Recall that given a left action $G \times X \to X$ of a group $G$ on a set $X$, the orbit of $x \in X$ is

$$G \cdot x = \{ g \cdot x \mid g \in G \}.$$ 

There is a canonical bijection

$$G/G_x \to G \cdot x \quad aG_x \leftrightarrow a \cdot x$$

where

$$G_x = \{ g \in G \mid g \cdot x = x \} = \text{the stabilizer of } x.$$ 

**Def.** A point $x \in X$ is a **fixed point** of the action $G \times X \to X$ if $g \cdot x = x$ for all $g \in G$.

(equivalently $G \cdot x = \{ x \}$, equivalently $G_x = G$)

**Ex.** $S_n$ acts on $\mathbb{R}^n$ by $\sigma \cdot (x_1, \ldots, x_n) = (x_{\sigma^{-1}(1)}, \ldots, x_{\sigma^{-1}(n)})$.

$x = (x_1, \ldots, x_n)$ is a fixed point $\iff x_1 = x_2 = \cdots = x_n$.

**Ex.** If a group $G$ acts on $G$ by left multiplication, $a \in G$ is fixed $\iff$ $ga = a \quad \forall g \\
\implies g = e$. 

So if $G \neq \{e\}$, there are no fixed points.

**Ex.** A group $G$ acts on itself by conjugation:

$$G \times G \to G \quad g \cdot a = ga g^{-1}.$$ 

$a \in G$ is fixed $\iff g a g^{-1} = a \quad \forall g \in G$ 

$\implies ga = ag \quad \forall g$. 

The set of all fixed points for conjugation is $Z(G) = \{ a \in G \mid ga = ag \quad \forall g \in G \}$.

**HW** $Z(G)$ is a normal subgroup, it's called the **center** of $G$. 

The stabilizers for the action of conjugation also have a name:  if \( G \) acts on \( G \) by conjugation, \( x \in G \)

\[
G_x = \text{Cent}_G(x) = \{ g \in G \mid gxg^{-1} = x \}
\]

The centralizer of \( x \).

**Note:** \( x \in Z(\text{Cent}_G(x)) \)

---

**Proposition 18.1** (compare with Goodman, 5.4.2)

Suppose \( G \) is a finite group and \( |G| = p^k \), \( p \) prime \( k \in \mathbb{N} \).

Then \( p \mid |Z(G)| \). In particular \( |Z(G)| \geq p \).

The proof uses the so called class equation:

Suppose \( G \) is a finite group. Then conjugation has finitely many orbits. In particular there are finitely many orbits \( O_i \). On with \( |O_i| \geq 1 \). The rest of the orbits are singletons. Their union is \( \mathbb{Z}(G) \).

Choose \( x_i \in O_i \), \( i = 1, \ldots, n \). Then

\[
|G| = |Z(G)| + \sum_{i=1}^n |G \cdot x_i|
\]

Since \( |G \cdot x_i| = |G/G_{x_i}| = |G/\text{Cent}(x_i)| = \frac{|G|}{|\text{Cent}(x_i)|} \)

\[
\Rightarrow |G| = |Z(G)| + \sum_{i=1}^n \frac{|G|}{|\text{Cent}(x_i)|}
\]

The class equation.

**Proof of 18.1** By the class equation

\[
p^k = |Z(G)| + \sum_{i=1}^n \frac{p^k}{|\text{Cent}(x_i)|}
\]

Since \( |G/\text{Cent}(x_i)| \geq 1 \) and since \( p^k = \left[ \frac{p^k}{|\text{Cent}(x_i)|} \right] |\text{Cent}(x_i)| \)

\[
p \mid \left[ \frac{p^k}{|\text{Cent}(x_i)|} \right] + 1
\]
Proposition 18.2 (compare with 5.4.3 in Goodman)

Suppose \( p \) is prime, \( G \) a group with \( |G| = p^2 \). Then either \( G \cong \mathbb{Z}/p^2 \) or \( G \cong \mathbb{Z}/p \times \mathbb{Z}/p \).

