Theorems with group actions on finite groups

① **Cauchy's Theorem:** If $p \mid |G|$ for prime p, then G has an element of order p. (or equivalently a subgroup of order p).

Proof: Will make $\mathbb{Z}/p$ (not G) act on a set and use fixed-point congruence

$|X| \equiv |\mathrm{Fix}_{\mathbb{Z}/p}(X)| \bmod p$.

Let $X = \{(g_1, \ldots, g_p) \in G^p : g_1 g_2 \cdots g_p = 1\}$ $\quad g_p = (g_1 g_2 \cdots g_{p-1})^{-1}$

$|X| = |G|^{p-1} \equiv 0 \bmod p$. Bring in group action:

$g_1 g_2 \cdots g_p = 1 \Rightarrow g_1 (g_2 \cdots g_p) = 1$

$\Rightarrow (g_2 \cdots g_p) g_1 = 1 \Rightarrow g_2 g_3 \cdots g_p g_1 = 1$

If $(g_1, \ldots, g_p) \in X \Rightarrow (g_2, \ldots, g_p, g_1) \in X \Rightarrow (g_3, \ldots, g_p, g_1, g_2) \in X$, etc.

All cyclic shifts of $(g_1, \ldots, g_p) \in X$ are in X.

Let $\mathbb{Z}/p$ act on X by $(j \bmod p) \cdot (g_1, \ldots, g_p) = (g_{1+j}, \ldots, g_{p+j})$

view indices as in $\mathbb{Z}/p$

Check this is action of $\mathbb{Z}/p$ on X:

- $(0 \bmod p)(g_1, \ldots, g_p) = (g_1, \ldots, g_p)$ ✓
- $(a \bmod p)[(b \bmod p)(g_1, \ldots, g_p)] = (a \bmod p)(g_{1+b}, \ldots, g_{p+b})$

$= (g_{1+b+a}, \ldots, g_{p+b+a})$ ✓

$[(a \bmod p) + (b \bmod p)](g_1, \ldots, g_p) = (a+b \bmod p)(g_1, \ldots, g_p)$

$= (g_{1+a+b}, \ldots, g_{p+a+b})$ ✓

From $\underbrace{|X|}_{\substack{\equiv 0 \bmod p \\ \text{from above}}} \equiv |\mathrm{Fix}_{\mathbb{Z}/p}(X)| \bmod p \Rightarrow p \mid |\mathrm{Fix}_{\mathbb{Z}/p}(X)|$

What is a fixed point $(g_1, \ldots, g_p)$?

It means $(g_1, \ldots, g_p) = (g_{1+j}, \ldots, g_{p+j})$ $\forall j$

$\Rightarrow$ all of $g_1, \ldots, g_p$ are equal!

Thus, $\mathrm{Fix}_{\mathbb{Z}/p}(X) = \{(g, g, \ldots, g) \in X : g \in G\}$.

$\hookrightarrow g^p = 1$

□

continued

$\boxed{\text{(2) Theorem: For all nontrivial } p\text{-groups } G,\ Z(G) \neq \{1\}.}$

Proof: Let G act on G by conjugation, so the fixed points $= Z(G)$.

Fixed point congruence says here: $|G| \equiv |Z(G)| \bmod p$.

$|G| \equiv 0 \bmod p$ since G is a p-group, so $|Z(G)| \equiv 0 \bmod p \Rightarrow$

$p \mid |Z(G)|$. Since $|Z(G)| \geq 1$ and $p \mid |Z(G)|$, we get $|Z(G)| \geq p$.

Therefore, $Z(G) \neq \{1\}$. $\square$

$\boxed{\text{(3) Theorem: If } |G| = p^2, \text{ then } G \cong \mathbb{Z}/p^2 \text{ or } \mathbb{Z}/p \times \mathbb{Z}/p.}$

Proof: Since $|G| = p^2$ for p prime, we know that G is abelian.

