Recall :

→ let X be a set. Then any bijection on X is called a permutation, of X.

→ Collection of all permutations of X forms a group w.r.t. the function composition.

→ If $X = \{1, 2, \ldots, n\}$, then permutation group on X has $n!$ elements. This permutation group is denoted by S_n.

Example : # $S_1 = \{e\}$.

$$S_2 = \left\{ \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \right\}.$$

$$S_3 = \left\{ \underbrace{\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}}_{= e}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\}.$$

~~Cyclic permutation~~ :

In general $\alpha \in S_n$, i.e. if $\alpha : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ is a bijection then
$$\alpha \equiv \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \alpha(1) & \alpha(2) & \alpha(3) & \cdots & \alpha(n) \end{pmatrix}.$$

~~Cyclic permutation~~

Inverse of a permutation

Let

$$\alpha = \begin{pmatrix} 1 & 2 & \cdots & n \\ \alpha(1) & \alpha(2) & \cdots & \alpha(n) \end{pmatrix} \in S_n .$$

Then

$$\alpha^{-1} = \begin{pmatrix} \alpha(1) & \alpha(2) & \cdots & \alpha(n) \\ 1 & 2 & & n \end{pmatrix}.$$

Example ;

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \in S_3$$

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

Cyclic permutation : Let $\{a_1, a_2, \ldots, a_n\} \subseteq \{1, 2, \ldots, m\}$

Then the permutation of type

$$a_1 \to a_2 \to a_3 \to a_4 \to \cdots \to a_{n-1} \to a_n \to$$

and the other elements of $\{1, 2, \ldots, m\}$ are fixed.

i.e.

$$\begin{pmatrix} a_1 & a_2 & a_3 & \cdots & a_{n-1} & a_n & i_1 & i_2 & \cdots & i_k \\ a_2 & a_3 & a_4 & \cdots & a_n & a_1 & i_1 & i_2 & \cdots & i_k \end{pmatrix}$$

where $i_t \in \{1, 2, \ldots, m\} \setminus \{a_1, a_2, \ldots, a_n\}$.

This permutation has an special notation:

$$(a_1\ a_2\ \cdots\ a_n).$$

Example: $(1\ 2\ 3\ 4) \in S_4$

$\Downarrow$

refers to the permutation

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

If $(a_1, a_2, \cdots, a_n)$ is a cyclic permutation, then we say this cycle has length n.

$$\boxed{(a_1\ a_2\ \cdots\ a_n)^{-1} = (a_n\ a_{n-1}\ \cdots\ a_1)}$$

Ex: Give an Example of a permutation, which is not cyclic.

Ex: List all 3-cycles, 4-cycles in S_4.

Def: Two cyclic permutations $(a_1 a_2 \cdots a_n)$, $(b_1 b_2 \cdots b_m)$ in S_k are said to be disjoint if no element in S_k appear in both $(a_1 a_2 - a_n)$, $(b_1 b_2 - b_m)$.

Example: $(4\ 5), (3\ 4\ 5) \in S_5$

are not disjoint.

$(2\ 3), (4\ 5) \in S_5$ are disjoint.

Ex: Any two disjoint permutations commute.

Thm: Every permutation $\sigma \in S_n$ can be written as product of disjoint cycles.

Proof: Choose $a_1 \in \{1, 2, \dots, n\}$.

$$a_1 \to \underset{\sigma(a_1)}{a_2} \to \underset{\sigma(a_2)}{a_3} \to \dots \to a_k \to \underset{\sigma(a_k)}{a_1}$$

$(a_1\ a_2 \dots a_k)$.

Choose $b_1 \in \{1, 2, \dots n\} \setminus \{a_1, a_2, \dots a_k\}$.

Then $$b_1 \to \underset{\sigma(b_1)}{b_2} \to \dots \to \underset{\sigma(b_{t-1})}{b_t} \to \underset{\sigma(b_t)}{b_1}$$

$(b_1 \dots b_t)$.

Choose $c_1 \in \{1, 2, \dots, n\} \setminus \{a_1, a_2, \dots a_k, b_1, b_2, \dots b_t\}$

and we continue this process until we exhaust all the elements of $\{1, 2, \dots, n\}$.

Illustrate.

$$\begin{pmatrix} 1 & \cancel{2} & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 7 & 5 & 4 & 6 & 1 \end{pmatrix} \in S_7.$$

$$\Downarrow$$

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

Recall:

$$S_3 = \{ e, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2) \}$$

Transposition:

A cyclic permutation of length 2 is called a transposition.

