Last time:
- symmetric group S_n
- two-row notation $\begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix}$
- cycle notation $(i_1\, i_2 \cdots i_k)$.

A transposition just means a cycle of length 2:

e.g. $(1\ 3)$ swaps 1 and 3 (fixes everything else).

Proposition: Any permutation $\alpha \in S_n$ can be written as

$$\alpha = \tau_1 \tau_2 \cdots \tau_k$$

a product of transpositions.

$\tau_i = (j_i\ k_i)$ transposition.

Definition: Let $\alpha \in S_n$ and write

$$\alpha = \tau_1 \tau_2 \cdots \tau_k \qquad (*)$$

a product of transpositions.

The sign of α is defined as

$$\operatorname{sign}(\alpha) = (-1)^k$$

where k = number of transpositions in $(*)$

Important point: For given α, may be many ways to write it as $\alpha = \tau_1 \cdots \tau_k$

Example: in S_3, $\alpha = (1\,2)$ $\leftarrow k=1$

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

But the number $(-1)^k$ only depends on α, not on how we choose to write it as a product of transpositions.

Definition: if $\operatorname{sign}(\alpha) = 1$ we say α is even;
if $\operatorname{sign}(\alpha) = -1$ we say α is odd.

Example:

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

So $\operatorname{sign}(1\,2) = (-1)^1 = (-1)^3 = -1$

So $(1\,2)$ is odd.

b) $(i_1 \cdots i_k) = \underbrace{(i_1\, i_k) \cdots (i_1\, i_2)}_{k-1 \text{ transpositions}}$

So $\operatorname{sign}(i_1 \cdots i_k) = (-1)^{k-1}$.

Generators of Groups

Def: Let G be a group and $g_1, \ldots, g_k \in G$.
We say G is generated by $g_1, \ldots, g_k$ if every $g \in G$ can be written as a product of the g_i's and their inverses, the g_i^{-1}'s.

Example: $g = g_2^{-1} g_1^4 g_3 g_1^{-1}$. $\leftarrow$ "word" in the g_i

If G is generated by $g_1, \ldots, g_k$ we use the notation $\boxed{G = \langle g_1, \ldots, g_k \rangle}$.

Example: The dihedral group D_n is generated by rotation by $2\pi/n$, called r, and reflection, called s:

$$D_n = \langle r, s \rangle$$

since we have seen $D_n = \{e, r, \ldots, r^{n-1}, s, \ldots, r^{n-1}s\}$.

Generating S_n

Already saw any $\alpha \in S_n$ can be written as a product of transpositions.
So the set of transpositions generates S_n.

But we can find smaller generating sets:

Proposition 1: S_n is generated by the transpositions

$$\tau_1 = (1\ 2),\quad \tau_2 = (1\ 3),\quad \ldots,\quad \tau_n = (1\ n).$$

Proof: We already know set of all transpositions generates S_n. So it is enough to write any transposition $(i\ j)$ as a product of the τ_i's.

This is easy:

$$(i\ j) = \underbrace{(1\ i)}_{\tau_{i-1}}\underbrace{(1\ j)}_{\tau_{j-1}}\underbrace{(1\ i)}_{\tau_{i-1}}. \qquad \blacksquare$$

Proposition 2: S_n is generated by the transpositions

$$\sigma_1 = (1\ 2),\quad \sigma_2 = (2\ 3),\quad \ldots,\quad \sigma_{n-1} = (n-1\ n).$$

Proof: By Proposition 1, it's enough to write any of the τ_i as a product of σ_j's, which can be done as follows:

$$\begin{aligned}\tau_j = (1\ j) &= (j-1\ j)\cdots(2\ 3)(1\ 2)(2\ 3)\cdots(j-1\ j) \\ &= \sigma_{j-1}\cdots\sigma_2\,\sigma_1\,\sigma_2\cdots\sigma_{j-1}\end{aligned}$$

$\blacksquare$

The Alternating Group

The set of even permutations in S_n is denoted:

$$A_n = \{\alpha \in S_n \mid \text{sign}(\alpha) = 1\}.$$

This is a group: if α, β are even, then

$$\underbrace{\text{sign}(\alpha\beta)}_{(-1)^{k+l}} = \underbrace{\text{sign}(\alpha)}_{(-1)^k}\underbrace{\text{sign}(\beta)}_{(-1)^l} \quad \text{so } \alpha\beta \text{ is even.}$$

~~The number of e~~ the alternating group A_n.

Number of elements: $|A_n| = \frac{|S_n|}{2} = \frac{n!}{2}$.

Example: A_3 has $\frac{3!}{2} = \frac{6}{2} = 3$ elements:

$$A_3 = \{e, (1\,2\,3), (1\,3\,2)\}$$

3-cycles

In general, A_n contains all the k-cycles ~~of~~ for $k \leq n$ and k odd. [Remember: $\text{sign}(i_1 \cdots i_k) = (-1)^{k-1}$].

(But it has more elements besides!)

Proposition: The alternating group A_n $(n \geq 3)$ is generated by 3-cycles of the form

$$(1\; i\; j) \qquad (1 < i, j \leq n,\ i \neq j)$$

Proof: By Proposition 1, every $\alpha \in A_n$ is a product of an even number of the τ_i:

$$\alpha = \underbrace{(1\ i_1)(1\ i_2)} \cdots\cdots \underbrace{(1\ i_{2k-1})(1\ i_{2k})}$$

Now pair them up and use $(1\ i)(1\ j) = (1\ j\ i)$ to get a product of 3-cycles. ∎

Application: The 15-puzzle.

In 1896 Sam Lloyd offered \$1000 to anyone who could transform this:

1	2	3	4
5	6	7	8
9	10	11	12
13	15	14	

(N)

slide tiles

to this:

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

(S)

Can it be done?

View a configuration of the puzzle as a permutation of $\{1, 2, \ldots, 15\}$ – i.e. an element of S_{15}.

Notice: Any permutation we can obtain from (S) must be even.

To see this, think of blank square as being labelled 16. Any move of the puzzle is a transposition. But to get blank square back to bottom-right it must make as many up-moves as down, and left moves as right. So <u>even</u> number of transposition.

<u>Corollary</u>: The puzzle cannot be solved.

<u>Proof</u>: The configuration (N) corresponds to the transposition (14 15), hence odd. ∎