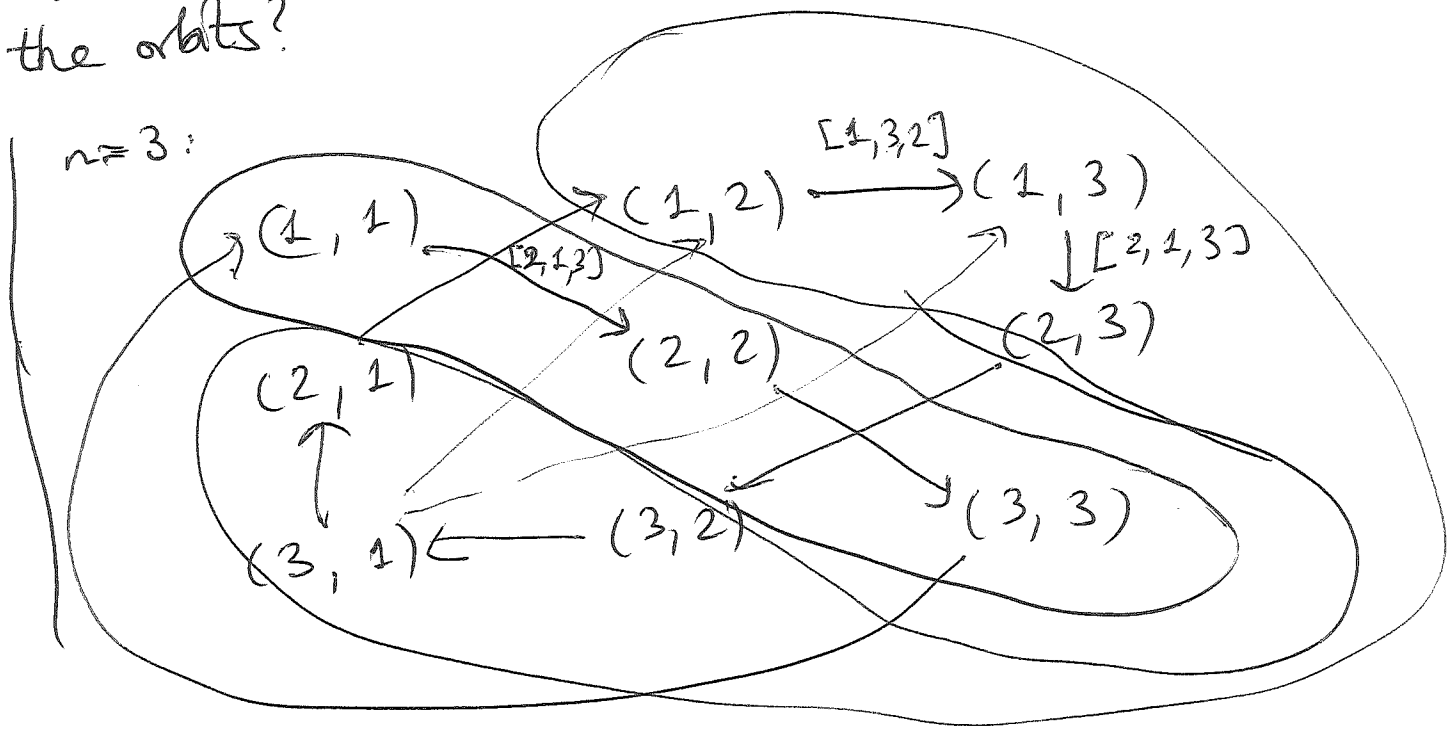
**Recall:** The "Counting Formula" (or Orbit-Stabilizer thm).

(1) If a ~~group~~ finite group $G$ acts on a set $S$, and if $s \in S$, then $|G| = |G_s| \cdot |O_s|$.

**Examples:** (1) Fix $n > 1$. The group $S_n$ acts on the set of all pairs of integers between 1 and $n$. This is the set $[n]^2$, where $[n] = \{1, 2, \dots, n\}$.

$$\sigma * (i, j) = (\sigma(i), \sigma(j))$$ ("elementwise action").

What are the orbits?



