Last time: (i) Given an action $G \times X \to X$, $x \in X$
the stabilizer of x is $G_x = \mathrm{Stab}(x) = \{ g \in G \mid g \cdot x = x \}$

(ii) G_x is a subgroup of G

(iii) Orbit/Stabilizer theorem:

$$f : G/G_x \longrightarrow G \cdot x, \quad f(gG_x) = g \cdot x$$

is a well-defined bijection.

(iv) $\sigma, \tau \in \mathrm{Sym}(X)$ are disjoint if $\{x \mid \sigma(x) \neq x\} \cap \{x \mid \tau(x) \neq x\} = \emptyset$.

(v) if σ, τ are disjoint then $\sigma(\tau(x)) = \tau(\sigma(x)) \quad \forall x$, ie $\sigma \circ \tau = \tau \circ \sigma$.

Definition $\sigma \in \mathrm{Sym}(X)$ is a cycle of length $r > 0$ if $\exists\, y_0, \dots, y_{r-1} \in X$, all distinct, s.t. $\sigma(x) = x$ for $x \neq y_0, \dots, y_{r-1}$

$\sigma(y_1) = y_2$, $\sigma(y_2) = y_3$, $\dots$ $\sigma(y_{r-2}) = y_{r-1}$ and $\sigma(y_{r-1}) = y_0$.

Note a cycle of length 1 is the identity map.

Goal Let X be a finite set, $\tau \in \mathrm{Sym}(X)$, $\tau \neq \mathrm{id}$.
Then there exist (unique) disjoint cycles $\sigma_1, \dots \sigma_k$ (of length > 1)
so that $\tau = \sigma_1 \circ \dots \circ \sigma_k$.

Definition Let $G \times X \to X$ be an action. $x \in X$ is a fixed point of the action if $g \cdot x = x \quad \forall g \in G$.
Equivalently $G \cdot x = \{x\}$, equivalently $G_x = G$, equivalently $|G \cdot x| > 1$.

Observation Any $\tau \in \mathrm{Sym}(X)$ gives rise to an action of $\mathbb{Z}$:

$$n \cdot x = \tau^n(x) \quad \forall n \in \mathbb{Z}.$$

Claim Let X be a finite set, $\tau \in \mathrm{Sym}(X)$. Suppose there exists exactly one orbit of the action of $\mathbb{Z}$ with more than 1 element, ie $\exists\, y_0 \in X$ s.t. $|\mathbb{Z} \cdot y_0| = r > 1$ and $\mathbb{Z} \cdot x = x$ for $x \notin \mathbb{Z} \cdot y_0$

Then τ is a cycle of length r.

Proof By the orbit/stabilizer theorem we have a bijection

$$\mathbb{Z}/\mathrm{stab}(y_0) \to \mathbb{Z}\cdot y_0$$

$\mathrm{stab}(y_0)$ is a subgroup of $\mathbb{Z}$, hence $\mathrm{stab}(y_0) = n\mathbb{Z}$ for some $n \geq 0$.

Since $|\mathbb{Z}\cdot y_0| = r$, $|\mathbb{Z}/n\mathbb{Z}| = r$. $\Rightarrow n = r$.

Therefore $\{0, \ldots, r-1\} \to \mathbb{Z}\cdot y_0$, $[k] \mapsto \tau^k(y_0)$

is a well-defined bijection. Let $y_k = \tau^k(y_0) = [k]\cdot y_0$.

Then $y_1 = \tau(y_0)$, $y_2 = \tau^2(y_0) = \tau(\tau(y_0)) = \tau(y_1)$ ...

and $y_0 = [r]\cdot y_0 = \tau^r(y_0) = \tau(\tau^{r-1}(y_0)) = \tau(y_{r-1})$.

For $x \notin \mathbb{Z}\cdot y_0$, $\tau(x) = x$

$\therefore$ τ is a cycle. □

Now let $\tau \in \mathrm{Sym}(X)$, $\tau \neq \mathrm{id}$. Consider the action of $\mathbb{Z}$ on X induced by τ:

$$n \cdot x := \tau^n(x)$$

Then X is a disjoint union of finitely many orbits: $\exists\, m > 0$ $x^{(1)}, \ldots, x^{(m)} \in X$ so that

$$X = \mathbb{Z}\cdot x^{(1)} \cup \ldots \cup \mathbb{Z}\cdot x^{(m)} \quad \text{with } \mathbb{Z}\cdot x^{(i)} \cap \mathbb{Z}\cdot x^{(j)} = \emptyset \text{ for } i \neq j.$$

Since $\tau \neq \mathrm{id}$, not all $x^{(i)}$'s are fixed points.

