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

If a finite group $G$ acts on a set $S$, and if $s \in S$, then $|G| = |G_s| \cdot |\mathcal{O}_s|.$

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 $[n] = \{1, 2, \ldots, n\}.$

\[ \sigma \star (i, j) = (\sigma(i), \sigma(j)) \] ('element-wise action').

What are the orbits?

\[ n = 3: \]

\[ (1, 1) \rightarrow (1, 2) \rightarrow (1, 3) \rightarrow [2, 1, 3] \]

\[ (2, 1) \rightarrow (2, 2) \rightarrow (2, 3) \rightarrow [3, 2, 1] \]

\[ (3, 1) \rightarrow (3, 2) \rightarrow (3, 3) \]
There are 2 orbits:

\[ O = \{ (i, i) \mid i \in \{1, 2, \ldots, n\} \} \]

\[ O \neq = \{ (i, j) \mid i \neq j \} \]

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

\[ G_{(i,j)} = \{ o \in S_n \mid o(i) = j \} \]

\[ |G_{(i,j)}| = |\text{permutations of } \{1, 2, \ldots, i-1, i+1, \ldots, n\}| = n \]

\[ = (n-1)! \]

\[ \Rightarrow n! = (n-1)! \cdot n. \]

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

\[ G_{(i,j)} = \{ o \in S_n \mid o(i) = i \text{ and } o(j) = j \} \]
\[(1) \quad |S_n| = |\{ \sigma \in S_n \mid \sigma(i) = i \text{ and } \sigma(j) = j^2 \}| \cdot |O_{(i,j)}|\]
\[\Rightarrow \quad n! = (n-2)! \]

\[\Rightarrow \quad |O_{(i,j)}| = \frac{n!}{(n-2)!} = n(n-1),\]

(2) Fix \( n \in \mathbb{N} \) and \( k \in \{0, 1, \ldots, n^2\} \).

Let \( S_k \) be the set of all \( k \)-element subsets of \( \mathbb{N}^2 = \{1, 2, \ldots, n^2\} \).

We shall prove \( |S_k| = \frac{n!}{k!(n-k)!} = \binom{n}{k} \).

To prove it, consider \( S_n \) acting on \( S_k \) by
\[\sigma \ast S = \{ \sigma(s) \mid s \in S \}\]
(k because \( \sigma \ast (\tau \ast S) = (\sigma \tau) \ast S \)).

What are the orbits?
Claim 1: $P_k$ is a single orbit (i.e., the action of $S_n$ on $P_k$ is transitive).

Proof: Given $S = \{s_1, s_2, \ldots, s_k\}$, $T = \{t_1, t_2, \ldots, t_k\} \in P_k$, we can always find a permutation $\sigma \in S_n$ that sends each $s_i$ to $t_i$. Then, $\sigma \ast S = T$. $\Box$
Claim 2: If $S \in \mathcal{P}_k$, then

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

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

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

$$\cong \{ \text{permutations of } S^3 \} \times \{ \text{permutations of } [n] \backslash S^3 \}$$

$$\xrightarrow{\text{isomorphism}} \{ \text{permutations of } S^3 \} \cdot \{ \text{permutations of } [n] \backslash S^3 \}$$

$$= k! \cdot (n-k)! .$$
\[ \Rightarrow |S_k| = \frac{|S_n|}{k!(n-k)!} = \frac{n!}{k!(n-k)!}. \]

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

Count "necklaces with \( p \) beads in \( q \) colors".

\[
\begin{align*}
1 & \quad 3 \\
2 & \quad 1
\end{align*}
\]

\[
\begin{align*}
2 & \quad 1 \\
3 & \quad 3
\end{align*}
\]
The cyclic group $C_p = (\mathbb{Z}/p\mathbb{Z})^*$ acts on $[q]^p$ by cyclic rotation:

$$k \ast \omega = g^k(\omega),$$

where $g((\omega_1, \omega_2, \ldots, \omega_p)) = (\omega_p, \omega_2, \omega_3, \ldots, \omega_{p-1}).$

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 $\omega^T_\omega$.

(1) yields $|C_p| = |G_\omega| \cdot |\omega^T_\omega| \Rightarrow |\omega^T_\omega| \mid p$

$$= p \Rightarrow |\omega^T_\omega| = 1 \text{ or } |\omega^T_\omega| = p.$$

But $|\omega^T_\omega| = 1 \iff \omega = g(\omega) \iff \omega = (a, a, \ldots, a)$ for some $a \in [q]^p$.

Thus, there are exactly $q$ orbits of size 1.
So we know:

\[(\# \text{ of orbits of size } 1) = q\]

and \((\# \text{ of orbits of size } 1) + \frac{q^p - q}{p}\) = (sum of the lengths of sizes of all orbits)

= \(|G_7|^p = q^p|.

Solving this for the \#s, you get

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

\[\Rightarrow (\# \text{ all orbits}) = q + \frac{q^p - q}{p} \]

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

Remark: Let \( G \) be a \( \mathbb{Z}_p \) 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 \( t = g \cdot s \). Then,

\[
G_t = \{ h \in G \mid h \cdot t = t \}
= \{ h \in G \mid h \cdot g \cdot s = g \cdot s \}
= \{ h \in G \mid g^{-1} \cdot h \cdot g \cdot s = s \}
\]

\[
\implies g^{-1} \cdot h \cdot g \in G_s
\]

\[
= \{ h \in G \mid g^{-1} \cdot h \cdot g \in G_s \}
= \{ g \cdot k \cdot g^{-1} \mid k \in G_s \} = g \cdot G_s \cdot g^{-1},
\]

thus \( G \cdot t \cong G_s \).

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
\[ g \ast H = \{ gh \mid h \in H \} = gH. \]
Thus, for any $a \in G$, we have
\[ g \ast (aH) = gaH. \]

**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 one orbit).

(b) $G_1H = H$.

**Proof.** (a) If $aH$ and $bH$ are two cosets in $G/H$, then
\[ ab^{-1} \ast H = a(b^{-1}b)H = aH. \]
Also, $G/H \neq \emptyset$.

(b) $G_1H = \{ g \in G \mid g \cdot 1H = 1H \} = \{ g \in G \mid g \in H \} = H$. \(\square\)
***Rmk.*** Apply (1) in Prop. 6.8.1:

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

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

---

**Def.** Let \( G \) be a group:

Let \( G \) act on \( G \) itself as follows:

\[ g \ast h = ghg^{-1} \]

("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:

\[ g \ast (i_1, i_2, \ldots, i_k) = (g(i_1), g(i_2), \ldots, g(i_k)) \]

\[ \text{cyclic perm.} \]
Example: $S_3$

$\begin{bmatrix} 1 & 2 & 3 \\ = \text{id} \end{bmatrix}$

$(1, 2, 3)$

$= (2, 3)$

$= (1, 2)$

$6 = 1 + 2 + 3$

$\begin{bmatrix} 6 & 6 & 6 \\ = \frac{6}{3} & \frac{6}{2} \end{bmatrix}$

$(1, 2, 3)$

$= [231]$

$(1, 3, 2)$

$= [3412]$

$g * g = g \neq g$