Lecture 18:

Last time: permutation groups.

$$S_n = \{ f : \{1,2,\dots,n\} \to \{1,2,\dots,n\} \mid f \text{ bijective} \}$$

$$S_A = \{ f : A \to A \mid f \text{ bijective} \}.$$

$(S_n, \underset{\nearrow \text{ composition}}{\circ})$ is a group.

notation.

$|S_n| = n!$

$\sigma(1) = 3$
$\sigma(2) = 1$
$\sigma(3) = 4$
$\sigma(4) = 2$

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

- $D_3 \cong S_3$ but $D_4 \not\cong S_4$.

Today:

- **Cayley's theorem**: Every finite group is isomorphic to a subgroup of S_n for some n.

maybe we'll do this next time.

proof: Let $(G, \cdot)$ be a finite group.

Consider the map $\varphi : G \to S_G$ ← this is the set G without the group structure.

$$g \mapsto \sigma_g$$

i.e. $\varphi(g) = \sigma_g$

with $\sigma_g(h) = gh$

$$\text{ie} \quad \sigma_g = \begin{pmatrix} \overbrace{h_1 \quad h_2 \cdots \quad h_{|G|}}^{\text{all the elements of } G} \\ gh_1 \quad gh_2 \cdots \quad gh_{|G|} \end{pmatrix}.$$

- φ is a group homomorphism; ie $\forall\, g_1, g_2$ $\varphi(g_1) \circ \varphi(g_2) = \varphi(g_1 g_2)$

Indeed: $(\varphi(g_1) \circ \varphi(g_2))(h) = \sigma_{g_1}(\sigma_{g_2}(h)) = \sigma_{g_1}(g_2 h) = g_1 g_2 h$
$= \sigma_{g_1 g_2}(h) = \varphi(g_1 g_2)(h)$!

- φ is injective:

Suppose $\varphi(g_1) = \sigma_{g_1} = \sigma_{g_2} = \varphi(g_2)$.

Then $\varphi(g_1)(e) = \varphi(g_2)(e)$

$g_1 \cdot e = g_2 \cdot e$ so $g_1 = g_2$.

- φ is not surjective, but if we consider

$$\tilde{\varphi} : G \longrightarrow \mathrm{Im}(\varphi) \qquad \tilde{\varphi}(g) = \varphi(g)$$

then $\tilde{\varphi}$ is surjective.

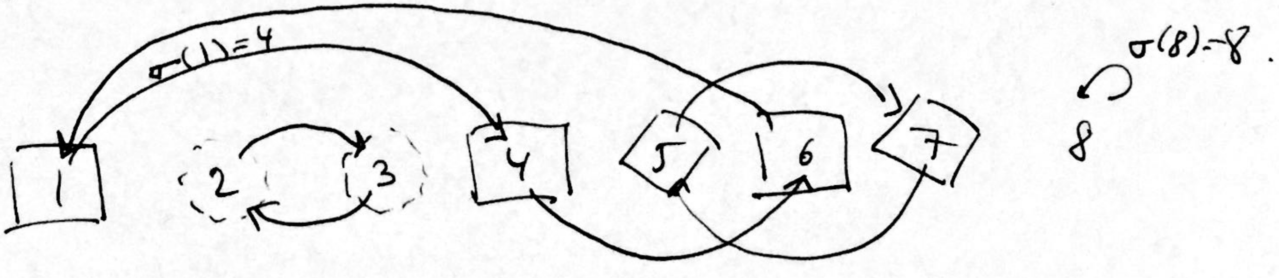
Hence $\tilde{\varphi}$ is an isomorphism.

$\square$

Orbits, cycles:

Consider $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 3 & 2 & 6 & 7 & 1 & 5 & 8 \end{pmatrix}$

Let's look at where σ takes elements:



This splits $\{1, 2, \dots, 8\}$ into groups:

$\{1, 4, 6\}$, $\{2, 3\}$, $\{5, 7\}$, $\{8\}$

these are called the orbits of σ.

$\{1,2,\dots,8\} = \{1,4,6\} \cup \{2,3\} \cup \{5,7\} \cup \{8\}$ ↙ orbit decomposition of $\{1,2,\dots,8\}$.

For $\sigma \in S_n$, let $\sim$ be defined by

$$a \sim b \iff \sigma^k(a) = b \text{ for some } k \in \mathbb{Z}.$$

Then $\sim$ is is an equivalence relation.

- reflexivity: $a = \sigma^0(a)$ $\forall a$

  so $a \sim a$ $\forall a$.

