h_j a$; $h_k a$ are equal.

if not, $h_j a = h_k a$

$\Rightarrow h_j e = h_k$

But $h_j \neq h_k$.

If this is not G, then consider set:
$\exists\ b \notin H$.

$\{b h_1, b h_2 \cdots b h_r\}$ and go on.

This isn't ∞ as G is finite.

Eg
If G is a finite group, $a \in G \overset{\text{P-T}}{\Rightarrow} O(a) \mid O(G)$.

★ If G is a group, $a \in G$ $O(a)$, least positive integer m, $a^m = e$.

Eg: If G is a finite group, $a^{O(G)} = e$. [Proof

$$a^{O(G)} = a^{O(A) \cdot m}$$

$$\Rightarrow e^m = e.$$

Eg: $\phi(n)$: ^ Group of all relative primes to n (No. of elements in a $< n$.

P.T. $a^{\phi(n)} \equiv 1 \bmod n$.

$(a, n) \equiv 1$

Ans:

Mid-1 to Mid-2

No. of cosets [Right or Left]

$O(G) / O(H)$.

Let us consider S_3:

$\phi = x_1 \to x_2,\ x_2 \to x_1,\ x_3 \to x_3$

$\psi : x_1 \to x_2,\ x_2 \to x_3,\ x_3 \to x_1$.

Let $H = \{e, \phi\}$

Right Cosets

$He = \{e, \phi\}$

$H\psi = \{\psi, \phi\psi\}$

$H\psi^2 = \{\psi^2, \phi\psi^2\}$

Left Cosets

$eH = \{e, \phi\}$

$\psi H = \{\psi, \psi\phi = \phi\psi^2\}$

$\psi^2 H = \{\psi^2, \psi^2\phi = \phi\psi\}$

The right cosets need not be the same as left cosets.

If $N = \{e, \psi, \psi^2\}$

Right Cosets

$Ne = \{e, \psi, \psi^2\}$

$N\phi = \{\phi, \psi\phi, \psi^2\phi\}$

Left Cosets

$eN = \{e, \psi, \psi^2\}$

$\phi N = \{\phi, \phi\psi, \phi\psi^2\}$

Here, right cosets are same as Left cosets, although not element by element.

such groups (H) are called Normal Subgroups.

Definition (Normal subgroups)

A subgroup N of G is a normal subgroup of G if $\forall\ g \in G,\ n \in N$

$$gng^{-1} \in N$$

or equivalently $gNg^{-1} \subseteq N$ (↓ is contained in)

$$\Rightarrow \boxed{gNg^{-1} = N}$$

- result which is true for normal subgroups.

Result N is a normal subgroup of G iff

$$gNg^{-1} = N \quad \forall\ g \in G.$$

① Assume $gNg^{-1} = N$

$\Rightarrow gNg^{-1} \subseteq N$ $\therefore N$ is normal.

② Assume $gNg^{-1} \subseteq N$, P.T $gNg^{-1} = N$ (↓ ⟶ ①)

True $\forall\ g$.

$\therefore g^{-1}N(g^{-1})^{-1} \in N$

$\Rightarrow g^{-1}Ng \subseteq N$

$\Rightarrow g(g^{-1}Ng)g^{-1} \subseteq gNg^{-1}$

(x)

since x is contained in N.

But x is nothing but N.

$\therefore \boxed{N \subseteq gNg^{-1}} \rightarrow ②$

from ①, ② $gNg^{-1} = N$.

~~Re~~ Result: P.T. if N is a normal subgroup, every right coset is a left coset and vice versa.

Property: $(gng^{-1})^m = gn^m g^{-1}$

$(gng^{-1})^2 = ghg^{-1} \cdot gng^{-1}$

$\Rightarrow gn^2g^{-1}$

Proof: (Result).

① $gNg^{-1} = N$ (N is normal)

$gNg^{-1} \cdot g = Ng$

$\Rightarrow gN = Ng$

So if N is normal left coset = Right coset.

② Converse:

Let $g \in G$, gN – Left Coset

$g \in gN$

$\therefore$ g is an element present in a left Coset gN.

No other ~~subgroup~~ Left coset of N has g.

Similarly g is also in Ng

Ng is unique.

$Ng = gN$.

$\Rightarrow gg^{-1} \cdot gNg^{-1} = Ngg^{-1}$

$= N$

$\Rightarrow$ it is a Normal

If we consider a group of Cosets of G. normal sub-

(Quotient group) G/N.

(Grp of cosets of a normal subgrp)

Closure: $(Na \cdot Nb)$ shd give back a right coset.

$N(a \cdot N)b$

$N(Na)b$

$\Rightarrow Nabb$ $(N \times N = N)$

$\in G$.

$\Rightarrow Nc$

which is a right coset.