Ex: $(1\ 2)$, $(2\ 3)$, $(1\ 3) \in S_3$ are transposition

Result: Any permutation $\sigma \in S_n$ can be written as product of transpositions.

Proof: Since $\sigma \in S_n$ can be written as product of disjoint cycles. Hence it is sufficient to show that any cycle in S_n can be written as product of transpositions.

Let $(a_1\ a_2\ \cdots\ a_n) \in S_n$ be a cycle of length n.

Note that:

$$(a_1\ a_2 \cdots\ a_n) = (a_1\ a_n)(a_1\ a_{n-1}) \cdots (a_1\ a_2).$$

Example:

Write $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 7 & 5 & 4 & 6 & 1 \end{pmatrix} \in S_7$ as product of transpositions.

$$\underline{(1\ 2\ 3\ 7)}\ (4\ 5)\ \underbrace{(6)}_{\text{identity}}.$$

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

Def: $\sigma \in S_n$ is said to be an even permutation if σ is a product of even no. of transpositions.

$\sigma \in S_n$ is said to be an odd permutation if σ is a product of odd permutation.

Example: $\overset{\text{identity}}{e} \in S_n$

$$e = \underline{(1\ 2)(2\ 1)}$$

e is an even permutation.

Permutation in above example is even.

Ex: Give an example of odd permutation.

Thm: let A_n be the collection of all even permutations of S_n. Then A_n is a group, called Alternating group. Moreover, $|A_n| = \frac{n!}{2}$.

Proof: let $\sigma, \tau \in S_n$ be even permutations.

Then $\sigma \cdot \tau$ is also an even permutation, since number of transpositions appear in $\sigma \cdot \tau$ will be same as no. of transpositions in σ + no. of transpo. in τ.

even + even = even.

let $\sigma = (a_1 a_2)(a_3 a_4) \cdots (a_{n-1}, a_n)$

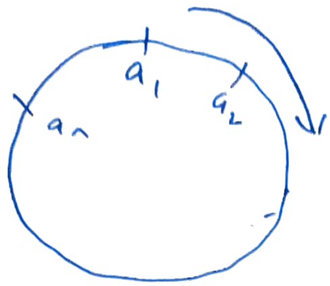
then $\sigma^{-1} = (a_{n-1} a_n)^{-1} \cdots (a_1 a_2)^{2}$

$= (a_{n-1} a_n) \cdots (a_1 a_2)$

So, If σ is even permutation hence σ^{-1} is also even permutation.

Recall: cyclic permutation; $\sigma = (a_1\, a_2 \cdots a_n) \in S_m$

means;



$\sigma(a_1) = a_2,\ \sigma(a_2) = a_3$
$\cdots\ \sigma(a_n) = a_1$

$a_1 \to a_2 \to a_3 \to \cdots \to a_n$

$$\sigma = \begin{pmatrix} a_1 & a_2 & \cdots & a_n & i_1 & i_2 & \cdots & i_k \\ a_2 & a_3 & \cdots & a_1 & i_1 & i_3 & \cdots & i_k \end{pmatrix}$$

$i_t \in \{1, 2, \ldots, m\} \setminus \{a_1, a_2, \ldots, a_n\}$.

Result: let $\alpha = (a_1\, a_2 \cdots a_m) \in S_k$ be a cyclic permutation of length m. Then $O(\alpha) = m$.

$$\alpha = (a_1\, a_2 \cdots a_m)$$

$\Rightarrow\ \alpha(a_1) = a_2,\ \alpha(a_2) = a_3 \cdots,\ \alpha(a_n) = a_1$

$\alpha^2 = (a_1\, a_2 \cdots a_m)^2 = ?$

$\alpha^2(a_1) = \alpha\,\alpha(a_1) = \alpha(a_2) = a_3$

$\alpha^2(a_2) = a_4,\quad \alpha^2(a_3) = a_5 \cdots,\ \alpha^2(a_{n-1}) = a_1$

$\alpha^2(a_n) = a_2$.

Note ~~that~~ in this example
~~it's not a left coset~~, a ~~right~~ coset

Applying 'α' m - times, we get

$$\alpha^m(a_1) = a_1, \quad \alpha^M(a_2) = a_2$$
$$\ldots \quad \alpha^m(a_m) = a_m$$

$\Rightarrow \quad O(\alpha) \leq m$

If $\quad O(\alpha) = s \not\leq m$, then

$$e(a_1) = \alpha^s(a_1) = a_1 \Rightarrow \alpha^s(a_1) = \alpha^{s-1}\alpha(a_1) = \alpha^{s-1}(a_2)$$
$$= \alpha^{s-2}(a_3) \ldots \alpha(a_s) = a_{s+1}$$

But $\quad a_1 \neq a_{s+1}$.

