Last time: Semidirect products

Thm (Cayley's Thm) Every finite gp $G$ is isom to a subgroup $S_n$ for some $n$. If $|G| = n$, then $G$ is isom to a subgroup of $S_n$.

Def 1 A permutation repn of a gp $G$ is $\phi: G \to S_n$, a homom.

Proof $G$ a gp. There is a bijective corr between perm repns of $G$ and actions of $G$ on $\{1, 2, \ldots, n\}$.

Pf: Suppose $G \subseteq \{1, 2, \ldots, n\}$.

For each $g$, have $m_g: \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$

Define $\phi: G \to S_n$ or $\phi(g) = m_g$

$$\phi(g_1 g_2) = m_{g_1 g_2} = m_{g_1} \circ m_{g_2} = \phi(g_1) \phi(g_2)$$

action

Conversely, suppose $\phi: G \to S_n$ is a homom. Then define $m_g: \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ as $m_g = \phi(g)$.

This defines an action $G$ as $\{1, 2, \ldots, n\}$.

Cor Let $\text{Perm}(S)$ denote the gp of permutations of a set $S$. Then, there is a bijective correspondence between actions of a gp $G$ on $S$ and homom $\phi: G \to \text{Perm}(S)$. 
actions of a group $G$ on a set $S$ and homomorphism $\phi: G \rightarrow \text{Perm}(S)$.

**Def:** An action is said to be **faithful** if
gs = s \quad \forall s \in S \implies g = 1.
Equivalently, $\ker \phi \cap G = \{1\}$.

**Pf of Cayley's Thm**

- $S = G * G$ by left multiplication
- This defines $\phi: G \rightarrow \text{Perm}(S) \cong S_n$ if $|G| = n$.
- $G * G$ by left mult is faithful
- $\implies \phi: G \rightarrow S_n$ is injective
- $\implies G \leq \text{S}(G)$ as desired.

---

An important action of $G$ on itself: $G * G$ by conjugation:
g * x = gxg^{-1}, \quad g \in G, \quad x \in G

The stabilizer of an element $x \in G$ for this action is

$\mathcal{Z}(x) = \{ g \in G : gxg^{-1} = x \} = \{ g \in G : gx = xg \}$
called the **centralizer** of $x$. 
The orbit of an elt \( x \in G \) for this action is
\[
C(x) = \{ x' \in G : \exists g \in G \text{ st. } x' = gxg^{-1} \}
\]
called the conjugacy class of \( x \).

Counting formula: \( |G| = |C(x)|/|Z(x)| \)

Also, the conj. classes partition \( G \)

(\( \phi \)) \( |G| = \sum_{C_j} |C_j| = |C_1| + |C_2| + \ldots + |C_k| \)

\( C \) a conj. class \( C_j \) are the conj. classes

Moreover, the \( |C_j| \) divide \( |G| \),
This eqn (\( \phi \)) is called the class eqn of \( G \).

\textbf{Proof:} \( \phi \)
\begin{enumerate}
\item \( Z(x) \) contains \( x \), and contains the center \( Z \) of \( G \).
\item \( x \in G \) is in \( Z \), the center \( c \mapsto Z(x) = \{ c \} \Rightarrow C(x) = \{ x \} \).
\end{enumerate}

\textbf{Example of class eqn,}
\[ G = S_3, \quad 1, x, y \]
\[
\text{• } Z(x): \text{ken}\ s \lfloor Z(x) \cap \{ 1 \} = 6, \ \text{ken}\ Z(x) \text{ contains}
1, x, x^2
\]
But \( y \notin Z(x) \) because \( yx \neq xy \)
But $y \not\in Z(x)$ because $xy \neq xy$

$\implies Z(x) = \{1, x, x^2\}$ has size 3,
$\implies |C(x)| = 2$

$\implies Z(y)$: know it contains 1, y. $x \not\in Z(y)$

$\implies |Z(y)| = 2 \implies |C(y)| = 3.$

$\implies 6 = |S_3| = 1 + 2 + 3$

---

**$p$-gps**

A gp $G$ is called a $p$-gp if $|G| = p^n$ for some prime $p$.

**Prop.** The center of a $p$-gp is not trivial.

**Pr.:** Consider the class eqns.

\[ p^n = |G| = 1 + |C_1| + |C_2| + \ldots + |C_r| \]

for the identity

Sizes of $|C_j| \mid p^n \implies$ if $|C_j| \neq 1$ then $d$ is div by $p$.

$\implies \exists j \mid |C_j| = 1$. $\implies$ center is nontrivial.

More generally

**Thm.** (Fixed pt Thm.) $G \cap S$, $G$ a $p$-gp, $|S|$ finite
**Prop.** Every gp of order \( p^2 \) is abelian.

---

**Proof:** \( G \) a gp of order \( p^2 \). \( Z(G) \neq \{1\} \).

\[ \Rightarrow |Z(G)| = p \text{ or } p^2. \]

Assume for sake of contradiction \( |Z(G)| = p \).

Then \( \exists x \in G \text{ with } x \notin Z(G) \).

Then \( Z(x) \in Z(G) \Rightarrow |Z(x)| > p \Rightarrow |Z(x)| = p^2 \Rightarrow Z(x) = G \Rightarrow xZ(G) = G. \]
Cor. If \( |G| = p^2 \), then either \( G \) is cyclic of order \( p^2 \) or \( G \) is a product of two cyclic groups of order \( p \).

**PF:** Every elt of \( G \) has order 1, \( p \), or \( p^2 \).

1. If \( G \) has an elt of order \( p^2 \), then \( G \cong C_{p^2} \) and we're done.
2. Otherwise, every elt \( 
eq 1 \) in \( G \) has order \( p \).

Let \( x \in G \) be such an elt. \( \langle x \rangle \neq G \)

Let \( y \in G \) be an elt not in \( \langle x \rangle \).

**Claim:** \( \langle x \rangle \times \langle y \rangle \rightarrow G \)

**PF:** \( \times \) is a gp homom because \( x \times y \) commute.

- Image is subgroup \( G \nsubseteq \langle x \rangle \Rightarrow \text{image is } G \)
- Map is surj gp homom \( \Rightarrow \) isom \( G / \ker \text{ both sides \ have size } p^2 \).