Associative: $Na(Nb \cdot Nc) = (Na \cdot Nb) \cdot Nc$

$\Rightarrow Na \cdot N(bc)$ $\quad$ $Nabc$

$\Rightarrow Nabc$

Inverse: Ne is the Identity

$\hookrightarrow Na^{-1}$

Problem: If G is a group and H is a subgroup of index 2 in G, P.T. H is a normal subgroup:

2 cosets: ① He, eH ② Hx $\hookrightarrow x \in G$, xH.

All ↑ Cosets together partition the group.
Left or right

$\therefore G = H \cup Hx$

$= H \cup xH$

$\therefore Hx = xH$

$H = xHx^{-1}$ $\therefore H$ is normal.

Eg: If N is a normal subgroup of G and H is any subgroup of G, P.T. NH is a subgroup of G.

Consider 2 elements n_1h_1, ~~n_2h_2 in NH~~

We need to P.T. ~~$(n_1h_1)(n_2h_2)^{-1} \in NH$~~

T.P. $(n_1h_1)(n_2h_2)^{-1} \in NH$ $\Rightarrow n_1h_1h_2^{-1}n_2 \in NH$

$\Rightarrow n_1h_x n_2 \in NH$

$\Rightarrow n_1 h_1 h_2^{-1} n_2^{-1}$

$\Rightarrow n_1 \underbrace{h'h_2^{-1}}$

$\downarrow$

$h'N$

$= Nh'$ [Normal]

$n''h''$

$\Rightarrow n_1 n''h''$

$\Rightarrow nh$

Eg: Suppose H is only subgroup of $O(H) = m$ of a finite group. Then P.T. H is a normal subgrp of G.

Let $H = \{h_1, h_2 \cdots h_m\}$

Let $x \in G$.

$xHx^{-1} = (\underbrace{xh_1x^{-1} \cdots xh_mx^{-1}}).$ P.T. this is a subgrp

all these elements are distinct.

because if $xh_rx^{-1} = xh_sx^{-1}$

$\Rightarrow h_r = h_s$ [False].

That is we have generated 2 subgrps of $O(H)$.

$\therefore xHx^{-1} = H$

↓

Normal.

Eg: Let N, M be normal subgroups. P.T. $N*M$ is a normal subgroup in G.

$gNg^{-1} = N$

$gMg^{-1} = M$

$gNg^{-1} \cdot gMg^{-1} = N*M$

$\Rightarrow g(NM)g^{-1} = NM$.

Also prove that $N*M$ is a subgroup.

Eg: Let N, M be Normal Subgroups $N \cap M = e$.

P.T. $nm = mn$.

(n commutes with every element in M)

↳ $nm \cdot (mn)^{-1} = e$

$\Rightarrow nmn^{-1}m^{-1} = e$.

To show: $nmn^{-1}m^{-1} \in N \cap M$

① $n(mn^{-1}m^{-1})$

$\in N$

$nn' \in N$

② $(nmn^{-1})m^{-1}$

$\in M$

$\Rightarrow m'M^{-1} \in M$.

$\therefore nmn^{-1}m^{-1} \in N, M$.

$\therefore nmn^{-1}m^{-1} \in N \cap M$

$\Rightarrow nmn^{-1}m^{-1} = e$

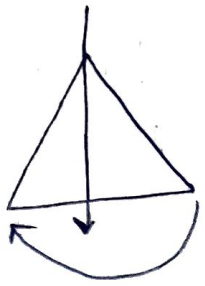
$\therefore mn = nm$

Dihedral Group

Let G be a group defined as:

$\boxed{x^i y^j}$ $i = (0, 1)$ ⟶ flipping

$j = (0, 1, \cdots n-1)$ ⟶ rotations $(2\pi/n)$ diff rotations



① $x^2 = e \quad y^n = e$

② $xy = y^{-1}x$

1. $(xy) \cdot (y^{-1}x) = x^2 = e$

2. $(xy) \cdot y = y^{-1}xy = y^{-1}y^{-1}x$
   (xy^2) $\Rightarrow y^{-2}x$

3. Similarly $xy^3 = y^{-3}x$

What is the general form of:

$(x^i y^j)(x^k y^l) = ?$

$i = \{0, 1\}$

Let $k = 1$.

$\Rightarrow x^i y^j y^{-l} x$

$\Rightarrow x^i y^{j-l} x$

$\Leftrightarrow x^{j+1} y^{l-j}$

general form: $\boxed{x^{i+k} y^{(-1)^k \cdot j + l}}$

Homomorphism

Let ϕ be a mapping from G to G' where G, G' are 2 groups such that for (elements in G, G' may be of diff type)

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

$*$ → operation in G

$\bullet$ → operation in G'

(x, y) → Elements of G.

Eg

Eg G is the group. Mapping : $\log x$

Mult. in G, Addition in G'. [+ve reals].

