Recall

The center $Z(G)$ of a group G is defined to be

$$Z(G) = \{ x \in G \mid gxg^{-1} = x \ \ \forall g \in G \}$$

$Z(G)$ is a normal subgroup of G; $Z(G)$ is abelian.

Recall also: Given an action $G \times X \to X$ of a group on a set, $x \in X$ is a fixed point [for the action] if $g \cdot x = x \ \ \forall g \in G$

Equivalently, $G \cdot x = \{x\}$.

Equivalently $\mathrm{Stab}(x) = G$.

Notation X^G = set of all fixed points

$$= \{ x \in X \mid g \cdot x = x \ \ \forall g \in G \}$$

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

$x = (x_1, \dots x_n) \in \mathbb{R}^n$ is a fixed point $\Leftrightarrow$

$$(x_1 \dots x_n) = (x_{\sigma^{-1}(1)}, \dots x_{\sigma^{-1}(n)}) \quad \forall \sigma \in S_n$$

$\Leftrightarrow x_1 = x_2 \dots = x_n$

$\therefore (\mathbb{R}^n)^{S_n} = \{ (x_1, \dots x_n) \in \mathbb{R}^n \mid x_1 = x_2 = \dots = x_n \}$.

Ex A group G acts on itself by conjugation:

$$g \cdot x = g x g^{-1}$$

$$G^G = \{ x \in G \mid gxg^{-1} = x \ \ \forall g \in G \} = Z(G).$$

Ex G acts on itself by left multiplication:

$$g \cdot x = gx$$

$$G^G = \{ x \in G \mid gx = x, \ \forall g \in G \} = \emptyset \quad (\text{unless } G = \{e\})$$

Notation Let G act on itself by conjugation. The stabilizer of $x \in G$ is $\mathrm{stab}(x) = \{ g \in G \mid gxg^{-1} = x \}$

Just for this action (conjugation) Stab(x) is called the centralizer of x and is denoted by Cent(x).
The orbit of x is called the conjugacy class of x.

Ex $G = S_n$, $x = (n-1\ n)$

Conjugacy class of $(n-1\ n) = \{\sigma(n-1\ n)\sigma^{-1} \mid \sigma \in S_n\}$

$= \{(\sigma(n-1)\ \sigma(n)) \mid \sigma \in S_n\}$

$=$ the set of all transpositions.

$\text{Cent}((n-1, n)) = \{\sigma \in S_n \mid (\sigma(n-1), \sigma(n)) = (n-1\ n)\}$

$\cong S_{n-2} \times \langle (n-1\ n) \rangle$

Note: Orbit/stabilizer thm $\Rightarrow$

there is a bijection $G/\text{Cent}(x) \to$ conj class of x

So in case of S_n and $x = (n-1\ n)$

\# of transpositions $= \binom{n}{2}$, $\quad |S_n| / |S_{n-2}| \times 2 = \dfrac{n!}{(n-2)!\,2}$ ✓

Remark $x \in Z(G) \iff$ conjugacy class of x is $\{x\}$.

Theorem (the class equation) Let G be a finite group, $G\cdot a_1, \ldots G\cdot a_n$ the full list of distinct conjugacy classes with $|G\cdot a_i| > 1$ (ie $a_i \notin Z(G)\ \forall i$). Then

$$|G| = |Z(G)| + \sum_{i=1}^{n} |G\cdot a_i| = |Z(G)| + \sum_{i=1}^{n} \frac{|G|}{|\text{Cent}(a_i)|}.$$

Proof Orbits for conjugation partition G and

$$|G\cdot a_i| \underset{\text{orbit/stabilizer}}{=} |G/\text{Stab}(a_i)| \underset{\text{Lagrange}}{=} |G| / |\text{Stab}(a_i)|$$

$\square$

Note: If G is abelian, $Z(G) = G$ and the class equation reduces to $|G| = |Z(G)|$

Proposition 17.1 Let G be a finite group with $|G| = p^k$ for some prime p and $k \geq 1$. Then $p \mid |Z(G)|$. In particular $|Z(G)| \geq p$.

Proof If $G = Z(G)$, nothing to prove: $|Z(G)| = p^k$.