- If G is cyclic, then $G \cong \mathbb{Z}/p^2$: $G = \langle g \rangle \Rightarrow$ there is a homomorphism $\mathbb{Z} \to G$ where $k \mapsto g^k$. It kills $p^2\mathbb{Z}$ (g has order p^2), so we get induced homomorphism $\mathbb{Z}/p^2 \to G$ where $k \bmod p^2 \longmapsto g^k$.
  This is onto, $|\mathbb{Z}/p^2| = |G|$, so it is 1-1. Therefore, $G \cong \mathbb{Z}/p^2$.
- If G is not cyclic, then $G \cong \mathbb{Z}/p \times \mathbb{Z}/p$:
  No element has order p^2: all $g \neq 1$ in G have order p.
  Pick $x \in G - \{1\}$, so $\langle x \rangle$ has order p.
  Pick $y \in G - \langle x \rangle$, so $\langle y \rangle$ has order p, and $\langle x \rangle \cap \langle y \rangle = \{1\}$
  (order p, different).
  Let $\mathbb{Z}/p \times \mathbb{Z}/p \to G$ by $(k \bmod p, \ell \bmod p) \mapsto x^k y^\ell$.
  This is a homomorphism since x, y commute.
  Its kernel is trivial: $x^k y^\ell = 1 \Rightarrow x^k = y^{-\ell} \in \langle x \rangle \cap \langle y \rangle = \{1\}$
  $\Rightarrow p \mid k,\ p \mid \ell$ ✓ Same size $\Rightarrow$ $G \cong \mathbb{Z}/p \times \mathbb{Z}/p$.

$\square$

continued...

$\boxed{④ \text{ Sylow Theorems:}}$ Let G be a finite group. For a prime p, let $Syl_p(G)$ be the set of p-Sylow subgroups of G.

$\boxed{\text{Ⓘ } Syl_p(G) \neq \emptyset : G \text{ has a } p\text{-Sylow subgroup.}}$

Proof: We'll prove a stronger result: for each $p^j \mid |G|$, there's a subgroup of order p^j in G. Let $|G| = p^k m$, $p \nmid m$.

If $j=0$: trivial, use $\{1\}$.

If $j=1$: (so $k \geq 1$): use Cauchy's theorem.

Now say $k \geq 2$ and $1 \leq j < k$ where there is a subgroup $H \subset G$ of order p^j.

We'll get a subgroup of order p^{j+1}: not all of G

Group action: left mult. on G/H (set being acted on) by group H (group that is acting is a p-group). So $h \in H$, $aH \in G/H \rightsquigarrow h \cdot aH = haH$.

By fixed-point congruence, $|G/H| \equiv |Fix_H(G/H)| \bmod p$

$|G/H| = \frac{|G|}{|H|} = \frac{p^k m}{p^j} = p^{k-j} m \equiv 0 \bmod p \Rightarrow |Fix_H(G/H)| \equiv 0 \bmod p$.

When is $gH \in G/H$ fixed by left mult. by H?

It means $hgH = gH \ \forall h \in H \Leftrightarrow g^{-1}Hg = H \ \forall h \in H$

$\Leftrightarrow g^{-1}Hg \in H \ \forall h \in H \quad \Leftrightarrow h \in gHg^{-1} \ \forall h \in H$

$\Leftrightarrow H \subset gHg^{-1}$ (finite gps) $\Leftrightarrow H = gHg^{-1}$

$\Leftrightarrow g \in N_G(H)$ is the same as $gH \in Fix_H(G/H)$

In left cosets G/H, the set of fixed pts for left mult by H is

$\underbrace{\{gH : g \in N_G(H)\}}_{= Fix_H(G/H)} = \underbrace{N_G(H)/H}_{\text{it's a gp since } H \triangleleft N_G(H)}$

By fixed-pt congruence above, $|N_G(H)/H| \equiv 0 \bmod p$. $\Rightarrow p \mid |N_G(H)/H|$

Since $p \mid |N_G(H)/H|$, Cauchy's thm tells us there's a subgp of order p in it. All subgps of $N_G(H)/H$ have the form H'/H where $H \subset H' \subset N_G(H)$.