$E G, G'$:

$$\phi(x \cdot y) = \log(xy)$$

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

Equal

So ϕ is a homomorphism

Eg: G is be the grp of non zero real numbers under multiplication

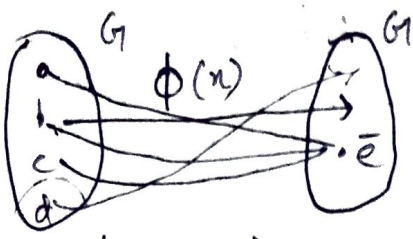
$$\phi(x) = x^2$$

Is $\phi(x)$ homomorphous.

Eg: $\phi(x) = 2^x$ Is this homomorphic (No)

Eg: $\phi(x) = (x+1)$. (No)

The Kernel K of a homomorphism :



(a, b, c) form the kernel.

Property of Kernel:

1. $\phi(e) = \bar{e}$

$$\phi(x) \cdot \bar{e} = \phi(x)$$
$$= \phi(xe)$$
$$\Rightarrow \phi(x) \cdot \phi(e)$$
$$\Rightarrow \bar{e} = \phi(e).$$

2. $\phi(x^{-1}) = (\phi(x))^{-1}$

$$\phi(e) = \bar{e}$$
$$\phi(x \cdot x^{-1}) = \bar{e}$$
$$\phi(x) \cdot \phi(x^{-1}) = \bar{e}$$
$$\phi(x) = (\phi(x^{-1}))^{-1}$$
$$\phi(x^{-1} \cdot x) = \bar{e}$$
$$\phi(x^{-1}) = (\phi(x))^{-1}$$

3. Kernel of a homomorphism is a normal subgroup.

if $x, y \in K$ $\phi(x) = e$ $\phi(y) = e$.

To prove: $x \cdot y \in K$; $\phi(xy) = \phi(x)\phi(y)$
$= \bar{e} \cdot e = e$.

$\therefore xy \in K$

Inverse: $\phi(x) = e$

$(\phi(x))^{-1} = e^{-1} = e$.

$\Rightarrow \phi(x^{-1}) = e$

$\therefore x^{-1} \in K$

it is a subgrp.

Normal: Consider gKg^{-1}.

$\phi(gKg^{-1})$

$\Rightarrow \phi(g) \cdot \phi(x) \cdot \phi(g^{-1})$

$\phi(x) \to e$

$\phi(g \cdot g^{-1})$

$\Rightarrow \phi(e)$

$\Rightarrow e$.

Theorm

If ϕ is the homomorphism of G onto $\bar{G}$ with Kernel K. then the set of all inverse images of $\bar{g} \in \bar{G}$ under ϕ in G is given by Kx where x is any particular inverse image of $\bar{g}$ in G.

if $(\bar{g} = \bar{e})$ we are done;

else if The inverse images of $\bar{g} \neq \bar{e}$.

Suppose $x \in G$ is one inverse of $\bar{g}$.

Let $k \in K$. $y = kx$

$\phi(y) = \phi(kx) = \phi(k) \cdot \phi(x) = \bar{e}\,\phi(x) = \phi(x) = \bar{g}$

$\bar{g}$ is the image of kx.

If Kx is not all of the inverse images of $\bar{g}$; let $\phi(z) = \bar{g} = \phi(x)$

$$\Rightarrow \phi(z)\cdot(\phi(x))^{-1} = \bar{e}$$

$$\phi(zx^{-1}) = \bar{e}$$

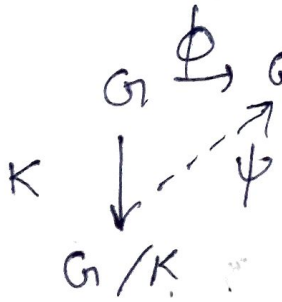
$zx^{-1} \in K$

$z \in Kx$

This mapping is one-one if $K = \{e\}$.

A Homo-morphism is isomorphism if it is Injective. It is isomorphic if it is bijective. (One-one)

Theorm Let ϕ be a homomorphism of G onto $\bar{G}$ with Kernel K. Then $G/K \sim \bar{G}$ (Isomorphic) [ϕ : onto]



$g \in G \rightarrow \phi(g)$

$g \in G \rightarrow \frac{G}{K} \rightarrow (Kg)$

$\phi(g) = \phi(Kg') = \phi(K)\cdot\phi(g') = \bar{e}\,\phi(g') = \phi(g')$

Mapping ψ is well defined.

$X, Y \in G/K$

$X = Kg \quad Y = Kf \quad XY = Kgf$

$$\psi(xy) = \psi(kgf)$$

$$\Rightarrow \phi(gf).$$

$$\Rightarrow \phi(g) \cdot \phi(f).$$

$$\Rightarrow \underset{X}{\psi(kg)} \cdot \underset{Y}{\psi(kf)}$$

For One-one:

If Kernel of ψ = Identity of G/K → K itself

it is one-one

If $\psi(x) = \bar{e}$ $\quad x = kg$: $\psi(x) = \psi(kg) = \phi(g) = \bar{e}$ ($g \in K$, $kg \in K$)

$x = ke$

$\psi(ke) \Rightarrow \phi(e) = \bar{e}$.

