Recap :

1. equivariant map. $f: X \to X'$

$$\begin{tikzcd} X \arrow[r, "f"] \arrow[d, "g"'] & X' \arrow[d, "g"] \\ X \arrow[r, "f"'] & X' \end{tikzcd}$$

$f(g\cdot x) = g\, f(x)$

2. Symmetric group S_n

$$\phi = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ p_1 & p_2 & \cdots & & p_n \end{pmatrix} \qquad p_i = \phi(i)$$

ex. $\phi \in S_4$ $\quad \phi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = (1\,2\,3\,4)$

3. canonical rep.

$\dim V = n.$ $\quad \hat{e}_i = \{0, 0, \cdots 1, 0, \cdots\}$
$\phantom{\dim V = n. \quad \hat{e}_i = \{0, 0, \cdots} i\text{th}$

$$\tau_\phi(\hat{e}_i)\Big(\equiv \sum_j A_{ji}\, \hat{e}_j\Big) \equiv \hat{e}_{\phi(i)}$$

$$A_{ji} = \hat{e}_j^T \hat{e}_{\phi(i)} = \delta_{j,\phi(i)}$$

4. $\phi. \xrightarrow{\text{cycle decomp.}} (1)(234)(5)\cdots$ $\quad$ unique $\forall \phi$

transposition decomp.

$$(a_1 a_2 \cdots a_r) = (a_1 a_r)(a_1 a_{r-1}) \cdots (a_1 a_2)$$

generators :

① $\sigma_i = (i. \ i+1)$

② (12) & $(12 \cdots n)$

5. transposition decomp. not unique.

but even & odd unique

<u>Definition</u> A permutation $\phi \in S_n$ is even (odd) if it is a product of even (odd) transpositions. ("Parity")

(equivalent)

<u>Definition</u>. If $\phi = \sigma_1 \cdots \sigma_t \overset{\in S_n}{\vee}$ is a complete factorization into disjoint cycles (signum)

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

cycle decomp. is unique $\Rightarrow$ sgn is well-defined

$(123) \in S_3$

- $sgn((123)) = (-1)^{3-1} = 1$ even.

- $S_6 \ni \phi = (123)(45) = (123)(45)(6)$ $n=6$, $t=3$

  $sgn = (-1)^3 = -1$

- transposition $\tau = (ij)$ $t = n-1$ $sgn(\tau) = (-1)^1 = -1$

- r-cycle. $t = (n-r)+1$ r odd $\Leftrightarrow$ even perm, even $\Leftrightarrow$ odd.

  $sgn\ \phi = (-1)^{n-t} = (-1)^{r+1}$

- $sgn(\tau\phi) = sgn(\tau)\, sgn(\beta)$ actually

  $sgn(\alpha\beta) = sgn(\alpha)\, sgn(\beta)$

We can define a homomorphism:

$$\begin{aligned} sgn: \ S_n &\longrightarrow \mathbb{Z}_2 \\ \phi &\longmapsto sgn(\phi) \end{aligned}$$

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

$sgn(\phi) = 1$. $\forall \phi \in A_n$

① odd is a subgroup ?

② $A_2 = \{1\}$

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

$A_4 = \{1,$
$(123), (132),$
$(124), (142)$
$(134)\ (143)$
$(234)\ (243)$ } 8
$(12)(34), (13)(24)$
$(14)(23)$ }

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

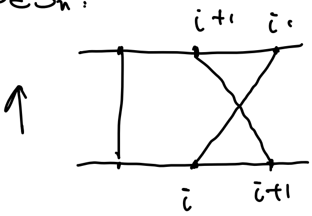
A_4 is not Abelian. $A_{n \geq 4}$ not

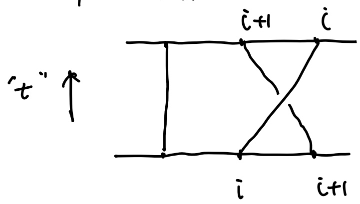
$(123)(124) = (13)(24)$

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

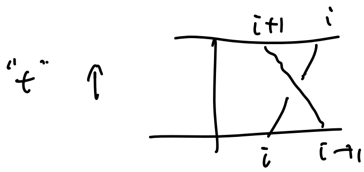
I. 4. Braiding group (10.1.3)

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



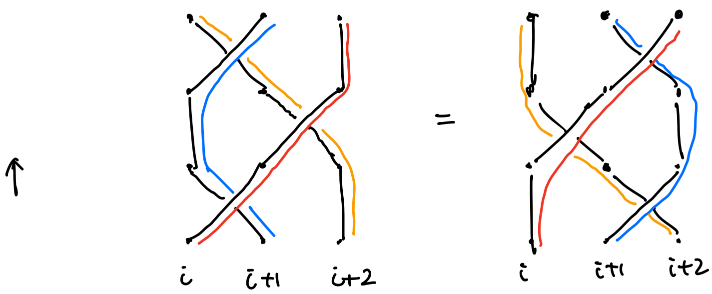


$\tilde{\sigma}(i)^{-1}$



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 & $\tilde{\sigma}_i$

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

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

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

$\sigma_i^2 = 1 \ \rangle$

$$B_n = \langle \tilde\sigma_1 \cdots \tilde\sigma_{n-1} \mid \tilde\sigma_i \tilde\sigma_j \tilde\sigma_i^{-1} \tilde\sigma_j^{-1} = 1. \quad |i-j| \geq 2$$

$$\tilde\sigma_i \tilde\sigma_{i+1} \tilde\sigma_i = \tilde\sigma_{i+1} \tilde\sigma_i \tilde\sigma_{i+1} \rangle \qquad (\tilde\sigma_i^2 \neq 1)$$

Anyon. fractional quantum hall.

Topological quantum computing

Yang-Baxter equations

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

$$\tilde\sigma_i \longmapsto \sigma_i$$

6. Cosets and conjugacy (7)

6.1. Cosets and Lagrange theorem 陪集/旁集

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

The set

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

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 $G = \mathbb{Z}$ $H = n\mathbb{Z}$

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

$$= \{i \mid i = g \bmod n\}$$

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

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

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

gH: $1 \cdot H = H$

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

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

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

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

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

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

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

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

"G" $= H$

right action of H on G.

$G \times H \longrightarrow G$

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

or left action:

$H \times G \to G$

$(h, g) \mapsto gh^{-1}$

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

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

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

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

cosets define an equivalence relation.

$g_1 \sim g_2$ if $\exists h \in H$. 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

$$|H| \text{ divides } |G|.$$

divides makes no sense for ∞

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

$$G = \bigcup_{i=1}^{m} g_i H .$$

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

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

$$a^p \equiv a \mod p.$$

<u>Definition</u>. G a group. H subgroup.

The set of left cosets in G

is denoted G/H

It is the set of orbits under the

recall above <u>right</u> group action of H on G.

It is also referred to as a

homogeneous space.

The cardinality of G/H is

the <u>index of H</u> in G. denoted

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

<u>Example</u>. 1. $G = S_3$ $\quad H = S_2$

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

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

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

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

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

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

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

② $g^2H = H$. $\Rightarrow g^2 \in H$

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

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

there are $\underline{8}$ 3-cycles in A_4
$(8 > 6)$

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

$\boxed{\text{Converse of Lagrange theorem is usually not true.}}$

digression: $[G:H] = 2$.
$G = H \cup gH \quad (g \notin H)$

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

"normal subgroup"

A special case: (leave for reading)

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 $\quad |S_3| = 6 = 2 \times 3$

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

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

② $|Q| = 8 = 2^3$

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

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

$j, -j$

$k, -k$

$|H| = 8$ $\quad Q$