Hence $\quad O(\alpha) = m.$

Example: What is the order of

$$\sigma = (1 \ 3 \ 5) \in S_5$$

$O(\sigma) = 3,$

Ex: Find order of each element of S_3

$$S_3 = \{(1), (12), (13), (23), (123), (132)\}$$

(1)	(12)	(13)	(23)	(123)	(132)
1	2	2	2	3	3

Ex: Compute:

Let $\sigma = (1\ 3\ 5\ 7)$, $\tau = (2\ 3\ 7) \in S_7$

Compute: $\sigma\tau$ and $\tau\sigma$

σ^2:

$\sigma\tau = (1\ 3\ 5\ 7)(2\ 3\ 7)$

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

$\tau\sigma = ?$

$o(\sigma) = 4$, $o(\tau) = 3$.

Result: Let $\sigma \in S_n$. Further assume $\sigma = \alpha_1 \alpha_2 \cdots \alpha_k$ where α_i's are disjoint cycles.

Then $o(\sigma) = \text{lcm}(o(\alpha_1), o(\alpha_2), \ldots, o(\alpha_k))$

Ex: $o(\sigma\tau) = \text{lcm}(3, 4) = 12$.

Cosets:

Let G be a group, and H be a subgroup of G. Define a left of H in G with representative $g \in G$ to be the set;

$$gH = \{gh : h \in H\}.$$

Similarly, right cosets are defied as (with representative $g \in G$):

$$Hg = \{hg : h \in H\}.$$

Convention: If all left cosets and right cosets coincide then we use the word coset.

Example: $G = \mathbb{Z}_6$, $H = \{0, 3\}$

What are all left cosets?

$$0 + H = H = \{0, 3\} = 3 + H$$

$$1 + H = \cancel{4+H}\ \{1, 4\} = 4 + H$$

$$2 + H = \{2, 5\} = 5 + H.$$

Exercise: Show that these are also all right cosets of H in G.

Example: $G = S_3$

> **Note that**: if $h \in H$ then $hH = Hh = H$.
> $\Downarrow$
> **Exercise**

$H = \{(1), (1\,2\,3), (1\,3\,2)\}$

Left cosets:

$(1)H = H = (1\,2\,3)H = (1\,3\,2)H = \{(1), (1\,2\,3), (1\,3\,2)\}$

$(1\,2)H = (1\,3)H = (2\,3)H = \{(1\,2), (1\,3), (2\,3)\}$

Right cosets:

$H(1) = H = H(1\,2\,3) = H(1\,3\,2) = H = \{(1), (1\,2\,3), (1\,3\,2)\}$

$H(1\,2) = H(1\,3) = H(2\,3) = \{(1\,2), (1\,3), (2\,3)\}$

Example: $G = S_3$, $H = \{(1), (1\,2)\}$

Left cosets:

$(1)H = (1\,2)H = H = \{(1), (1\,2)\}$

$(1\,3)H = (1\,2\,3)H = \{(1\,3), (1\,2\,3)\}$

$(2\,3)H = (1\,3\,2)H = \{(2\,3), (1\,3\,2)\}$.

Right cosets: $H(1) = H(1\,2) = H = \{(1), (1\,2)\}$

$H(1\,3) = H(1\,3\,2) = \{(1\,3), (1\,3\,2)\}$

$H(2\,3) = H(1\,2\,3) = \{(2\,3), (1\,2\,3)\}$.

So, a left coset may not be a right coset.

Thm: Let H be a subgroup of a group G. Then left cosets of H in G is a partition of G. In other words, any two left cosets of H in G is either disjoint or same, and the union of all left cosets is G.

Proof: (1) Let $g_1 H$ and $g_2 H$ be two left cosets of H in G. We show that either

$$g_1 H = g_2 H \quad \text{or} \quad g_1 H \cap g_2 H = \phi .$$

Let $g_1 H \cap g_2 H \neq \phi$. Claim: $g_1 H = g_2 H$.

Note that $g_1 H \cap g_2 H \neq \phi \Rightarrow \exists\, x \in g_1 H \cap g_2 H$.

$\Rightarrow \quad x = g_1 h$ and $x = g_2 h'$ for some $h, h' \in H$.