For onto: Since it is given that ϕ is ~~the~~ an onto mapping → onto

$$g \xrightarrow{\phi} \phi(g)$$

kg ↓

K

→ every g has a unique kg.

Eg: If H is a subgrp of G, then the centralizer $C(H) = \{x \in G \mid xh = hx \ \forall h \in H\}$

P.T. $C(H)$ is a subgrp.

closure: $xh = hx \ \forall h \in H$

for $xy \in H$

$(xy)h = h(xy)$

$\hookrightarrow x h y$

$\Rightarrow hxy$

$\therefore$ closure.

Inverse: $xh = hx$

$xhx^{-1} = h$

$hx^{-1} = x^{-1}h$

Eg: The center of G:

$\{z \in G \mid xz = zx \ \forall x \in G\}$

P.T. ~~$C(H)$ is a~~ it is a subgroup.

Eg: P.T. center of G is a normal subgrp.

$\boxed{x\,C(G)\,x^{-1} = C}$

$\Rightarrow Cx \cdot x^{-1}$

$= C.$

Eg: $U = \{ xyx^{-1}y^{-1} \mid x, y \in G \}$

is a subgroup called the Commutator Subgroup. This is a Normal subgroup.

Let $u_1 = x_1 y_1 x_1^{-1} y_1^{-1}$

$$gug^{-1} \in U$$

Consider $gxyx^{-1}y^{-1}g^{-1}$

$$\Rightarrow \underbrace{(gxg^{-1})}_{x'} \underbrace{(gyg^{-1})}_{y'} \underbrace{(gx^{-1}g^{-1})}_{x'^{-1}} \underbrace{(gyg^{-1})}_{y'^{-1}}$$

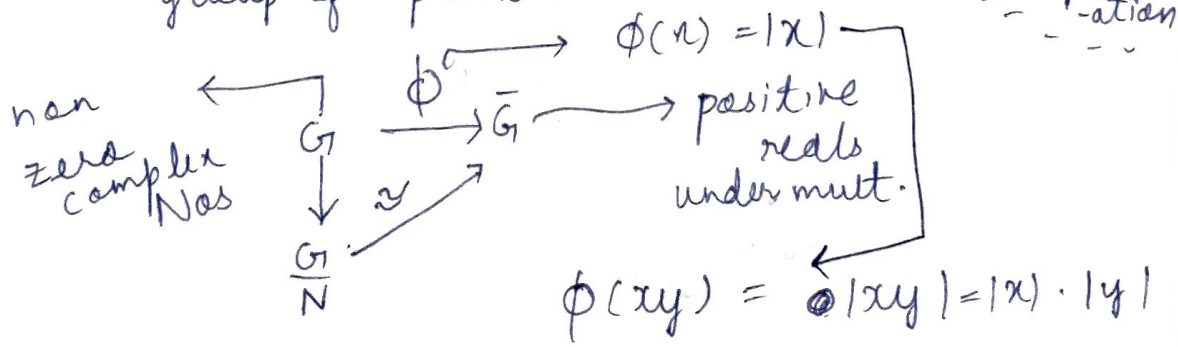
$$\Rightarrow x' y' x'^{-1} y'^{-1} \in U.$$

Eg: Let G be the group of non zero complex numbers under multiplication.

Let N be the set of complex numbers with absolute value 1.

$$N = \{ a + bi \mid a^2 + b^2 = 1 \}$$

Show that G/N is isomorphic to the group of positive reals under multiplication



$$\text{Ker}_\phi = \{ x \in G \mid \phi(x) = 1 \}$$

$$\Rightarrow \{ x \mid |x| = 1 \}$$

$$\Rightarrow N$$

From the first theorem of Isomorphism, this follows.

Eg: Let G_1 be the group of real nos. under addition, Let N be the subgrp of G_1 consisting of all integers. prove that G_1/N is isomorphic to the group of all complex numbers under multiplication.

G_1 → real numbers under addition

$G_1 \xrightarrow{\phi} \bar{G}$ ← complex numbers under multiplication

$\downarrow \quad \nearrow \approx$

$\frac{G_1}{K}$

$\phi(r) = e^{2\pi r i}$

[Is it homomorphism.

$\phi(r_1 + r_2) = e^{2\pi r_1 i} \cdot e^{2\pi r_2 i}$

hence yes].

Kernel: $\{r \mid \phi(r) = 1\}$

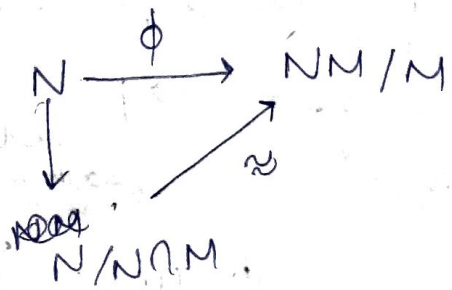
$\Rightarrow r \in N.$

$\therefore$ Proved.

