

Lecture 18:

Last time: permutation groups.

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

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

(S_n, \circ) is a group.

composition

notation.

$$|S_n| = n!$$

$$\begin{aligned} \sigma(1) &= 3 \\ \sigma(2) &= 1 \\ \sigma(3) &= 4 \\ \sigma(4) &= 2 \end{aligned}$$

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

$D_3 \cong S_3$ 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 $\varphi: G \rightarrow S_G$

this is the set G without the group structure.

$$g \mapsto \sigma_g$$

with $\sigma_g(h) = gh$

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

all the elements of G

$$i.e. \sigma_g = \begin{pmatrix} h_1 & h_2 & \dots & h_{|G|} \\ gh_1 & gh_2 & \dots & gh_{|G|} \end{pmatrix}$$

φ is a group homomorphism; i.e. $\forall g_1, g_2 \quad \varphi(g_1) \circ \varphi(g_2) = \varphi(g_1 g_2)$

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

$$= \sigma_{g_1 g_2}(h) = \varphi(g_1 g_2)(h) \quad |$$

• 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

$$\tilde{\varphi}: G \rightarrow \text{Im}(\varphi) \quad \tilde{\varphi}(g) = \varphi(g)$$

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

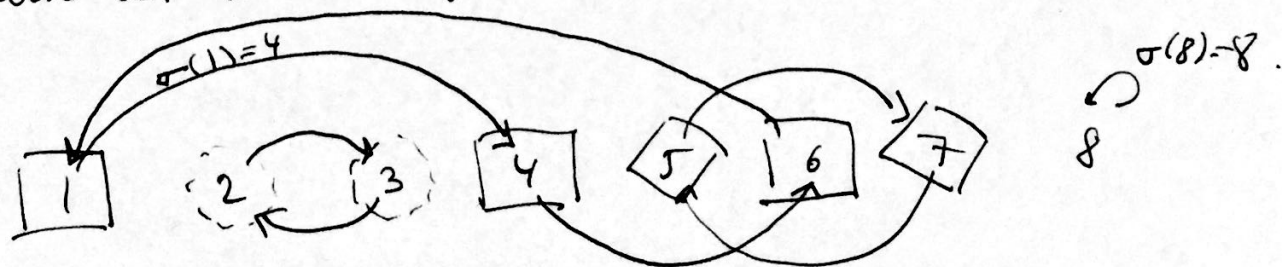
Hence $\tilde{\varphi}$ is an isomorphism.

□

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 .

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

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 an equivalence relation.

• reflexivity: $a = \sigma^0(a) \quad \forall a$
so $a \sim a \quad \forall a$.

• symmetry

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

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

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

so $b \sim a$

• transitivity: If $\sigma^{k_1}(a) = b$
and $\sigma^{k_2}(b) = c$

then $\sigma^{k_2}(\sigma^{k_1}(a)) = \sigma^{k_2}(b) = c$

$$\begin{array}{c} \text{"} \\ \sigma^{k_1+k_2}(a) = c \end{array}$$

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

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

\nearrow
2, 5 fixed.
1, 3, 4 moving

\nearrow
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 are cycles:

Notation: We write cycles $(a_1 a_2 \dots a_{k-1} a_k a_{k+1} a_{k+2} \dots a_n)$

as $(a_1 a_2 a_3 \dots a_{k-1} a_k) \leftarrow$ a "k-cycle". fixed part.

Ex: $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 1 & 3 & 5 \end{pmatrix} = (143)$

"1 goes to 4
4 goes to 3
3 goes back to 1"

$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 3 & 4 & 2 \end{pmatrix} = (25)$

"2 goes to 5
5 goes to 2"

Therefore $(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 4 & 3 & 2 \end{smallmatrix}) = (143)(25)$

Ex. $(12)(23) \stackrel{\text{in } S_3}{=} (\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{smallmatrix})(\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{smallmatrix}) = (\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{smallmatrix})$
 $(23)(12) = (132) \rightarrow \neq \left. \vphantom{(132)} \right] = (123)$

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

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