Recap :

1. $\phi \in S_n$

$$\phi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 2 & 4 & 1 & 3 \end{pmatrix} \equiv (1243) = (2431) = (4312) \cdots$$

$$(132)(1243) = (1)(24)(3) = (24)$$

2. $\phi \in S_n$ unique cycle decomposition

$\downarrow$

complete fact. into

disjoint cycles

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = (12)(34) = \cancel{(12)(34)[(34)(34)]}$$

3. Why S_n?

Cayley's theorem.

G is a subgroup of S_G

$\forall a \in G.$ $\quad L_a : G \to G$

$\qquad\qquad x \mapsto ax$

$$\left(\begin{array}{c} G = \{g_1, g_2, \cdots g_n\} \\ L_a G = \{ag_1, ag_2, \cdots ag_n\} \end{array} \right)$$

$$L_a \cdot L_a = L_{ab}$$

$$L : G \to \operatorname{im} G \subset S_G$$

$$a \to L_a$$

T "regular representation" of S_4. see e.g. Zee.

Consider S_n, n-dim carrier space V

$\vec{e}_i = \{0\ 0 \cdots \underset{i\text{-th}}{1}\ 0, 0\ 0\}^T \qquad V = \mathrm{span}\{\vec{e}_i\}$

$\phi \in S_n: \qquad T(\phi): \vec{e}_i \to \vec{e}_{\phi(i)}$

$$T(\phi)\vec{e}_i = \sum_{j=1}^{n} A(\phi)_{ji}\, \vec{e}_j \qquad A \in GL(n, K)$$

non-zero element $(i, \phi(i))$

		e	a	b	c
1	e	e	a	b	c
2	a	a	e	c	b
3	b	b	c	e	a
4	c	c	b	a	e

$\phi: V \to \mathrm{im}(V) \subset S_4$

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

$$T(a) = \begin{pmatrix} \begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix} & 0 \\ 0 & \begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix} \end{pmatrix}$$

4. generators of S_n.

$$(1\ 2 \cdots r) = (1\ r)(1\ r-1)\cdots(1\ 2)$$

① $\{(1\ r)\ (r \le n)\}$

② $\{\sigma_i := (i, i+1)\}$

③ $\{(1\ 2), (1\ 2 \cdots n)\}$

even / odd permutations

$$\mathrm{sgn}: S_n \to \mathbb{Z}_2$$
$$\phi \mapsto \mathrm{sgn}(\phi) \in \{\pm 1\}$$

1. $\phi = \tau_1 \cdots \tau_t \in S_n$ $\quad \tau_i$: cycles

$$\boxed{\mathrm{sgn}(\phi) = (-1)^{n-t}}$$

2. $\mathrm{sgn}(\sigma_1) = -1 \qquad \sigma_1 = (12)$

3. product of transposition & permutation

$$\mathrm{sgn}(\sigma\phi) = -\mathrm{sgn}(\phi)$$

$\sigma = (ij)$

(a) $(ij)(i a_1 a_2 \cdots a_k j b_1 b_2 \cdots b_l) = (i a_1 a_2 \cdots a_k)(j b_1 \cdots b_l)$

$$\begin{cases} i \mapsto a_1 \to a_1 \\ a_i \mapsto a_{i+1} \mapsto a_{i+1} \\ a_k \mapsto j \mapsto i \end{cases}$$

$$\begin{cases} j \mapsto b_1 \mapsto b_1 \\ b_i \mapsto b_{i+1} \\ b_l \mapsto i \mapsto j \end{cases}$$

(b) $(ij)(i a_1 \cdots a_k)(j b_1 b_2 \cdots b_l) = $ LHS $\overset{(ij)\cdot}{\longleftarrow}$ (a)

4. $\mathrm{sgn}(\phi_1 \phi_2) = \mathrm{sgn}(\phi_1)\,\mathrm{sgn}(\phi_2)$

3 $\to$ 4 : $\phi_1 = \sigma_1 \sigma_2 \cdots \sigma_k$

5: 4 shows that $\underline{sgn}$ is a homomorphism

$$sgn: \quad S_n \longrightarrow \mathbb{Z}_2$$
$$\phi \longmapsto sgn(\phi)$$

($\epsilon_{ijk} = sgn(ijk)$ in physics)

<u>Definition</u>: The <u>Alternating group</u> $A_n \subset S_n$ is the subgroup of S_n of <u>even</u> permutations.

$$sgn(\phi) = 1, \quad \forall \phi \in A_n$$

1. odd is a subgroup ?