✱

Eg: If N, M are normal subgroups of G_1.

P.T. NM/M is isomorphic to $N/N \cap M$.



homo-morphic

$\phi(n) = Mn$

$\phi(n_1 n_2) = Mn_1 n_2$

$\Rightarrow Mn_1 Mn_2 \Rightarrow \phi(n_1) \cdot \phi(n_2)$

Kernel: $\{n \in N \mid Mn = M\}$

That is $n \in M$

(as $Mn = M$ $\forall n \in M$)

$\therefore n \in N, M$

$\therefore n \in N \cap M$

Kernel: $N \cap M$.

hence proved.

Eg: Let G_1 be the grp of all non zero complex numbers under multiplication. $\bar{G}_1$ be the grp of all 2×2 matrices of the form $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ $\xrightarrow{\text{Mult.}}$ where not both a, b are 0.

Show that $G_1, \bar{G}_1$ are isomorphic.

Eg: P.T. Kernel is Normal Subgrp.

~~Statement~~:

$$\phi(g x g^{-1}) = \bar{e}$$

we need to prove the above

$$\phi(x) = \bar{e} \quad [x \in K]$$

$$\phi(x) \cdot \phi(g g^{-1}) = \bar{e}$$

$$[\phi(e) = \bar{e}]$$

$$\phi(g x g^{-1}) = \bar{e}$$

Mid 2 - End

Automorphism is a homomorphism of a group onto itself.

If G is a homomorphism to $\bar{G}$, then $\bar{G}$ is also a homomorphism to G.

$$G \simeq \bar{G}$$

$$\Rightarrow \bar{G} \simeq G.$$

$$\phi : G \to \bar{G}$$

then $\phi^{-1} : \bar{G} \to G$.

If $h_1, h_2 \in \bar{G}$

$$\phi^{-1}(h_1 h_2) = \phi^{-1}(\phi(h_1') \cdot \phi(h_2'))$$

$$\Rightarrow \phi^{-1}(\phi(h_1' h_2'))$$

$$\Rightarrow h_1' h_2'$$

$$\Rightarrow \phi^{-1}(h_1) \cdot \phi^{-1}(h_2).$$

so if G_1 is homomorphic to $\bar{G}_1$, $\bar{G}_1$ is also homomorphic to G_1. That is the reason (↳ Onto) why we assumed that there exists some element in G_1 which satisfies

$$\phi(g) = h'$$

$A(S) = S_3$ Symmetric Group.

~~A~~(G_1) ⇒ group of Automorphisms of G_1 onto itself

To prove: ~~A~~(G_1) is a subgroup of $A(S)$.

Consider 2 elements $T_1, T_2 \in A(G_1)$.

$$T_1(xy) = (T_1 x)(T_1 y)$$

$$T_2(xy) = (T_2 x)(T_2 y)$$

$$T_1 T_2 (xy) = T_1 (T_2 x)(T_2 y)$$

$$\Rightarrow (T_1 T_2 x)(T_1 T_2 y)$$

∴ If $T_1, T_2 \in A(G_1)$

Closure property.

If $T \in A(G_1)$

$T^{-1} \in A(G_1)$?

T^{-1} exists as $T \in A(S) \supset A(G_1)$

T is 1-1 & onto.

$$T(T^{-1}x)(T^{-1}y) = (TT^{-1})x\,(TT^{-1})y$$

$$T^{-1}(x)\,T^{-1}(y) = T^{-1}(xy)$$

$\Rightarrow xy$

We have proved $A(G)$ is a subgrp of $A(S)$

Now does this contain only the identity element?

Let $x_0 \in G$

G is Abelian

$$x_0 = x_0^{-1}$$

Choose a mapping T: $T(x_0) = x_0^{-1}$

where $T \neq I$.

$$T(xy) = (xy)^{-1}$$
$$= y^{-1}x^{-1}$$
$$= x^{-1}y^{-1}$$
$$= T(x)\,T(y)$$

Non Abelian:

$g \in G$, $T_g : G \to G$

$T_g x = g^{-1} x g \quad \forall x \in G$.

$x, y \in G$

$T_g x = g^{-1} x g$

T_g is onto

given $y \in G$

Let $x = gyg^{-1}$

$T_g(x) = g^{-1}xg$

$\Rightarrow g^{-1}(g.yg^{-1})g$

$\Rightarrow y$

Every y has a pre-image x.

$$T_g(x) = T_g(y)$$

$$g^{-1}xg = g^{-1}yg$$

$$\Rightarrow x = y$$

Let $x, y \in G$

$$T_g(xy) = g^{-1}(xy)g$$

$$\Rightarrow (g^{-1}xg)(g^{-1}yg) = (T_g x)(T_g y)$$

The group of such mappings T_g : Inner Automorphism.