There are 2 orbits:

$$\mathcal{O}_{=} = \{(i,i) \mid i \in [n]\};$$

$$\mathcal{O}_{\neq} = \{(i,j) \mid i \neq j\}.$$

What is $G_{(i,i)}$?

$$G_{(i,i)} = \{\sigma \in S_n \mid \sigma(i) = i\}.$$

$$\overset{(1)}{\Longrightarrow} \quad \underbrace{|S_n|}_{= n!} = \underbrace{|\{\sigma \in S_n \mid \sigma(i) = i\}|}_{= |\{\text{permutations of } [n] \setminus \{i\}\}| = (n-1)!} \cdot \underbrace{|\mathcal{O}_{(i,i)}|}_{= \mathcal{O}_{=}, \; = n}$$

$$\Longrightarrow \quad n! = (n-1)! \cdot n.$$

What is $G_{(i,j)}$ for $i \neq j$?

$$G_{(i,j)} = \{\sigma \in S_n \mid \sigma(i) = i \text{ and } \sigma(j) = j\}$$

$\Rightarrow$ (1) $|S_n| = |\{\sigma \in S_n \mid \sigma(i)=i \text{ and } \sigma(j)=j\}| \cdot |\mathcal{O}_{(i,j)}|$

$= n!$ $\qquad = (n-2)!$

$$\Rightarrow |\mathcal{O}_{(i,j)}| = \frac{n!}{(n-2)!} = n(n-1).$$

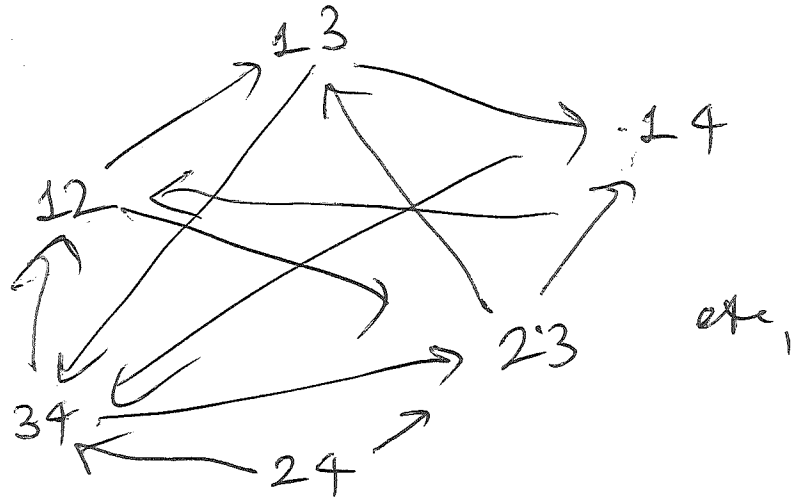
(2) Fix $n \in \mathbb{N}$ and $k \in \{0, 1, \ldots, n\}$.
Let $\mathcal{P}_k$ be the set of all $k$-element subsets of $[n] = \{1, 2, \ldots, n\}$.
We shall prove $|\mathcal{P}_k| = \frac{n!}{k!(n-k)!} = \binom{n}{k}$.

To prove it, consider $S_n$ acting on $\mathcal{P}_k$ by

$$\sigma * S = \sigma(S) = \{\sigma(s) \mid s \in S\}.$$

(because $\sigma * (\tau * S) = (\sigma\tau) * S$).
What are the orbits?

E.g. $n=4$, $k=2$




etc.

Claim 1: $\mathcal{P}_k$ is a single orbit (i.e., the action of $S_n$ on $\mathcal{P}_k$ is transitive).

Proof: Given $S=\{s_1, s_2, \ldots, s_k\}$, $T=\{t_1, t_2, \ldots, t_k\}$ in $\mathcal{P}_k$, we can always find a permutation $\sigma \in S_n$ that sends each $s_i$ to $t_i$. Then, $\sigma * S = T$. □

**Claim 2:** If $S \in \mathcal{P}_k$, then

$$|G_S| = k! \cdot (n-k)!.$$

**Proof:** $G_S = \{\sigma \in S_n \mid \sigma * S = S\}$

$= \{\sigma \in S_n \mid \sigma(s) \in S$ for each $s \in S$; $\sigma(s) \notin S$ for each $s \notin S\}$

$\cong \{\text{permutations of } S\} \times \{\text{permutations of } [n] \setminus S\}$

(isomorphism)

$\Rightarrow |G_S| = \underbrace{|\{\text{permutations of } S\}|}_{=k!} \cdot \underbrace{|\{\text{permutations of } [n] \setminus S\}|}_{=(n-k)!}$

□

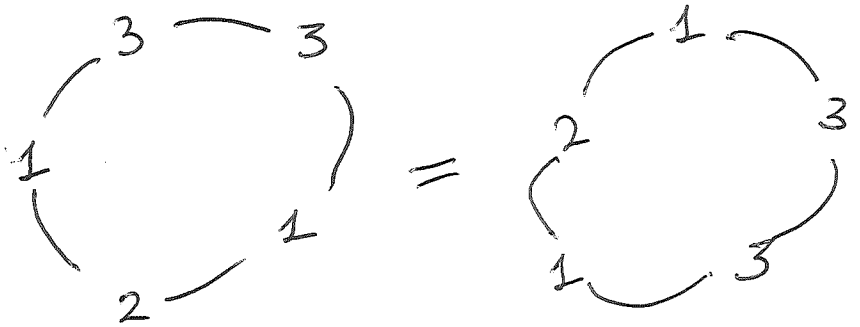
Now, fix $S \in \mathcal{P}_k$.

