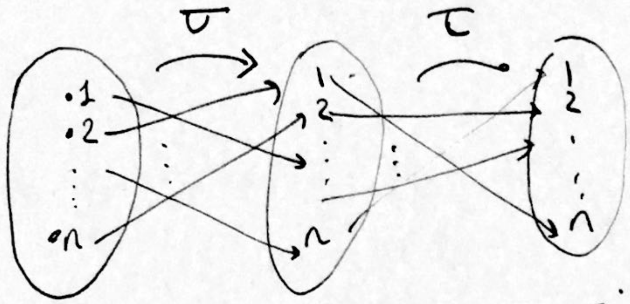
Lecture 17:

Permutation groups

- Let $A = \{1, 2, \dots, n\}$.
- Consider the set
$$S_n = \{ \overset{f : A \to A}{f : \{1,2,\dots,n\} \to \{1,2,\dots,n\}} \mid f \text{ is bijective} \}.$$
- 

We can look at the composition operation on S_n.

$$\circ : \begin{array}{ccc} S_n \times S_n & \longrightarrow & S_n \\ (\sigma, \tau) & \longmapsto & \sigma \circ \tau \end{array}$$

given by $(\sigma \circ \tau)(a) = \sigma(\tau(a))$.

<u>Notation:</u> If
$\sigma(1) = 2$
$\sigma(2) = 3$
$\sigma(3) = 4$
$\sigma(4) = 1$
we write

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

In general

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & & \sigma(n) \end{pmatrix}$$

How do we know that $\circ$ is a binary operation?

We need to check that $\sigma \circ \tau$ is bijective for σ and τ bijective. It's enough to check just injectivity or surjectivity. (since $\{1, 2, \dots, n\}$ is finite)

Assume $\sigma \circ \tau(a) = \sigma \circ \tau(b)$

then $\sigma(\tau(a)) = \sigma(\tau(b))$

Since σ is injective:

$$\tau(a) = \tau(b)$$

And since τ is injective:

$$a = b.$$

Example:

$$\overset{\sigma}{\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 3 & 4 \end{pmatrix}} \circ \overset{\tau}{\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 5 & 4 & 3 \end{pmatrix}. \qquad \sigma(\underbrace{\tau(1)}_{2}) = 1.$$

Theorem: $(S_n, \circ)$ is a group.

Proof: Already seen that $\circ$ is a binary operation on S_n. Associativity is from associativity of function composition. Identity element is $id: \{1, 2, \dots, n\} \to \{1, 2, \dots, n\}$, $id(a) = a$.

Inverses: we know that bijective functions have inverses.

$\square$

$\underline{n=3}$: elements are

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \mu_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

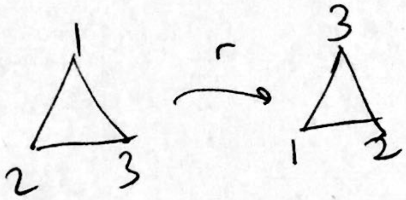
$$\rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \mu_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$\rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \quad \mu_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

$$\rho_1^2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$\rho_1^3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = e.$$

$$\mu_1^2 = e = \mu_2^2 = \mu_3^2 \quad \ldots$$



- $S_3 \cong D_6$

by $e \mapsto 1$ $\qquad \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \mapsto s$

$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \mapsto r$ $\qquad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \mapsto sr$

$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \mapsto r^2$ $\qquad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \mapsto sr^2.$

Conjecture: $S_n \cong D_{2n}$? False.

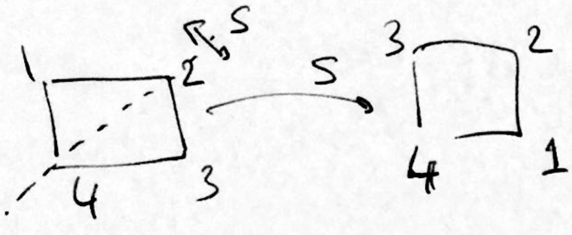
$$|S_n| = n!$$

$$|D_{2n}| = 2n.$$

Still, there is a subgroup of S_4 which is isomorphic to D_8.

Observe that we can write each element of D_8 as a permutation:

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



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

in general: $1 \mapsto$ new spot for 1
$2 \mapsto$ new spot for 2
$3 \mapsto$ new spot for 3
$4 \mapsto$ new spot for 4.

<u>Cayley's theorem</u>: Every finite group is isomorphic to a subgroup of S_n for some n.

<u>proof idea</u>: Let $G = \{g_1, g_2, g_3, \dots, g_n\}$ $n = |G|$.

We can consider the map $\varphi: G \to S_n$ given by $\varphi(g) = \begin{pmatrix} g_1 & g_2 & \cdots & g_n \\ gg_1 & gg_2 & \cdots & gg_n \end{pmatrix}$

this doesn't make sense since $gg_i \notin \{1, 2, \dots, n\}$ what we mean is that:

$\varphi(g_k)(i) = j$ if $g_k g_i = g_j$.

alternative: we could have defined S_n to be maps $f: A \to A$ for any set A.

we still need to prove:

- φ is a homomorphism.
- φ is injective

(then φ will be bijective with its image)

- image of φ is a subgroup.