$T_g, T_h \in I(G)$

$$xT_gT_h = (g^{-1}xg)T_h$$

$$= h^{-1}(g^{-1}xg)h$$

$$\Rightarrow (gh)^{-1}x(gh)$$

$$\Rightarrow xT_{gh}$$

Let there be a mapping ψ from

$$G \longrightarrow A(G).$$

$$\psi(g) = T_g$$

ψ is homomorphism:

$$\psi(gh) = T_{gh} = T_gT_h = \psi(g)\psi(h)$$

$\Rightarrow$ Kernel of ψ

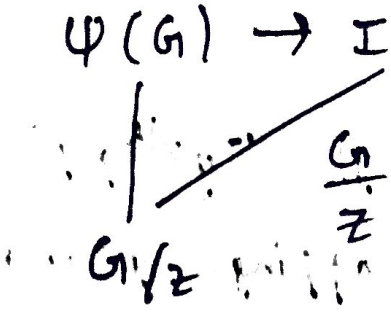
$$= \{g \in G \mid \psi(g) = I\}$$

$\psi(g) = T_g = I$.

$T_g(x) = g^{-1}xg = I_x = x$

$xg = gx$

$\therefore$ Kernel is the Center of the grp.



Eg: Integers ; $T_x = -x$. Is this Auto-morphism

$\pm$ Reals ; $T_x = x^2$ Is this Auto-morphism

Permutation group

S: set of mappings of n elements onto themselves.

A(S) ⇒ { group of all 1-1 mappings of S onto S }

S_3: $x_1 \to x_2$
$x_2 \to x_1$
$x_3 \to x_3$

$\begin{pmatrix} x_1 & x_2 & x_3 \\ x_2 & x_1 & x_3 \end{pmatrix}$ → Permutation

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

Let $\theta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$ $\psi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}$

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

$\psi\theta \Rightarrow \theta(\psi(1)) = \theta(1) = 3$

$\theta\psi = \psi(\theta(1)) = \psi(3) = 2$

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

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

$\boxed{\theta^3 = I}$

n elements: after n iterations, we get back θ.

but here (4 → 4) is redundant so θ^3.

Let S be a set

$\theta \in A(S)$.

ginen 2 elements $a, b \in S$

$a \equiv_\theta b$: if $b = a\theta^i$

($i \Rightarrow$ +ve or -ve or 0 $\Rightarrow$ integer)

[Read as a is congruent to b mod θ]

We can reach b from a ~~the~~ by iterating through θ i times.

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

$1 \equiv_\psi 3$

as $3 = (1)\psi^2$

$\psi(1) = 2 \quad \psi^2(1) = \psi(2) = 3$

Theorm : The above relation is an equivalence relation.

Reflexive: a should be congruent to a.

$a \equiv_\theta a$ if $a = a\theta^i$

$a \equiv a\theta^0$

∴ Reflexive

$f(x) = x$: Identity if $f(x)$ is defined $\forall x$:

else: fixed pt. mapping

Symmetric: if $a \equiv_\theta b$,

$a = b\,\theta^i$

$\because \theta \in$ group of mappings, inverse exists.

$\Rightarrow b = a\,\underbrace{\theta^{-i}}$

Inverse mapping : i times

Transitive: $a \equiv_\theta b$, $b \equiv_\theta c$

$b = a\,\theta^i$ $\quad c = b\,\theta^j$

$\Rightarrow (a\theta^i)\,\theta^j$

$\Rightarrow a\,\theta^{i+j}$

$\Rightarrow a \equiv_\theta c$

Orbit

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

Orbit of 1: $\underbrace{(1, 2)}$ cycle

Orbit of 3: (3)

Orbit of 4: (4 5 6).

Eg: given an Orbit; find the permutation

(1 2 3)

$$\zeta_\theta: \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 3 & 1 & 4 & 5 & 6 & 7 & 8 & 9 \end{pmatrix}$$

$C_1 : (5\ 6\ 4\ 1\ 8)$

$C_2 : \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 2 & 3 & 1 & 6 & 4 & 7 & 5 & 9 \end{pmatrix}$

Find the permutation which arises from C_1 followed by C_2.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 3 & 8 & 1 & 6 & 4 & 7 & 5 & 9 \end{pmatrix} \quad [C_1 C_2]$$

(Single cycle corresponding to both cycle).

$ Every permutation can be represented as a product of '2-cycles'.

An ordered pair is a 2 cycle.

2-cycles = Transpositions

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

$1 \to 2 \to 3 \to 1$

$1 \to 2 \to 1 \to 3 \to 1$

2 is going to 3 via 3

m cycle : $(1, 2 \ldots m) = (1\,2)(1\,3)\ldots(1\,m)$

this is not unique:

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

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

$3 \to 1 \to 3 \to 2 \to 3$

Eg: Find the Orbits and Cycles of following permutation:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 3 & 4 & 5 & 1 & 6 & 7 & 9 & 8 \end{pmatrix}$$

Orbit (1) = (1 2 3 4 5)

Orbit (8) = (8 9).