- symmetry

  $a \sim b$, i.e $\sigma^k(a) = b$

  $$\Rightarrow \sigma^{-k}(\sigma^k(a)) = \sigma^{-k}(b)$$

  $$\Rightarrow a = \sigma^{-k}(b)$$

  so $b \sim a$

- transitivity: If $\sigma^{k_1}(a) = b$

  and $\sigma^{k_2}(b) = c$

  then
  $$\begin{array}{cl} \sigma^{k_2}(\sigma^{k_1}(a)) & = \sigma^{k_2}(b) = c \\ \| & \\ \sigma^{k_1+k_2}(a) = c & \end{array}$$

  so $a \sim c$.

Def: • The equivalence classes of $\sim$ are called the orbits of σ.

- The orbit of i is the equivalence class of i under $\sim$.

Ex: $\begin{pmatrix}1&2&3&4&5&6&7\\5&7&3&6&4&2&1\end{pmatrix}$

$\sigma(1)=5$

$\sigma(5)=4$

$\sigma(4)=6$

$\sigma(6)=2$

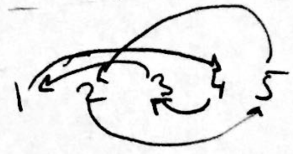
$\sigma(2)=7$

$\sigma(7)=1$

$\sigma(3)=3$

two orbits

$\{1,2,4,5,6,7\}$ and $\{3\}$



Remark: We can write $\begin{pmatrix}1&2&3&4&5\\4&5&1&3&2\end{pmatrix}$ as

$$\left(\begin{matrix}1\\4\end{matrix}\ \boxed{\begin{matrix}2\\2\end{matrix}}\ \begin{matrix}3\\1\end{matrix}\ \begin{matrix}4\\3\end{matrix}\ \boxed{\begin{matrix}5\\5\end{matrix}}\right)\circ\left(\boxed{\begin{matrix}1\\1\end{matrix}}\ \begin{matrix}2\\5\end{matrix}\ \boxed{\begin{matrix}3&4\\3&4\end{matrix}}\ \begin{matrix}5\\2\end{matrix}\right)$$

↗ 2,5 fixed.
1,3,4 moving

↗ 1,3,4 fixed
2,5 moving.

Def: A *cycle* is a permutation that contains at most one orbit of size >1.

Ex: the two permutations above $\begin{pmatrix}1&2&3&4&5\\4&2&1&3&5\end{pmatrix}$ and $\begin{pmatrix}1&2&3&4&5\\1&5&3&4&2\end{pmatrix}$ are cycles.

Notation: We write cycles $\begin{pmatrix}a_1 & a_2 & \cdots & a_{k-1} & a_k & a_{k+1}\ a_{k+2}\ \cdots\ a_n\\ a_2 & a_3 & \cdots & a_k & a_1 & \underbrace{a_{k+1}\ a_{k+2}\ \ \ a_n}_{\text{fixed part.}}\end{pmatrix}$

as $(a_1 a_2 a_3 .. a_{k-1} a_k)$ ← a "k-cycle".

Ex: $\begin{pmatrix}1&2&3&4&5\\4&2&1&3&5\end{pmatrix}=(1\,4\,3)$ "1 goes to 4
4 goes to 3
3 goes back to 1"

$\begin{pmatrix}1&2&3&4&5\\1&5&3&4&2\end{pmatrix}=(2\,5)$ "2 goes to 5
5 goes to 2"

Therefore $\begin{pmatrix}1&2&3&4&5\\4&5&4&3&2\end{pmatrix} = (1\,4\,3)(2\,5)$

in S_3

Ex: $(1\,2)(2\,3) = \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix} = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$

$(2\,3)(1\,2) = (1\,3\,2) \longrightarrow \neq \qquad = (1\,2\,3)$

Remark: Even though S_n is not commutative, disjoint cycles commute.

Theorem: Every finite permutation σ is a product of disjoint cycles.

Lecture 19:

Last time: cycles, orbits.

- orbit of i under $\sigma \in S_n$
  are all elements of $\{1,2,\dots,n\}$ of the form $\sigma^k(i)$.
- **Cycle:** a permutation that has at most 1
  orbit of size >1.
- ex: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 2 & 4 & 1 \end{pmatrix} = (1\,3\,2\,5)$

  1 goes to 3
  3 goes to 2.
  2 goes to 5
  5 goes to 1.

- Cycle decomposition:

ex: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 5 & 7 & 6 & 1 & 4 & 9 & 3 & 8 \end{pmatrix}$

$= (1\,2\,5)(3\,7\,9\,8)(4\,6)$

disjoint.

Theorem: Every finite permutation can be written as a product of disjoint cycles.

Even and odd permutations:

Def: A 2-cycle (ij) is called a transposition.

