Last time Given a set X

$\mathrm{Sym}(X) = \{ f : X \to X \mid f \text{ is invertible} \}$

$\mathrm{Sym}(X)$ is a group with the group operation = composition.

Special case: $X = \{1, 2, \dots n\}$, $n \in \mathbb{N}$.

We write $S_n = \mathrm{Sym}(\{1, \dots n\})$

the group of permutation on n letters.

An element $\sigma \in S_n$ is called a permutation.

Claim S_n has $n!$ elements

(we write $|S_n| = n!$)

Proof For $\sigma \in S_n$, $\sigma(1), \sigma(2), \dots \sigma(n)$ are all distinct.
(otherwise σ is not invertible)

There are n choices for $\sigma(1)$

$n-1$ choices for $\sigma(2)$

$n-2$ —— // —— $\sigma(3)$

$\vdots$

1 choice for $\sigma(n)$

$\Rightarrow$ total number of choices is $n \cdot (n-1) \cdot \dots \, 2 \cdot 1 = n!$ $\square$

Given $\sigma \in S_n$ we can picture it as

$$\begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & & \sigma(n) \end{pmatrix}$$

This is too cumbersome. Better notation:

Write σ as a product of disjoint cycles.

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

What does σ do? $1 \to 4 \to 2 \to 6$ a cycle

3 a cycle

$5 \to 7$ a cycle.

So we write $\sigma = (1\,4\,2\,6)(3)(5\,7) = (1\,4\,2\,6)(5\,7)$.

<u>Note</u> 1) we can interpret each cycle <u>separately</u> as a permutation:

$$(1\,4\,2\,6) \leftrightarrow \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 6 & 3 & 2 & 5 & 1 & 7 \end{pmatrix}$$

$$(3) \leftrightarrow \mathrm{Id} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{pmatrix}$$

$$(5\,7) \leftrightarrow \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 3 & 4 & 7 & 6 & 5 \end{pmatrix}$$

2) $\sigma = (1\,4\,2\,6) \circ (5\,7)$

↖ composition of permutations

<u>Ex</u> Write $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 \\ 5 & 12 & 2 & 1 & 9 & 11 & 4 & 3 & 7 & 10 & 13 & 8 & 6 \end{pmatrix}$ as a product of disjoint cycles.

<u>Solution</u> $\sigma = (1\,5\,9\,7\,4) \circ (2\,12\,8\,3) \circ (6\,11\,13)$

In this notation $S_2 = \{\mathrm{id}, (12)\}$

$S_3 = \{\mathrm{id}, (12), (13), (23), (123), (132)\}$.

<u>Our goal</u> Thm (Goodman, 1.5.3) Any permutation in S_n can be written uniquely (up to order) as a product of disjoint cycles.

Goodman is vague in his definition of "cycle" and "disjoint."

<u>Definition</u> $\sigma \in S_n$ is a <u>cycle of length r</u> if $\exists x_1, \ldots x_r \in \{1, \ldots n\}$ all distinct such that

$$\sigma(x_i) = x_{i+1} \quad \text{if} \quad 1 \leq i < r$$
$$\sigma(x_r) = x_1$$

and $\sigma(x) = x$ for $x \neq x_1, \ldots x_r$.

We write $\sigma = (x_1\; x_2\; \ldots\; x_r)$.

<u>Definition</u> Two permutations $\sigma, \tau \in S_n$ are <u>disjoint</u> if $\forall x \in \{1, \ldots n\}$

$$\sigma(x) \neq x \Rightarrow \tau(x) = x$$
$$\tau(x) \neq x \Rightarrow \sigma(x) = x$$

<u>Example</u> $(123), (45) \in S_7$ are disjoint
$(123), (425) \in S_7$ are not disjoint.

If $\sigma(x) = x$ we say "σ fixes x." If $\sigma(x) \neq x$ we say "σ moves x".

Thus σ and τ are disjoint $\Leftrightarrow$ What's moved by one is fixed by the other.