Orbit (6, 7) → (6 7)

Cycles: (1 2 3 4 5) (6) (7) (8 9)

⇒ Disjoint

Eg: Express the ~~above~~ below permutation as product of disjoint cycles;

Final Ans ↑

$\theta = (1\,5)\ (1\,6\,7\,8\,9)\ (4\,5)\ (1\,2\,3)$

$\textcircled{T} = T_1\ T_2\ T_3\ T_4$

$\because T(1) = T_1\ T_2\ T_3\ T_4(1)$

$\Rightarrow T_1\ T_2\ T_3(2) \Rightarrow T_1\ T_2(2) = 2$

$T(2) = 3 \quad T(3) = 6 \quad T(4) = 1 \quad T(5) = 4$

$T(6) = 7 \quad T(7) = 8 \quad T(8) = 9 \quad T(9) = 1$

$$T: \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 3 & 6 & 1 & 4 & 7 & 8 & 9 & 1 \end{pmatrix}$$

Eg: (1 2) (1 2 3) (1 2)

$T = T_1\ T_2\ T_3$

$T(1) = 3 \quad T(2) = 1 \quad T(3) = 2$

(1 3 2)

Eg: Find the cycle structure of all powers of $T: (1\ 2\ 3\ 4\ 5\ 6\ 7\ 8)$.

$T^2 = T \cdot T$

$T^2(1) = 3$ | $T^2(2) = 4$
$T^2(3) = 5$ | $T^2(4) = 6$
$T^2(5) = 7$ | $T^2(6) = 8$
$T^2(7) = 1$ | $T^2(8) = 2$

$\Rightarrow (1\ 3\ 5\ 7)(2\ 4\ 6\ 8)$

$T^3 = T \cdot T \cdot T$

$(4\ 7\ 2)(5\ 8\ 3\ 6\ 1)$

Even Permutations: Even no. of 2^{1}s cycles in representation

To see the effect of Odd permutation:

Define $P(x_1 x_2 x_3 x_4 x_5) = \prod_{i<j} (x_i - x_j)$

Let $\Rightarrow \theta(1\ 3\ 4)(2\ 5)$

$\theta = (1\ 3)(1\ 4)(2\ 5)$

Apply θ on P;

$P = (x_1 - x_2)(x_1 - x_3)(x_1 - x_4)(x_1 - x_5)$
$(x_2 - x_3)(x_2 - x_4)(x_2 - x_5)(x_3 - x_4)$
$(x_3 - x_5)(x_4 - x_5)$

If we permute over the indices

$$\theta = (1\ 3\ 4)(2\ 5)$$

$\theta(P)$ can be written as:

$$(x_3 - x_5)(x_3 - x_4)(x_3 - x_1)(x_3 - x_2)$$
$$(x_5 - x_4)(x_5 - x_1)(x_5 - x_2)(x_4 - x_1)$$
$$(x_4 - x_2)(x_1 - x_2).$$

Odd permutation changes the sign of the function.

Even perm. . Even perm $\Rightarrow$ Even permutation

Even . Odd = Odd

Alternating group:

S_n is a group of all mappings of n elements onto themselves.

[Each element is a permutation].

A_n: set of even permutation

A_n is a subgroup of S_n:

Closure: Even . Even = Even

Inverse: Inverse of an permutation exists and is also even.

No. of elements in A_n: $\frac{n!}{2}$

define ψ : $\psi(S_n) = W = \{1, -1\}$

$\psi(s) = 1$ s is even

$= -1$ s is odd

Is ψ homomorphic ?

E-E : $\psi(\underbrace{s_1 s_2}_{\text{Even}}) = 1 = \psi(s_1) \cdot \psi(s_2)$

$\psi(s_1 s_2) \to 1$, $\psi(s_1) \to 1$, $\psi(s_2) \to 1$

E-O : $\psi(s_1 s_2) = -1 = \psi(s_1) \cdot \psi(s_2)$

$\psi(s_1 s_2) \to -1$ (odd), $\psi(s_1) \to -1$, $\psi(s_2) \to 1$

O-O : $\psi(\underbrace{s_1 s_2}_{\text{Even}}) = \psi(s_1) \cdot \psi(s_2)$

$\psi(s_1 s_2) \to 1$, $\psi(s_1) \to -1$, $\psi(s_2) \to -1$

$\psi : S_n \to W$

$\frac{S_n}{A_W}$ $\xrightarrow{N}$ $\longrightarrow$ One-One Onto

So $O(W) = O\left(\frac{S_n}{A_W}\right)$

Kernel of S_n under ψ :

$\{ s \mid \psi(s) = 1 \}$

$\hookrightarrow$ Even permutations

$\therefore O\left(\frac{S_n}{A_n}\right) = 2$

$\Rightarrow O(A_W) = \frac{n!}{2}$

Eg: Compute

Inverse of a permutation: $S\begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ b_1 & b_2 & \cdots & b_n \end{pmatrix}$