2. $A_2 = \{1\}$

   $A_3 = \{1, (123), (132)\}$

   $|A_n| = |S_n|/2 = n!/2$

   $A_4 = \{1,$
   $(123), (132),$
   $(124), (142)$
   $(134)\ (143)$
   $(234)\ (243)$ } 8

   $(12)(34), (13)(24)$
   $(14)(23) \}$

   $|A_4| = 12$

3. A_3 is Abelian $A_3 \cong \mathbb{Z}_3 \cong \mu_3$

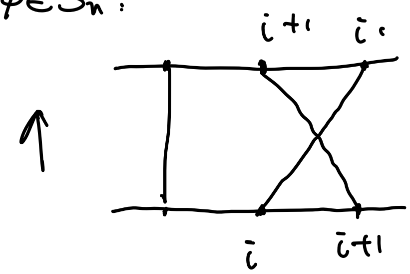
A_6 is not Abelian.

$$(123)(124) = (13)(24)$$

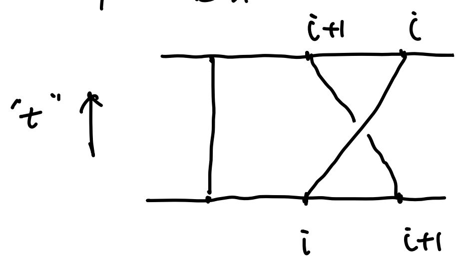
$$(124)(123) = (14)(23)$$

- Symmetric group & braiding group

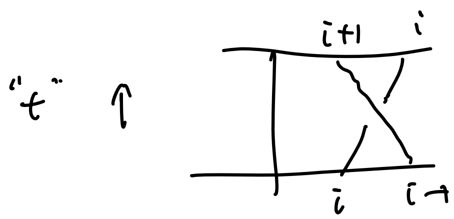
$\phi \in S_n$:



$\tilde{\phi} \in B_n$ $\quad \tilde{\sigma}(i) = (\widetilde{i, i+1})$

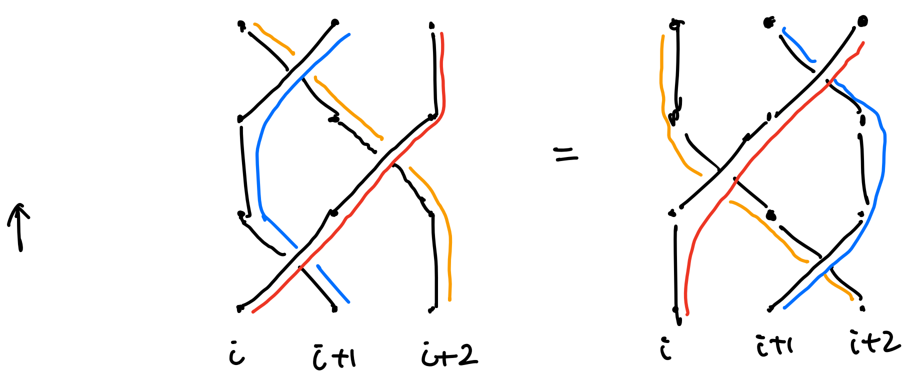


$\tilde{\sigma}(i)^{-1}$



① $\tilde{\sigma}_i \tilde{\sigma}_j = \tilde{\sigma}_j \tilde{\sigma}_i \quad (|i-j| \geq 2)$

② $\tilde{\sigma}_i \tilde{\sigma}_{i+1} \tilde{\sigma}_i = \tilde{\sigma}_{i+1} \tilde{\sigma}_i \tilde{\sigma}_{i+1}$



difference between σ_i & $\tilde{\sigma}_i$

$\sigma_i^2 = 1 \qquad \tilde{\sigma}_i^2 \neq 1$

$$S_n = \langle \sigma_1 \cdots \sigma_{n-1} \mid \sigma_i \sigma_j \sigma_i^{-1} \sigma_j^{-1} = 1 ,\ |i-j| \geq 2$$

$$\sigma_i \sigma_{i+1} \sigma_i = \sigma_{i+1} \sigma_i \sigma_{i+1} ,$$

$$\sigma_i^2 = 1 \ \rangle$$

$$B_n = \langle \tilde{\sigma}_1 \cdots \tilde{\sigma}_{n-1} \mid \tilde{\sigma}_i \tilde{\sigma}_j \tilde{\sigma}_i^{-1} \tilde{\sigma}_j^{-1} = 1 . \quad |i-j| \geq 2$$

$$\tilde{\sigma}_i \tilde{\sigma}_{i+1} \tilde{\sigma}_i = \tilde{\sigma}_{i+1} \tilde{\sigma}_i \tilde{\sigma}_{i+1} \ \rangle \qquad (\tilde{\sigma}_i^2 \neq 1)$$

Topological quantum computing

$$\phi : B_n \longrightarrow S_n \qquad \text{homo.}$$

$$\tilde{\sigma}_i \longmapsto \sigma_i$$

6. Cosets and conjugacy

6.1. Cosets and Lagrange theorem

Definition: Let $H \subset G$ be a subgroup.

The set

$$gH := \{gh \mid h \in H\} \subset G$$

is a left-coset of H.

(right-coset $Hg = \{hg \mid h \in H\}$)

$g \in G$ is a representative of gH (Hg)

Example. ① $G = \mathbb{Z}$. $H = n\mathbb{Z}$

$$g + H = \{g + n \cdot r \mid r \in \mathbb{Z}\}$$
$$= \{i \mid i \equiv g \bmod n\}$$

$n = 2$ H & $H+1$

② $G = S_3$ $H = S_2 = \{1, (12)\} \subset S_3$

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

gH: $1 \cdot H = H$

$(12)H = \{(1\,2), 1\} = H$

$(13)H = \{(13), (123)\}$

$$(23)H = \{(23), (132)\}$$

$$(123)H = \{(123), (123)(12) = (13)\}$$

$$(132)H = \{(132), (23)\}$$

[$L \neq R$: $\quad H(123) = \{(123), (23)\} \neq (123)H$]

Observation: The (left) cosets are either the same or disjoint.