May assume $x^{(1)}, \ldots, x^{(k)}$ are not fixed. Call their orbits nontrivial

Let $r_i = |\mathbb{Z}\cdot x^{(i)}|$, $1 \leq i \leq k$. Then $r_i > 1$

For each i define $\sigma_i : X \to X$ by $\sigma_i(y) = \begin{cases} y & y \notin \mathbb{Z}\cdot x^{(i)} \\ \tau(y) & y \in \mathbb{Z}\cdot x^{(i)} \end{cases}$

Then the action of $\mathbb{Z}$ defined by σ_i (ie $n \cdot x = \sigma_i^n(x)$) has exactly one nontrivial orbit, namely $\mathbb{Z}\cdot x^{(i)}$.

By the claim each σ_i is a cycle of length r_i.

Moreover by construction σ_i and σ_j are disjoint for $i \neq j$.

Finally $\tau = \sigma_1 \circ \ldots \circ \sigma_k$.

This proves existence

Uniqueness? Suppose $\tau = \mu_1 \circ \cdots \circ \mu_\ell$, where μ_i's are disjoint cycles. Then each μ_i has exactly one nontrivial orbit. It's the set $Y_i = \{y \in X \mid \mu_i(y) \neq y\}$.
Since μ_j's are disjoint $\Rightarrow \mu_j(y) = y \quad \forall y \in Y_i$. ($\forall j \neq i$)

$\Rightarrow$ It follows that $\forall y \in Y_i$, $\tau(y) = \mu_i(y)$
(since the other μ's don't move the points of Y_i and since they commute)
Consequently Y_i is an orbit of the action of $\mathbb{Z}$ defined by τ. $\Rightarrow$ Y_i is $\mathbb{Z} \cdot x^{(s)}$ for some s.
But $\mathbb{Z} \cdot x^{(s)}$ is the orbit of τ_s. (unique nontrivial)
It follows that $\mu_i = \tau_s$
Consequently, up to order, μ_i's are τ_s's. □

Lagrange's theorem Let G be a finite group, $H < G$ a subgroup. Then $|G| = |H \backslash G| |H| = |G/H| |H|$.

Definition The index of H in G is $|G:H| := |G/H|$, the size of the set G/H.

Proof of Lagrange's theorem Since G is finite, so is H.
Recall that $H \backslash G$ is the set of orbits for the action of H on G which is defined by $a \cdot g = ag \quad \forall a \in H, g \in G$.
Since G is finite, so is $H \backslash G$. $\Rightarrow \exists g_1, \ldots, g_k \in G$ s.t.
$H \backslash G = Hg_1 \cup Hg_2 \cup \cdots \cup Hg_k$, $Hg_i \cap Hg_j = \emptyset$.
Now $\text{stab}(g_i) = \{h \in H \mid hg_i = g_i g\} = \{h \in H \mid h = e\} = \{e\}$.
Orbit/stabilizer theorem $\Rightarrow |Hg_i| = |H| \quad \forall i$.
$\Rightarrow |G| = |Hg_1| + \cdots + |Hg_k| = \underbrace{|H| + \cdots + |H|}_{k}$, where $k = |H \backslash G|$.

$\therefore |G| = |H|\,|H\backslash G|.$

G/H is the set of orbits for the action of H on G given by $a \cdot g = ga^{-1}$ $\forall a \in H,\ g \in G$.

"Same" argument shows: $\text{stab}(g) = \{e\}$, hence $|H| = |H \cdot g| = |gH|$ by the orbit/stabilizer theorem.

"Same" counting argument now gives

$$|G| = |H|\,|G/H|.$$

WARNING In general $gH \neq Hg$ and G/H, $H\backslash G$ are two different partitions of G.

Ex $G = S_3$ $H = \langle (12) \rangle = \{id, (12)\}$.

By Lagrange's theorem $|G/H| = |H\backslash G| = \frac{|S_3|}{2} = \frac{6}{2} = 3$

$(12)(13) = \begin{pmatrix} 1\to3\to3 \\ 3\to1\to2 \\ 2\to2\to1 \end{pmatrix} = (132)$, $\Rightarrow H(13) = \{(13), (132)\}$

$\Rightarrow H\backslash G = \{H,\ H(13),$ the rest of $G\}$ $\quad$ ($\{(23), (123)\}$)

$= \{H, \{H(13),\ H(23)\}$.

$G/H = \{H,\ (13)H,$ the rest of $G\}$

$(13)(12) = \begin{pmatrix} 1\mapsto2\mapsto2 \\ 2\mapsto1\mapsto3 \\ 3\mapsto3\mapsto1 \end{pmatrix} = (123)$. $\Rightarrow (13)H = \{(13), (123)\}$

$\Rightarrow G/H = \{\{H, (12)\}, \{(13), (123)\}, \{(23), (132)\}\}$

while

$H/G = \{\{id, (12)\}, \{(13), (132)\}, \{(23), (123)\}\}$.