$\Rightarrow \quad g_1 h = g_2 h' \Rightarrow g_1 = g_2 h' h^{-1}$

$\Rightarrow g_1 \in g_2 H$

Now, let $a \in g_1 H \Rightarrow a = g_1 h''$

$= g_2 h' h^{-1} h''$

$\Rightarrow \quad a \in g_2 H$

$\Rightarrow \boxed{g_1 H \subseteq g_2 H}$

Similarly, we can show that $g_2 H \subseteq g_1 H$, and hence

$\boxed{g_1 H = g_2 H}$

Similar, result hold for right cosets.

Thm: Let H be a subgroup of a group G. Then the number of left cosets of H in G is the same as number of right cosets of H in G.

Proof:

L_H := Collection of all left cosets of H in G.

R_H := Collection of all right cosets of H in G.

Claim: $|L_H| = |R_H|$.

To show this we define a map from L_H to R_H which is a bijection.

Define:

$$\phi : L_H \longrightarrow R_H$$

$$\phi(gH) = Hg^{-1}.$$

ϕ is well-defined:

Let; $gH = g'H \Rightarrow Hg'^{-1} = Hg^{-1}$ (follows from result).

$$\Rightarrow \phi(gH) = \phi(g'H).$$

ϕ is 1-1:

$$\phi(g_1H) = \phi(g_2H)$$

$$\Rightarrow Hg_1^{-1} = Hg_2^{-1}$$

$$\Rightarrow g_1H = g_2H$$ (Follows from Lemma).

ϕ is onto:

Let $Hg \in R_H$, but then

Choose $\phi(g^{-1}H) = Hg$

Hence ϕ is onto and $|L_H| = |R_H|$.

//

Thm: Let H be a subgroup of a group G. Then the number of elements in any two left cosets is same.

Pf: Let gH and $g'H$ be two left cosets.

Claim: $|gH| = |g'H|$.

To show this fact, it is sufficient to show that the number of elements in any left coset xH is same as the number of elements in H.

Define a map;

$$\phi : H \longrightarrow xH \text{ as}$$

$$\phi(h) = xh.$$

Claim: ϕ is one-one and onto.

ϕ is one-one:

$$\phi(h) = \phi(h') \Rightarrow xh = xh' \Rightarrow h = h'.$$

ϕ is onto:

let $xh \in xH$, but then $\phi(h) = xh$.

Hence $|H| = |xH|$ and so $|g_1H| = |g_2H| = |H|$.

Def: Let G be a group and H be a subgroup of G. Then the index of H in G, ~~is~~ is the number of left (right) cosets of H in G. The index of H in G is denoted by $[G : H]$.

Example $G = \mathbb{Z}_6$, $H = \{0, 3\}$ $[G : H] = 3$.

Lagrange's thm

Theorem: Let G be a finite group and H be a subgroup of G. Then $O(H) = |H|$ is a divisor of $O(G)$ (or $|G|$).

Proof:

Let $a_1H, a_2H, \ldots, a_tH$ be the distinct left cosets of H in G. We know;

(1) $G = a_1H \cup a_2H \cdots \cup a_tH.$

(2) $|a_1H| = |a_2H| = \cdots = |a_tH| = |H|.$

(3) Since a_iH are distinct, so $a_iH \cap a_jH = \phi$ $i \neq j$.

$$\Rightarrow |G| = \sum_{i=1}^{t} |a_iH| = \sum_{i=1}^{t} |H| = t \cdot |H|$$

$$\Rightarrow |G| = t \cdot |H|$$

Hence proved.

Moreover, $[G:H] = \dfrac{O(G)}{O(H)}$.

Cor: Every group of prime order is cyclic.

Proof: Let G be a group with $|G| = p$, p being a prime number

~~Similar~~

Let $a (\neq e) \in G$. Consider $H = \langle a \rangle$. Since only divisors of p are 1, and p so $|H| = |\langle a \rangle| = 1$ or p.

But since, $a \neq e$ so, $|\langle a \rangle| = p$.

$\Rightarrow \langle a \rangle = G$ and so G is cyclic.

Thm: If G is a finite group and $a \in G$, then

$$O(a) \mid O(G).$$

Proof: Let $H = \langle a \rangle$. Then $O(H) = O(a)$.

So, $O(H) \mid O(G) \Rightarrow O(a) \mid O(G)$.

Thm: If G ~~be~~ is a finite group of order n, then $a^n = e \ \forall a \in G$.

Pf: We have $O(a) \mid O(G)$.

So if $O(a) = m \Rightarrow n = mt$

$$\Rightarrow a^n = a^{mt} = (a^m)^t = e^t = e$$

\#

Normal Subgroup

Def: Let G be a group and H be a ~~not~~ subgroup of G. H is said to be a normal subgroup of G if

$\forall g \in G, \forall h \in H, \quad ghg^{-1} \in H.$

Example: (1) Any subgroup of abelian group is normal.