[seen as group action: "X" $= G$

"G" $= H$

right action of H on G.

$$G \times H \longrightarrow G$$

$$(g, h) \longmapsto gh.$$]

Proof: suppose $g \in g_1 H \cap g_2 H$ then

$$g = g_1 h_1 = g_2 h_2 \qquad h_i \in H$$

$$g_1 = g_2 h_2 h_1^{-1} = g_2 h \qquad h = h_2 h_1^{-1} \in H$$

$$\Rightarrow g_1 \cdot H = g_2 H \qquad (\text{not } g_1 \cdot h = g_2 h)$$

Left cosets define an equivalence relation.

$$g_1 \sim g_2 \quad \text{if } \exists h \in H. \text{ s.t. } g_1 = g_2 h$$

$$(g_1 H = g_2 H)$$

Theorem (Lagrange): If H is a subgroup of a finite group G, then

$|H|$ divides $|G|$.

Proof. $|g_i H| = |H|$ $\forall g_i \in G$, and

$G = \bigcup_{i=1}^{m} g_i H$, m is the number of distinct cosets

$\Rightarrow |G| = m|H|$

Corollary. if $|G| = p$ is a prime. then G is a cyclic group.

$G \cong \mu_p \cong \mathbb{Z}_p$

Proof. pick a $g \in G$. s.t. $g \neq 1$

$H = \langle g \rangle = \{1, g, g^2 \cdots\}$

$|H| \,\Big|\, |G| \Rightarrow |H| = p \Rightarrow G = H.$

Corollary (Fermat's little theorem)

a integer. p. prime

$a^p = a \mod p.$

Definition. G a group. H subgroup.

The set of left cosets in G is denoted G/H

It is the set of orbits under the right group action of H on G.

It is also referred to as a homogeneous space.

The cardinality of G/H is the index of H in G. denoted

$$[G : H] \quad \left(= |G|/|H| \right)$$

Example. 1. $G = S_3 \qquad H = S_2$

$$G/H = \{ H,\ (123)H,\ (132)H \}$$

$$[G : H] = 6/2 = 3$$

2. $G = \langle w \mid w^{2N} = 1 \rangle \qquad H = \langle w' \mid w'^{N} = 1 \rangle$

$$w = e^{i\frac{\pi}{N}} \qquad\qquad w' = e^{i\frac{2\pi}{N}}$$

$$[G : H] = 2 \qquad G/H = \{ H,\ wH \}$$

3. $G = A_6 \quad H = \{1, (12)(34)\} \cong \mathbb{Z}_2$

$[G : H] = 6$

? is there an H s.t. $[G : H] = 2$?

if H exists. $G/H = \{H, gH\}$ $(H \neq gH)$
$(g \notin H)$

① if $g^2H = gH \Rightarrow gH = H \Rightarrow g \in H$ ×

② $g^2 H = H \Rightarrow g^2 \in H$

$\Rightarrow$ regardless of $g \in H$ or not, $g^2 \in H$. now consider 3-cycles

$((23)(123) = (132) \Rightarrow$ 3-cycle is the square of another 3-cycle

there are $\underline{8}$ 3-cycles in A_4

$(8 > 6)$

$\Rightarrow$ No $|H| = 6$

Converse of Lagrange theorem is usually not true..

A special case:

Theorem (Sylow's first theorem). Suppose p is prime and p^k divides $|G|$ for $k \in \mathbb{N}^+$

Then there is a subgroup of order p^k

Example.

① S_3 $|S_3| = 6 = 2 \times 3$

2: $S_2 \cong \mathbb{Z}_2$

3: $A_3 \cong \mathbb{Z}_3$

② $|Q| = 8 = 2^3$

$|H| = 2$: $\{\pm 1\}$

$|H| = 4$: $\{1, -1, i, -i\}$

$j, -j$

$k, -k$

$|H| = 8$ Q

6.2 Conjugacy

Definition (a) a group element h is conjugate to h'

$\exists g \in G$. s.t. $h' = g h g^{-1}$

(b) conjugacy defines an equivalence relation.

The equivalence class is called the

conjugacy class (of h)

$C(h) := \{ g h g^{-1} : \forall g \in G \} \left(=: h^G\right)$

(c) $H \subset G$ is a subgroup. its conjugate

$H^g := gHg^{-1} = \{ghg^{-1} : h \in H\}$ is also a subgroup

① $e \in H^g$ $\quad geg^{-1} = e$

② $(gh_1g^{-1})(gh_2g^{-1}) = g(h_1h_2)g^{-1} \in H^g$

③ $I(gh_1g^{-1}) = gh_1^{-1}g^{-1} \in H^g$