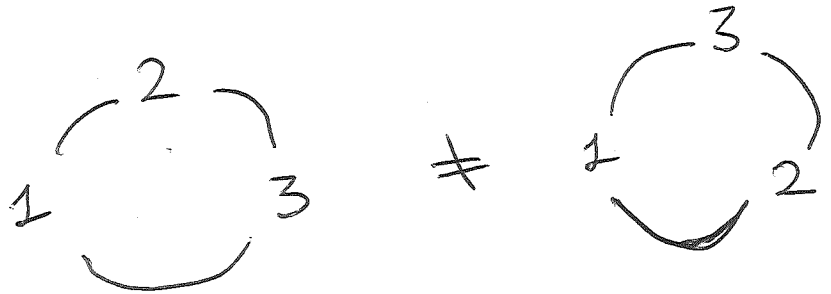
$\overset{(1)}{\Rightarrow} |S_n| = \underbrace{|G_S|}_{=k!(n-k)! \text{ (by Claim 2)}} \cdot |\mathcal{O}_S| = k! \cdot (n-k)! \cdot |\mathcal{P}_k|$ ($\mathcal{P}_k$ (by Claim 1))

$$\Rightarrow \quad |S_k| = \frac{|S_n|}{k!\cdot(n-k)!} = \frac{n!}{k!\cdot(n-k)!}. \qquad \square$$

(3) Let $p$ be a prime, let $q \in \mathbb{N}$.

~~Count~~. Count "necklaces with $p$ beads in $q$ colors".



The cyclic group $C_p = (\mathbb{Z}/p\mathbb{Z})^+$ acts on $[q]^p$ by cyclic rotation:

$$\overline{k} * \omega = \rho^k(\omega),$$

where $\rho((\omega_1, \omega_2, \ldots, \omega_p)) = (\omega_p, \omega_1, \omega_2, \ldots, \omega_{p-1})$.

The necklaces with $p$ beads in $q$ colors are the orbits of this $C_p$-action. How many such necklaces exist?

Consider any $\omega \in [q]^p$ and its orbit $\mathcal{O}_\omega$.

(1) yields $\underbrace{|C_p|}_{=p} = |G_\omega| \cdot |\mathcal{O}_\omega| \Rightarrow |\mathcal{O}_\omega| \mid p$

$$\Rightarrow |\mathcal{O}_\omega| = 1 \text{ or } |\mathcal{O}_\omega| = p.$$

But $|\mathcal{O}_\omega| = 1 \iff \omega = \rho(\omega) \iff \omega = (a, a, \ldots, a)$ for some $a \in [q]$;

thus, there are exactly $q$ orbits of size 1.

So we know:

(# of orbits of size 1) $= q$

and (# of orbits of size 1) + $p \cdot$ (# orbits of size $p$)

$=$ (sum of the ~~lengths of~~ sizes of all orbits)

$= |[q]^p| = q^p$.

Solving this for the #s, you get

$$(\#\text{ orbits of size } p) = \frac{q^p - q}{p}.$$

$$\Rightarrow \boxed{(\#\text{ all orbits}) = q + \frac{q^p - q}{p}}.$$

(Hence, $p \mid q^p - q$, which is Fermat's Little Theorem, for $q \in \mathbb{N}$.)

Remark: Let $G$ be a ~~group~~ group and $S$ a set on which $G$ acts. Let $s$ and $t$ be two elements of $S$ lying in the same orbit. Then, (1) suggests $|G_s| = |G_t|$.

We can prove this more directly:

Let $g \in G$ such that $t = g * s$. Then,

$$G_t = \{h \in G \mid h * t = t\}$$
$$= \{h \in G \mid h * g * s = g * s\}$$
$$= \{h \in G \mid \underbrace{g^{-1} * h * g * s = s}\}$$
$$\Leftrightarrow g^{-1}hg \in G_s$$
$$= \{h \in G \mid g^{-1}hg \in G_s\}$$
$$= \{ghg^{-1} \mid h \in G_s\} = gG_sg^{-1},$$

thus $G_{g*t} \cong G_s$.

General constructions of group actions.

Def. Let $G$ be a group, and $H$ a subgroup of $G$.
Then, $G/H = \{aH \mid a \in G\}$, is the set of all left cosets.