<u>Lemma 3.1</u> Suppose $\sigma, \tau \in S_n$ are disjoint. Then
$$\sigma \circ \tau = \tau \circ \sigma$$

<u>Proof</u> $\sigma \circ \tau = \tau \circ \sigma \Leftrightarrow \forall x \in \{1, \ldots n\}$ $\sigma(\tau(x)) = \tau(\sigma(x))$.

Now for any $x \in \{1, \ldots n\}$ either

(i) x is fixed by σ <u>and</u> τ

(ii) x is moved by σ (hence fixed by τ)

(iii) x is moved by τ (hence fixed by σ)

In case (i),
$$\sigma(\tau(x)) = \sigma(x) = x = \tau(x) = \tau(\sigma(x))$$

In case (ii)
$$y = \sigma(x) \neq x.$$

Since σ is invertible, it's 1-1 $\Rightarrow$ $\sigma(x) \neq \sigma(y) = \sigma(\sigma(x))$

$\Rightarrow \sigma(x)$ is moved by σ. $\Rightarrow$ $\sigma(x)$ is fixed by τ

$\Rightarrow \tau(\sigma(x)) = \sigma(x)$

On the other hand $\tau(x) = x$. $\Rightarrow \sigma(x) = \sigma(\tau(x))$

$\Rightarrow \tau(\sigma(x)) = \sigma(\tau(x))$.

Case (iii) is the same as (ii) with σ and τ switched.

We now prove

Theorem 3.1 For any finite set X any $\sigma \in Sym(X)$ can be written uniquely up to order as a product of disjoint cycles.

Proof We need to prove existence of a decomposition into cycles and its uniqueness.

To prove existence we use induction on $n = |X|$, the # of elements of X.

If $|X| = 1$ $Sym(X)$ has only one element, Id_X.
Not much to prove.

Suppose theorem holds for every set Y with $|Y| \le n$.
X is a set with $n+1$ elements, $\pi \in Sym(X)$, $\pi \ne id$

Since $\pi \ne id$, $\exists x_0 \in X$ s.t $\pi(x_0) \ne x_0$

let $x_1 = \pi(x_0)$, $x_2 = \pi(x_1) = \pi(\pi(x_0))$, $x_3 = \pi(x_2) \dots$

Since X is finite, not all x_i's are distinct.

Let k be the largest integer so that

$$x_0, x_1, \dots x_k \quad \text{are distinct.}$$

Claim $\pi(x_k) = x_0$.

Reason Since $x_0, x_1, \dots x_k, x_{k+1} = \pi(x_k)$ are not distinct and $x_0, \dots x_k$ are distinct, $\pi(x_k) = x_i$ for some $i < k$. If $i > 0$, $x_i = \pi(x_{i-1})$.

$\Rightarrow \pi(x_k) = \pi(x_{i-1})$. But π is 1-1. $\Rightarrow x_k = x_{i-1}$ and $i-1 < k$.

This contradicts that $x_0, \dots x_k$ are all distinct.

Now let $X_1 = \{x_0, \dots x_k\}$ $Y = \{x \in X \mid x \notin X_1\}$.

Then $\pi(X_1) \subseteq X_1$ and $\pi(Y) \subseteq Y$ [why?]

(in fact $x_0 \xrightarrow{\pi} x_1 \to x_2 \to \dots x_k$)

Now set

$$\pi_1(x) = \begin{cases} \pi(x) & x \in X_1 \\ x & x \in Y \end{cases} \qquad \pi_2(x) = \begin{cases} x & x \in X_1 \\ \pi(x) & x \in Y \end{cases}$$

Then π_1, π_2 are disjoint permutations and $\pi = \pi_1 \circ \pi_2$

By inductive assumption (since $|Y| = |X| - (k+1)$)
$\pi_2 : Y \to Y$ is a product of disjoint cycles.
π_1 is a cycle.

$\Rightarrow \quad \pi = \pi_1 \circ \pi_2$ is a product of disjoint cycles.