Ex: You can write other permutations by composing transpositions.

$$(1\,2\,3) = (13)(12)$$

$$(1\,2\,3\,4\,5) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}$$

$$= (15)(14)(13)(12)$$

A QUICK AND CONFUSING WAY TO THINK ABOUT IT:

$$1\ 2\ 3$$

$$\downarrow (13)$$

$$\cancel{3\ 1\ 2}\ 3\ 2\ 1$$

$$\downarrow (12)$$

$$2\ 3\ 1$$

Lemma: Every cycle is a product of transpositions

proof: $(a_1 a_2 \ldots a_n) = (a_1 a_n)(a_1 a_{n-1}) \ldots (a_1 a_2)$

Corollary: Every (finite) permutation is a product of transpositions.

proof: since each permutation is a product of cycles and each cycle is a product of transpositions, each permutation is a product of transpositions □ (there is also a nice proof by induction of this)

Theorem: A permutation can be written as either a product of an even number of transpositions or an odd number of transpositions but not both.

proof: there are two proofs, both nice but one is nicer! (which one?)

proof 1: We will observe that if σ is a permutation, and (ij) is a transposition, then $(ij)\sigma$'s number of orbits differs ~~with~~ from σ's number of orbits by 1.

case 1: In the cycle decomposition of σ, i and j are in different cycles (or orbits)

$$\sigma = (a_1, \dots, a_{s-1}, i, a_{s+1}, \dots, a_{n_1})(b_1 b_2 \dots b_{k-1} j b_{k+1} \dots b_{n_2}) \dots$$

more cycles (disjoint).

If we multiply by (ij), we get:

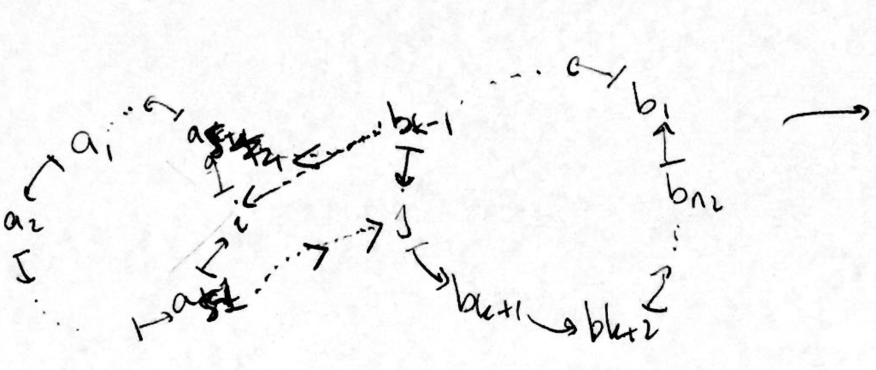
$$(ij)\sigma = (ij)(a_1 a_2 \dots a_{s-1}\, i\, a_{s+1} \dots a_{n_1})(b_1 b_2 \dots b_{k-1}\, j\, b_{k+1} \dots b_{n_2})\,\sigma'$$

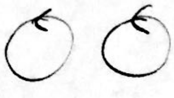
other cycles.

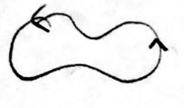
~~$= (a_1 a_2 \dots a_{s-1}\, i\, b_{k+1}$~~

$$= (a_1 a_2 \dots a_{s-1}\, j\, b_{k+1} \dots b_{n_2} b_1 \dots b_{k-1} \cancel{b_k}\, i\, a_{s+1} \dots a_{n_1})\,\sigma'$$

So 2 cycles became 1 cycle:



replaces  by



Case 2: Suppose i and j are in the same orbit of σ

$$\sigma = (a_1\, a_2 \ldots a_{s-1}\, i\, a_{s+1} \cdots a_{k-1}\, j\, a_{k+1} \cdots a_n)\, \underset{\text{other disjoint cycles}}{\sigma'}$$

$$(ij)\sigma = (ij)(a_1 \ldots a_{s-1}\, i\, a_{s+1} \cdots a_{k-1}\, j\, a_{k+1} \cdots a_n)\sigma'$$

$$(ij)\sigma = (a_1 \ldots a_{s-1}\, j\, a_{k+1} \cdots a_n)(a_{s+1}\, a_{s+2} \cdots a_{k-1}\, i)$$

one cycle became two.

Conclusion: each transposition changes the number of orbits from even to odd or odd to even. Hence the parity of the number of transpositions is the parity of the number of orbits.

Proof 2 uses linear algebra.

Proposition: There is a subgroup of $GL_n(\mathbb{R})$ isomorphic to S_n.

proof: Consider the set of permutation matrices:

$$\sigma \longmapsto \varphi(\sigma) = (a_{ij}) \quad \text{where } a_{ij} = \begin{cases} 1 & \text{if } j = \sigma(i) \\ 0 & \text{otherwise.} \end{cases}$$

ex: $\varphi(123) = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$ (THEN: $\varphi(\sigma)(e_i) = e_{\sigma(i)}$).

φ is an injective group homomorphism.

Observe that $\det \varphi(ij) = -1$. So number of transpositions is even if $\det\varphi(\sigma) = 1$, odd if $\det \varphi(\sigma) = -1$.