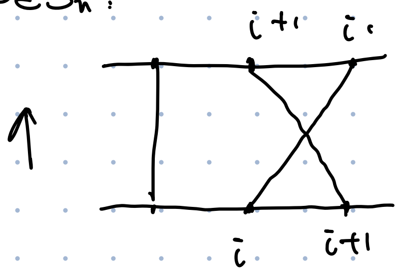
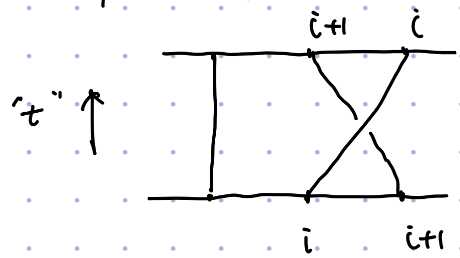
– Symmetric group & braiding group (10.1.3)

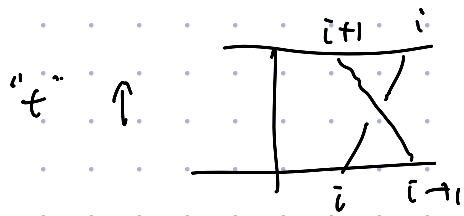
$\phi \in S_n$:



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

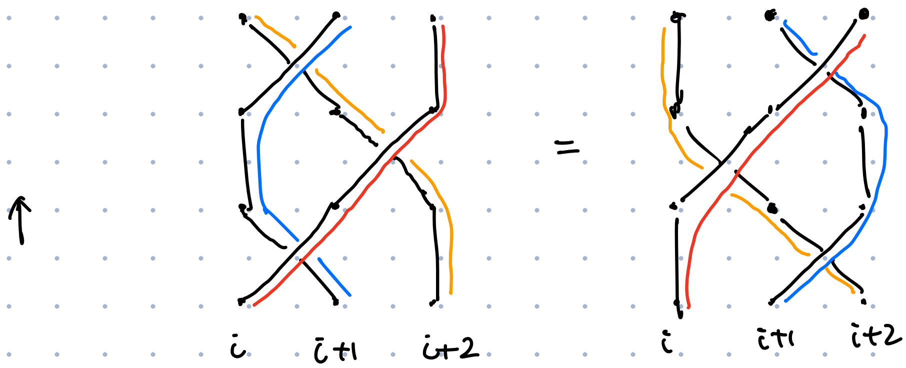


$\tilde{\sigma}(i)^{-1}$



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

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 & $\hat{\sigma}_i$

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

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

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

$\sigma_i^2 = 1 \ \rangle$

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

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

Anyon . fractional quantum hall.
Topological quantum computing
Yang - Baxter equations

$\phi : B_n \longrightarrow S_n$ homo.
$\tilde{\sigma}_i \longmapsto \sigma_i$

6. Cosets and conjugacy (7)

6.1. Cosets and Lagrange theorem 陪集/旁集

<u>Definition</u>: Let $H \subset G$ be a subgroup.

The <u>set</u>

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

is a <u>left-coset of H</u>.

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

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

<u>Example</u>. 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: $1 \cdot H = H$

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

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

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

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

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

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

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:

$$H \times G \to G$$
$$(h, g) \longmapsto \underline{\underline{gh^{-1}}}$$

Proof: suppose $g \in g_1H \cap g_2H$ then

$$g = g_1h_1 = g_2h_2 \qquad h_i \in H$$

$$g_1 = g_2 \underline{h_2 h_1^{-1}} = g_2 h \qquad h = h_2h_1^{-1} \in H$$

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

cosets define an equivalence relation.

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

$$(g_1H = g_2H)$$

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

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

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

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

recall above 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

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

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

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

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

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

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

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

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

$[G:H] = 6$

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

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

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

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

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

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

$(8 > 6)$

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

Converse of Lagrange theorem is usually not true.

digression: $[G:H] = 2$.

$G = H \cup gH$ $(g \notin H)$

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

"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: $\quad S_2 \cong \mathbb{Z}_2$

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

② $|Q| = 8 = 2^3$

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

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

$\qquad\qquad\qquad\quad j, -j$

$\qquad\qquad\qquad\quad k, -k$

$|H| = 8 \quad Q$