Consider the conjugation action of $G$ on itself:
\[ c: G \rightarrow \text{Aut}(G) \]
\[ g \mapsto C_g = g x g^{-1} \]

Recall: stabilizers of this action is the centralizer:
\[ C(x) = \{ g \in G \mid g x g^{-1} = x \} \]

orbits of this action are called conjugacy classes:
\[ [x] = \{ g x g^{-1} \mid g \in G \} \]

Center of $G = \text{Ker}n$el of this action:
\[ Z(G) = \{ g \in G \mid g x g^{-1} = x \text{ for all } x \in G \} \]
\[ = \{ z \in G \mid [z] = \{ z \} \} \]

Also recall: the orbits of a $G$-action on a set $X$ form a partition of $X$.
\[ \Rightarrow \text{conjugacy classes are a partition of } X. \]

Class Equation:
\[ |G| = |Z(G)| + \sum_{G \setminus Z(G)} \frac{|G|}{|C(g)|} \]

Proof:
\[ |G| = |Z(G)| + \sum_{C(g)} \frac{|G|}{|C(g)|} \]

\[ = \sum_{\text{conjugacy classes}} \frac{|G|}{|C(g)|} \]

\[ = \sum_{\text{conjugacy classes of size } 1} \frac{|G|}{|C(g)|} \geq 1 \]
Example:

- \( G = S_3 \)  recall: conjugacy class of permutations is determined by its cycle type.

conjugacy classes:

\[ Z(S_3) = \{ e \} \]
\[ \{ (12), (13), (23) \} \]
\[ \{ (123), (132) \} \]

\[ G = 1 + 3 + 2 \]  

- \( G = D_4 = \{ e, r, r^2, r^3, j, rj, r^2j, r^3j \} = \langle r, j | r^4 = e, j^2 = r^2, rj = jr^-1 \rangle \)

conjugacy classes? « use \( jrj = r^3 \) »

\[ 2(D_4) \]
\[ \{ e, 3 \} \]
\[ \{ r^2j \} \]
\[ \{ r, r^3j \} \]
\[ \{ j, r^2j \} \]
\[ \{ rj, r^3j \} \]

\[ 2(D_4) \]

\[ \{ e, 3 \} \]
\[ \{ r^2j \} \]
\[ \{ r, r^3j \} \]
\[ \{ j, r^2j \} \]
\[ \{ rj, r^3j \} \]

Note: we know the subgroups of \( D_4 \) are abelian.

in general: if \( x \in G \) \( \langle x \rangle \leq C(x) \) combine the 2 facts you see that \( |C(x)| \) has order 4

if \( x \notin \eta(D_4) \)

=> conjugacy classes have size 2

For this might be better to leave it as "direct check" which is also not hard...
What does this tell us about structure of groups?

Recall: \( |G| = p \) a prime then

Lagrange's theorem \( \Rightarrow G \cong \mathbb{Z}_p. \)

What if \( |G| = p^2 \)?

**Proposition:** if \( |G| = p^n, \ n \geq 1 \), then \( |Z(G)| > 1 \)

(i.e. center contains a nonidentity element.

**Proof:** the class equation tells us:

\[
|G| = |Z(G)| + \sum_{c\neq 1} \frac{|G|}{|c|}
\]

divisible by \( p \)

\( \frac{|G|}{|c|} \) divisible by \( p \) since

\[ \frac{16}{|c|} \gg 1 \] and it divides \( p^a. \)

\( \Rightarrow |Z(G)| \) divisible by \( p \) \( \Rightarrow |Z(G)| > p > 1. \) \( \square \)
Proposition: If $|G| = p^2$, $p$ a prime, then $G$ is isomorphic to either $Z_{p^2}$ or $Z_p \times Z_p$.

Proof: For any $g \in G$, $o(g) | p^2 \Rightarrow o(g) = 1, p, p^2$

If $o(g) = 1 \Rightarrow g = e$

If $o(g) = p^2 \Rightarrow G \cong Z_{p^2}$.

Suppose $G \not\cong Z_{p^2}$, then $o(g) = p \nRightarrow g \neq e$ in $G$.

By previous proposition, $|Z(G)| > 1$. Let $g$ be a nonidentity element in $Z(G)$.

Since $g \in Z(G)$, $gh = hg \forall h \in G$, i.e., commutes with all elements of $G$.

Let $h \in G \setminus \langle g \rangle$. Then $o(h) = p$ and we must have $\langle g \rangle \cap \langle h \rangle = \{e\}$.

Since $\langle g \rangle \cap \langle h \rangle \subseteq \langle g \rangle$, if $|\langle g \rangle \cap \langle h \rangle| \neq 1$ it must be $p$.

$\Rightarrow \langle g \rangle \cap \langle h \rangle = \langle g \rangle$

$\therefore \langle h \rangle \not\subseteq \langle g \rangle$.

It follows that $|\langle g \rangle \langle h \rangle| = p^2 \Rightarrow G = \langle g \rangle \langle h \rangle$.

Since $g, h$ commute with each other $\Rightarrow G$ abelian

$\Rightarrow \langle g \rangle, \langle h \rangle$ both normal

$\Rightarrow G \cong \langle g \rangle \times \langle h \rangle \cong Z_p \times Z_p$. $\square$
Recall: Lagrange \( \Rightarrow H \leq G \) then \( |H| \) divides \( |G| \).

Converse not necessarily true. 

But actually in all of our examples so far it does hold. Let’s give one.

**Example:** \( A_4 \) contains no subgroup of order 6.

**Proof:**

1. If \( H \trianglelefteq A_4 \) has order 6, then \( H \) is normal (it has index 2).
2. So \( A_4 / H \) is a group of order 2.
3. If \( x \in A_4 \) then \( x^2 \in H \) (since \( (xH)^2 = eH \) in \( A_4 / H \)).
4. If \( x \in A_4 \) has order 3, then \( x = (x^2)^2 \in H \).

This means there are \( \leq 6 = |H| \) elements of order 3.

This is a contradiction since

\[
(123) \quad (124) \quad (134) \quad (234) \\
(132) \quad (142) \quad (143) \quad (243)
\]

all have order 3!

Next:

Sylow Theorems which are a kind of converse.