$I_n: \begin{pmatrix} b_1 & b_2 & \cdots & b_n \\ a_1 & a_2 & \cdots & a_n \end{pmatrix}$ $\quad S.I_n = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ a_1 & a_2 & \cdots & a_n \end{pmatrix}$ → Identity

Eg: Find out $a^{-1}ba$

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

$b = (1\ 5\ 7\ 9)$

$a = \cancel{(3\ 5\ 2)} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 4 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix}$

$\Rightarrow \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 5 & 4 & 2 \end{pmatrix}$

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

$a^{-1} = (2\ 5\ 3\ 1)$

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

$b = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 2 & 3 & 4 & 7 & 6 & 9 & 8 & 1 \end{pmatrix}$

$a^{-1}ba = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 7 & 2 & 4 & 5 & 6 & 9 & 8 & 3 \end{pmatrix}$

$\Rightarrow (2\ 7\ 9\ 3)$

Eg: P.T. the smallest subgroup of S_n containing $(1,2)$ and $(1,2,\cdots n)$ is S_n.

Or in other words these cycles generate S_n.

We need to show, every transposition can be generated from the product of these cycles

$(n\ n-1\ \dots\ 2\ 1)(1\ 2)(1\ 2\ 3\ \dots\ n) = (2,3)$

$(n\ n-1\ \dots\ 3\ 2\ 1)(2\ 3)(1\ 2\ 3\ 4\ \dots\ n) = (3,4)$

$= (4,5)$

In this manner, I generated 2 cycles of the form $(i, i+1)$

So we got one type of 2-cycles

$(1\ 2)\ (2\ 3)\ (1\ 2)$

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

$= (1\ 3)$.

$(1\ 3)\ (3\ 4)\ (1\ 3)$

$\Rightarrow (1\ 4)$

$(1\ 4)\ (4\ 5)\ (1\ 4)$

$= (1\ 5)$

$(1\ n-1)\ (n-1,\ n)\ (1,\ n-1)$

$= (1,\ n)$.

$\Rightarrow (1, i)$ is done

$(1, i)\ (1, j)\ (i, 1)$

$\Rightarrow (i, j)$.

If $a, b \in G$, b is said to be conjugate to a if $\exists$ an element c such that

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

$$b \sim a$$

Conjugacy class: $C_a \Rightarrow \{c \mid a \sim c\}$

This is an equivalence relation.

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

Symmetric: $b = x^{-1} a x$

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

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

These belong to the group.

Symmetric

Transitive: $a \sim b$, $b \sim c$

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

$$b = y^{-1} c y$$

$$a = x^{-1} y^{-1} c y x$$

$$\Rightarrow (yx)^{-1} c (yx)$$

Transitive.

If C_a is the no. of elements in class of a;

Total Number of elements in G: $\sum_{a \in G} C_a$

dont count classes which have already come.

Normalizer of:

① An element: $N(a) = \{ x \in G_1 / xa = ax \}$

② A subgroup: $N(H) = \{ x \in G_1 / xh = hx \ \forall \ h \in H \}$

↳ centralizer

Center $N(G_1) = \{ x \in G_1 / xg = gx \ \forall g \in G_1 \}$

P.T. $N(a)$ is a subgroup.

Let $x, y \in N(a)$.

$ax = xa$, $ay = ya$

Closure: (xy) should belong to $N(a)$.

$axy = xya$.

$\Rightarrow (ax)y$

$\Rightarrow x(ay)$

$\Rightarrow xya$

Inverse: $x^{-1}a = ax^{-1}$

$xa = ax$

$a = x^{-1}ax$

$\underline{ax^{-1} = x^{-1}a}$

$\Rightarrow$ The cosets formed by the Normalizer form the conjugate class of an element

If G is a finite group

$$C_a = \frac{O(G)}{O(N(a))}$$

Method Pick 2 elements in the same right coset of $N(a)$ and show that they $\in C_a$.

Let $x, y \in$ same right coset of $N(a)$

$y = nx$ where $n \in N(a)$.

$na = an$.

$y^{-1} = (nx)^{-1} = x^{-1}n^{-1}$.

$y^{-1}ay = x^{-1}n^{-1}a\,nx$

$\Rightarrow x^{-1}n^{-1}nax$

$\Rightarrow x^{-1}ax$

$\Rightarrow x, y \in C(a)$

Claim-2 on the other hand if x, y are in diff right cosets of $N(a)$.

$$(x^{-1}ax) \neq (y^{-1}ay)$$

Suppose not:

$x^{-1}ax = y^{-1}ay$

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

$\Rightarrow yx^{-1} \in N(a)$.

$\Rightarrow$ contradiction.

Eg: S_3 : (12), (23), (13),
(123), (132), (1)(2)(3).

Find conj class of (12).

$C(1,2) = \{ b \in G \mid \exists\, (x)^{-1}(12)(x) = (12) \}$

Let $x = (12)$

$(12)^{-1}(12)(12) \Rightarrow (12)$.