Why? $g \in G, \quad h \in H$

$\Rightarrow ghg^{-1} = gg^{-1}h = h \in H.$

$\Rightarrow H$ is normal in G.

(2) For any group G. $\{e\}$ and G are normal in G.

(3) A_n is a normal subgroup of S_n.

$\sigma \in S_n, \quad \tau \in A_n$

$\Rightarrow \sigma\tau\sigma^{-1}$ is always an even permutation.

(4) Every subgroup of Q_8 is normal in Q_8.

Illustration :

$$H = \{\pm 1\}.$$

$x \in G$, $\quad x \cdot -1 \cdot x^{-1} = 1 \qquad x = \pm i, \pm j, \pm k.$

Theorem:

Result: H is a normal subgroup of G

iff

$\forall g \in G$, $gHg^{-1} = H$, where

$gHg^{-1} = \{ghg^{-1} : h \in H\}.$

Pf:
Fix, $g \in G$. Since H is normal in G.

$ghg^{-1} \in H \quad \forall h \in H$

$\Rightarrow gHg^{-1} \subseteq H.$

Now, if $h \in H$, then consider the element, $g^{-1}hg \in H.$

But then $g \underline{g^{-1}hg} g^{-1} = h \in gHg^{-1}$

Hence, $H \subseteq gHg^{-1}.$

So, $\boxed{gHg^{-1} = H}$

We have seen that a left coset may not be same as a right coset.

Result: The subgroup H of G is a normal subgroup iff every left coset of H in G is a right coset of H in G.

Pf: Let H be normal in G.

$$\Rightarrow gHg^{-1} = H$$

$$\Rightarrow gHg^{-1}g = Hg$$

$$\Rightarrow gH = Hg$$

Conversely, Suppose, every left coset is also a right coset. Let gH be a left coset, then

i.e. $gH = Hk$ for some $k \in G$.

However, note that $g \in gH$, so $g \in Hk$.

Also, $g \in Hg$.

But, we know that any two right cosets are either disjoint or identical.

Hence $Hk = Hg$ and so

$$gH = Hg \Rightarrow gHg^{-1} = Hgg^{-1} = H$$

$$\Rightarrow gHg^{-1} = H \quad \forall g \in G$$

$\Rightarrow$ H is normal

Result: Let $A, B \subseteq G \to$ group.

Define. $A \cdot B = \{ a \cdot b ; \ a \in A, b \in B \}$.

Observation. $H \cdot H = H$, where H is a subgroup of G.

Clearly, $H \subseteq H \cdot H$, since if $h \in H$

then $h \cdot e \in H \cdot H$.

Moreover, closure property imply that if

$h_1 h_2 \in H \cdot H$, so $h_1 h_2 \in H$

Hence $H \cdot H \subseteq H$ and so $\boxed{H \cdot H = H}$

Result: A subgroup H of G is a normal subgroup of G iff the product of two right cosets of H in G is again a right coset of H in G.

Pf: Let H be a normal subgroup of G.

$\Rightarrow \forall g \in G, \quad gH = Hg$

Let Hx and Hy be two right cosets of H in G.

So, $Hx \, Hy = H(xH)y = HHxy = Hxy$.

Conversely,

Assume $\forall g_1, g_2 \in G \quad Hg_1 Hg_2 = Hg_1g_2$.

We show that H is normal in G.

To show this, it is sufficient to show that $\forall x \in G, \quad xH = Hx$.

~~Let $a \in xH$. Now, $x^{-1} \in x^{-1}H$~~

Let $a \in Hx$. Now, $x^{-1} \in Hx^{-1}$

$\cancel{\Rightarrow ax^{-1} \in HxHx^{-1} = HxHx^{-1} \neq H}$

$\cancel{\Rightarrow ax^{-1} \in H}$

$\cancel{\Rightarrow ax^{-1} = h \text{ for some } h \in H}$

$\cancel{\Rightarrow a = hx}$

$\Rightarrow \quad x^{-1}a \in Hx^{-1}Hx = H$

$\Rightarrow \quad x^{-1}a = h$ for some $h \in H$

$\Rightarrow \quad a = xh \Rightarrow a \in xH$

$\Rightarrow \quad \boxed{Hx \subseteq xH}$

Similarly, show that $\boxed{xH \subseteq Hx}$

Hence $xH = Hx$ and so H is normal in G.