Suppose $Z(G) \neq G$. Then $\exists n \geq 1$, $a_1 \ldots a_n \notin G$ s.t. $Cent(a_i) \neq G$. Now apply the class equation. We set

$$p^k = |G| = |Z(G)| + \sum_{i=1}^{n} |G/Cent(a_i)|$$

Lagrange's thm $\Rightarrow$ $|G/Cent(a_i)| \cdot |Cent(a_i)| = |G| = p^k$.

$\Rightarrow p \mid (|G/Cent(a_i)|) \ \forall i$.

$\Rightarrow p \mid |Z(G)| = |G| - \sum_{i=1}^{n} |G/Cent(a_i)|$

Since $|Z(G)| \neq 0$, $|Z(G)| = p \cdot m$ for some $m \in \mathbb{Z}$.

On the other hand $|Z(G)| \mid |G| = p^k$. $\Rightarrow$ $|Z(G)| = p^\ell$ for some $1 \leq \ell < k$. $\square$

Corollary 17.2 Suppose p is prime and G is a group with p^2 elements. Then $G \cong \mathbb{Z}_{p^2}$ or $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$.

Proof Let $g \in G$, $g \neq e$. Then $|\langle g \rangle| \mid |G| = p^2$.

$\Rightarrow |\langle g \rangle| = p$ or p^2.

If $\exists g \in G$ s.t. $|\langle g \rangle| = p^2$ Then $G = \langle g \rangle$ and $G \cong \mathbb{Z}_{p^2}$.

Otherwise $g \in G, g \neq e \Rightarrow |\langle g \rangle| = p$.

By 17.1 $|Z(G)| > 1$. $\Rightarrow \exists g \in Z(G)$ s.t. $g \neq e$.

Since $|\langle g \rangle| = p$, and $|G| = p^2$, $\exists h \in G$ s.t. $h \notin \langle g \rangle$.

Then $|\langle h \rangle| = p$ as well.

Since $h \notin \langle g \rangle$, $\langle h \rangle \cap \langle g \rangle \neq \langle g \rangle$.

On the other hand, $\langle h \rangle \cap \langle g \rangle$ is a subgroup of $\langle g \rangle$.

Since $|\langle g \rangle| = p$, $|\langle h \rangle \cap \langle g \rangle| \mid p$ and $\langle h \rangle \cap \langle g \rangle \neq \langle g \rangle$

$|\langle h \rangle \cap \langle g \rangle| = 1$.

$\Rightarrow \langle h \rangle \cap \langle g \rangle = \{e\}$.

Since $g \in Z(G)$, $h g h^{-1} = g$. $\Rightarrow h g^k h^{-1} = g^k \ \forall k$

$\Rightarrow h^\ell g^k h^{-\ell} = g^k \quad \forall k, \ell.$

$\Rightarrow f: \langle h\rangle \times \langle g\rangle \longrightarrow G, \quad f(h^\ell, g^k) = h^\ell g^k$

is a homomorphism:

$$f((h^\ell, g^k)(h^{\ell'}, g^{k'})) = f(h^{\ell+\ell'}, g^{k+k'}) = h^{\ell+\ell'} g^{k+k'}$$
$$= h^\ell g^k h^{\ell'} g^{k'} = f(h^\ell, g^k) f(h^{\ell'}, g^{k'}).$$

$\ker f = \{(h^\ell, g^k) \mid h^\ell g^k = e\}$

$h^\ell g^k = e \Rightarrow h^\ell = g^{-k} \in \langle h\rangle \cap \langle g\rangle = \{e\}$

$\Rightarrow \ker f = \{(e,e)\} \Rightarrow f$ is injective

$|\langle h\rangle \times \langle \ell\rangle| = p \times p = p^2$

$\Rightarrow f$ is surjective, hence an isomorphism

Since $\langle h\rangle \cong \mathbb{Z}_p \cong \langle g\rangle$, we're done:

$G \cong \langle g\rangle \times \langle h\rangle \cong \mathbb{Z}_p \times \mathbb{Z}_p$ $\square$

Next time

Thm (Cauchy) Let G be a finite group. Suppose a prime p divides $|G|$. Then $\exists a \in G$, $a \neq e$ s.t. $a^p = e$.

(i.e. $\exists a \in G$ s.t. $|\langle a\rangle| = p$).