The group $G$ acts on $G/H$ by

$$g * S = \{gs \mid s \in S\} = gS.$$

Thus, for any $a \in G$, we have

$$g * (aH) = gaH.$$

~~This action~~

Prop. 6.8.1. Let $H$ be a subgroup of a group $G$.

(a) The action of $G$ on $G/H$ is transitive (i.e., there is exactly 1 orbit).

(b) ~~For any~~ $G_{1H} = H$.

Proof. (a) If $aH$ and $bH$ are two cosets in $G/H$, then

$$ab^{-1} * bH = a\cancel{b^{-1}}\cancel{b}H = aH.$$

Also, $G/H \neq \emptyset$.

(b) $G_{1H} = \{g \in G \mid g \cdot 1H = 1H\} = \{g \in G \mid g \in H\} = H.$ □

~~Cor.~~ Rmk. Apply (1) in Prop. 6.8.1:

$$|G| = \underbrace{|G_{1H}|}_{=H} \cdot \underbrace{|\mathcal{O}_{1H}|}_{=G/H \text{ (by (2))}} = |H| \cdot \underbrace{|G/H|}_{=[G:H]}$$

$$= |H| \cdot [G:H].$$

Def. Let $G$ be a group.
Let $G$ act on $G$ itself as follows:

$$g * h = ghg^{-1}.$$

("Action by conjugation" or "adjoint action")

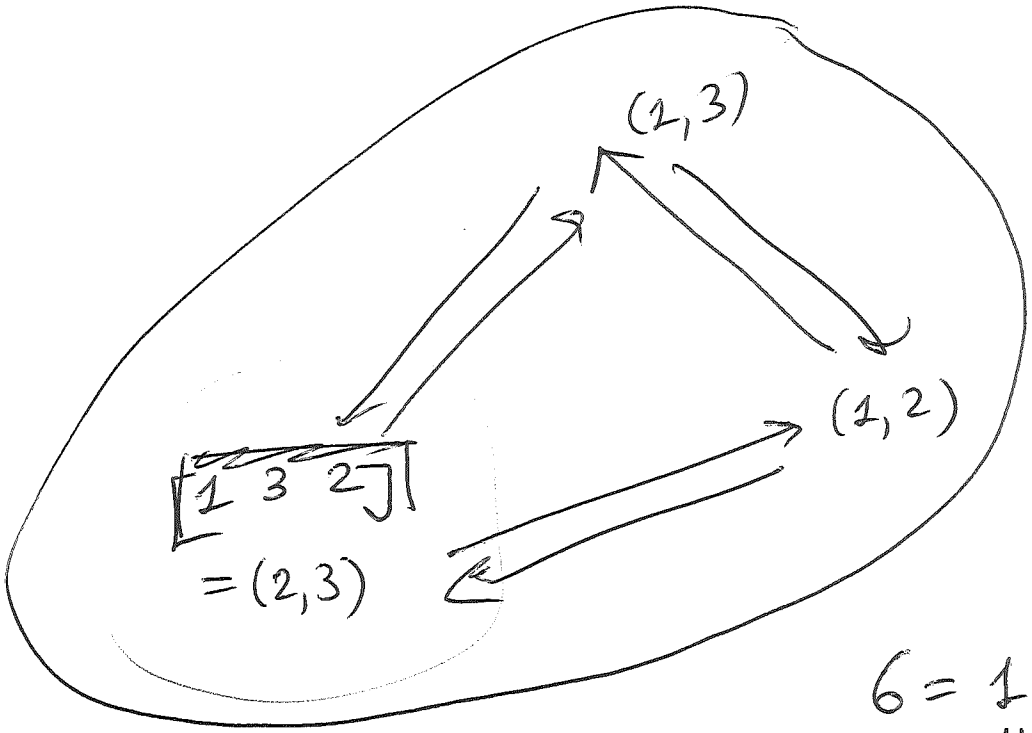
↑ never omit this symbol

Rmk. The orbits of this action are the conjugacy classes of $G$.

Ex: Conjugacy action of $S_n$ on itself:

$$g * \underbrace{(i_1, i_2, \dots, i_k)}_{\text{cyclic perm.}} = (g(i_1), g(i_2), \dots, g(i_k)).$$

Ex: $S_3$




[1 2 3)
=id

$6 = 1 + 2 + 3$
$\| \quad \| \quad \|$
$\frac{6}{6} \quad \frac{6}{3} \quad \frac{6}{2}$

(1,2,3)
=[2 3 1]

(1,3,2)
=[3 1 2]

$g * g = g g g^{-1} = g$