In particular \( G \) is abelian.

Proof

Since \( |G| = p^2 \), \( \forall g \in G, g \neq e \), \( |\langle g \rangle| \) is \( p \) or \( p^2 \).

If \( |\langle g \rangle| = p^2 \), \( G = \langle g \rangle \). \( \Rightarrow \) \( G \cong \mathbb{Z}/p^2 \).

Now suppose \( \exists g \in G \) sat \( G = \langle g \rangle \). Then \( \forall g \in G, g \neq e \) \( |\langle g \rangle| = p \).

Note: If \( h \neq e \) and \( h \notin \langle g \rangle \), then \( \langle h \rangle \cap \langle g \rangle = \{e\} \).

Reason: \( |\langle h \rangle \cap \langle g \rangle| \) \( |\langle g \rangle| = p \). \( \Rightarrow \) \( |\langle h \rangle \cap \langle g \rangle| = 1 \) or \( p \).

If \( |\langle h \rangle \cap \langle g \rangle| = p \), \( \langle h \rangle \cap \langle g \rangle = \langle g \rangle \). \( \Rightarrow \) \( h \in \langle g \rangle \),

which is a contradiction. \( \square \)

Now by 18.1, \( |Z(G)| \geq p \). Pick \( g \in Z(G), g \neq e \).

By assumption \( |\langle g \rangle| = p \). Pick \( h \in G \setminus \langle g \rangle \).

Then \( \langle h \rangle \cap \langle g \rangle = \{e\} \).

Also, since \( g \in Z(G), \langle g \rangle \leq Z(G) \)

\((\text{for example since } \mathbb{Z}/G \text{ is a subgroup})\)

\(\Rightarrow \forall k, k' \in \mathbb{Z}, h^k g^l = g^l h^k.\)

Now consider \( f: \langle h \rangle \times \langle g \rangle \rightarrow G \)

\( f(h^k, g^l) = h^k g^l \)

\( f \) is a homomorphism:

\[ f((h^k g^l)(h^{r}, g^s)) = f(h^{k+r}, g^{l+s}) = h^{k+r} g^{l+s} = h^k g^l h^r g^s = f(h^k, g^l) f(h^r, g^s) \]
\( \ker f = \{ (h^k, g^l) \mid h^k \cdot g^l = e \} \)
\( = \{ (h^k, g^l) \mid (h)^k = g^{-l} e < g > \} \)
\( = \{ (e, e) \} \quad \text{since} \quad (h) \cap < g > = \{ e \}. \)

\( |< h > \times < g > | = |< h >| \cdot |< g >| = p \cdot p \)
\( f \) is injective \( \Rightarrow \quad |f(< h > \times < g >)| = p^2 \)
\( \Rightarrow \quad f(< h > \times < g >) = G \)
\( \Rightarrow \quad f: < h > \times < g > \rightarrow G \) is an \( \infty \)o.

\( \text{Suppose} \quad < h > \cong \mathbb{Z}/p, \quad < g > \cong \mathbb{Z}/p \)
\( G \cong \mathbb{Z}/p \times \mathbb{Z}/p. \)

---

Next time:

\underline{Cauchy's Theorem}

Suppose \( G \) is a finite group, \( p \) is prime and \( p \mid |G|. \)
Then \( \exists g \in G \) s.t. \( |< g > | = p. \)

Our proof of Cauchy's will use

\underline{Observation}

Suppose \( G \) is a group, \( a, b \in G \) \( ab = e. \)
Then: \( ba = e. \)

Proof

\( ab = e \Rightarrow b = a^{-1}. \Rightarrow ba = a^{-1} a = e. \)

Compare with: \( f, h: X \rightarrow X \) two maps, \( f \circ h = \text{id}, \)
\( \Rightarrow \quad h \circ f = \text{id}. \)