So there's such H' where H'/H has order p. Since $|H| = p^j$,

$|H'| = |H'/H| \cdot |H| = p \cdot p^j = p^{j+1}$

We've shown that if G has subgp H of order p^j and $j<k$, then $H \subset H'$ where H' is a subgp with $|H'| = p^{j+1}$ (since $H' \subset N_G(H)$, $H \triangleleft H'$). This shows if H is a p-subgp of G, there's tower $H \subsetneq H' \subsetneq \ldots \subset \{p\text{-Sylow}\}$.

□

continued...

$\boxed{\text{(II) For } P, Q \in Syl_p(G),\ Q = gPg^{-1} \text{ for some } g \in G \text{, so all } p\text{-Sylow subgroups are conjugate.}}$

(II) For $P, Q \in Syl_p(G)$, $Q = gPg^{-1}$ for some $g \in G$, so all p-Sylow subgroups are **conjugate**.

Proof: Let $P, Q \in Syl_p(G)$. We want $g \in G$ s.t. $Q = gPg^{-1}$.

Make group Q (p-gp) act on set G/P by left mult. $q \cdot gP = qgP$.

Use fixed pt cong.: $|G/P| \equiv |Fix_Q(G/P)| \bmod p$.

$|G/P| = |G|/|P| = \frac{p^k m}{p^k} = m \not\equiv 0 \bmod p$ since $p \nmid m$.

Since LHS $\not\equiv 0 \bmod p$, $|Fix_Q(G/P)| \neq \emptyset$.

Thus, gP is fixed by a Q-action: $qgP = gP \ \forall q \in Q$

$\Leftrightarrow g^{-1}qgP = P \ \forall q \in Q \Leftrightarrow g^{-1}qg \in P \ \forall q \in Q \Leftrightarrow g^{-1}Qg \subset P$.

Since Q is a p-Sylow, $|g^{-1}Qg| = p^k = |P|$. Thus, $g^{-1}Qg = P$.

Therefore, $Q = gPg^{-1}$. □

(III) Let $n_p = |Syl_p(G)|$ and $|G| = p^k m$ for $k \geq 0$, $p \nmid m$. Then $n_p \equiv 1 \bmod p$ and $n_p | m$.

Proof: Let $n_p = |Syl_p(G)|$. We want $n_p \equiv 1 \bmod p$.

Let group P (p-gp) act on $Syl_p(G)$ by conjugation.

Use fixed pt cong.: $|Syl_p(G)| \equiv |Fix_P(Syl_p(G))| \bmod p$.

The $Fix_P(Syl_p(G))$ is all $Q \in Syl_p(G)$ s.t. $xQx^{-1} = Q \ \forall x \in P$

Let $Q \in Fix_P(Syl_p(G))$, so $xQx^{-1} = Q \ \forall x \in P \Rightarrow P \subset N_G(Q)$.

Also $Q \subset N_G(Q)$ and $N_G(Q) < G$.

Since $|P| = |Q| = p^k$ = max p-power in $|G|$, we get P, Q are p-Sylows in $N_G(Q)$. By Sylow (II), all p-Sylows in $N_G(Q)$ are conjugate, so $P = gQg^{-1} = Q$ for some $g \in N_G(Q)$. So $Q = P$, so $Fix_P(Syl_p(G)) = \{P\}$.

Return to fixed pt cong.: $n_p \equiv |\{P\}| \bmod p \Rightarrow n_p \equiv 1 \bmod p$. ✓

Last part: $n_p | m$ ($|G| = p^k m$, $p \nmid m$)

Let G act on $Syl_p(G)$ by conjugation. This has one orbit (Sylow (II)). By orbit-stabilizer formula,

$\underbrace{\text{size of } Syl_p(G)}_{n_p} = \frac{|G|}{|*|} \Rightarrow n_p \,|\, |G| \Rightarrow n_p | p^k m$.

We know that $n_p \equiv 1 \bmod p$, so $\underset{(n_p,\, p) = 1}{n_p \nmid p^k}$. Therefore, $n_p | p^k m \Rightarrow n_p | m$. □