Tuesday
10/15

Specific group action

G acting on G by conjugation:
$g \cdot a = gag^{-1}$

conjugacy class of a $\longrightarrow$ $G \cdot a = \{gag^{-1} \mid g \in G\}$

$N_G(\{a\}) = C_G(\{a\}) \longrightarrow G_a = \{g \in G \mid gag^{-1} = a\}$
$ga = ag$

Recall

G acting on A

$G \cdot a = \{g \cdot a \mid g \in G\}$ ← orbit of $a \in A$

$G_a = \{g \in G \mid g \cdot a = a\}$ ← stabilizer of $a \in A$

Thm: $|G \cdot a| = |G / G_a|$

$D_8$ acting on $D_8$ by conjugation

conjugacy classes:

$\{1\}$
$\{r, r^3\}$
$\{r^2\}$
$\{sr, sr^3\}$
$\{s, sr^2\}$

Cl

Let
and
be re
distinc
of G
Then,
|G

where $C_G$

## Class Equation

Let $G$ be a finite group and let $g_1, g_2, \dots, g_r$ be representatives of the distinct conjugacy classes of $G$ not contained in $Z(G)$.

Then,

$$|G| = |Z(G)| + \sum_{i=1}^{r} \left| G / C_G(g_i) \right|$$

where $C_G(g_i) = C_G(\{g_i\})$

$\left| G / C_G(g_i) \right|$: size of $G \cdot g_i$ = size of conjugacy class that $g_i$ is in.

**Ex:** $D_8 = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\}$

$Z(D_8) = \{1, r^2\}$

conjugacy classes not contained in $Z(G)$

| | |
|---|---|
| $\{r, r^3\}$ | $g_1 = r$ |
| $\{s, sr^2\}$ | $g_2 = s$ |
| $\{sr, sr^3\}$ | $g_3 = sr^3$ |

$$|D_8| = |Z(D_8)| + \left| D_8 / C_{D_8}(r) \right| + \left| D_8 / C_{D_8}(s) \right| + \left| D_8 / C_{D_8}(sr^3) \right|$$

$$= |\{1, r^2\}| + |D_8 \cdot r| + |D_8 \cdot s| + |D_8 \cdot (sr^3)|$$

$$= |\{1\}| + |\{r^3\}| + |\{r, r^3\}| + |\{s, sr^2\}| + |\{sr, sr^3\}|$$

Proof of class equation:

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

Why? The conjugacy class of $x \in G$ is $G \cdot x = \{ gxg^{-1} \mid g \in G \}$.
And $\{ gxg^{-1} \mid g \in G \} = \{x\}$ iff $gxg^{-1} = x$ for all $g \in G$ iff $gx = xg$ for all $g \in G$
iff $x \in Z(G)$

Let $Z(G) = \{ 1, z_2, \ldots, z_m \}$.

Let $K_1, K_2, \ldots, K_r$ be the conjugacy classes not contained in $Z(G)$.

Let $g_1, g_2, \ldots, g_r$ be representatives of $K_1, \ldots, K_r$ respectively [that is, $g_i \in K_i$ so $K_i = G \cdot g_i$]

So, the conjugacy classes of $G$ are

$$\{1\}, \{z_1\}, \ldots \{z_m\}, K_1, K_2, \ldots, K_r .$$

...(G).

...or all $g \in G$
...)

$Z(G)$.
$g_i \in K_i$
$= G \cdot g_i$

Since the conjugacy classes partition $G$, we get that

$$|G| = \underbrace{|\{1\}| + |\{z_1\}| + \cdots + |\{z_m\}|}_{|Z(G)|} + |K_1| + |K_2| + \cdots + |K_r|$$

$$= |Z(G)| + \sum_{i=1}^{r} |K_i|$$

$$= |Z(G)| + \sum_{i=1}^{r} |G \cdot g_i|$$

$$= |Z(G)| + \sum_{i=1}^{r} |G / C_G(g_i)|$$

$\blacksquare$

$C_G(g_i) = G_{g_i}$

# Goal:

**Previously**: If $|G| = p$ where $p$ is prime,
then $G \cong \mathbb{Z}_p$. ($G$ is cyclic)

**Two thms from now**: If $|G| = p^2$ where $p$ is prime,
then $G$ is abelian.

**Theorem:** Let $G$ be a group of size $p^\alpha$ where $p$ is prime and $\alpha \geq 1$. Then $|Z(G)| > 1$.

$Z(G) \neq \{1\}$

**Proof:** By the class equation

$$|G| = |Z(G)| + \sum_{i=1}^{r} |G| / |C_G(g_i)|$$

where $g_1, g_2, \ldots, g_r$ are representatives of the distinct conjugacy classes not contained in $Z(G)$.

Since $C_G(g_i) \leq G$ we have that $|C_G(g_i)|$ divides $|G| = p^\alpha$.

So, $|C_G(g_i)| = p^{k_i}$ where $0 \leq k_i \leq \alpha$.

If $|C_G(g_i)| = p^\alpha$, then $C_G(g_i) = \{g \in G \mid gg_ig^{-1} = g_i\} = G$.

($|C_G(g_i)| = p^\alpha$ ie $C_G(g_i) = G$; $gg_ig^{-1} = g_i$ means $gg_i = g_ig$)

So, if $|C_G(g_i)| = p^\alpha$, then $g_i \in Z(G)$.

But each $g_i$ is not in $Z(G)$.

So, $|C_G(g_i)| = p^{k_i}$ with $0 \leq k_i < \alpha$.

$\Rightarrow$ So, $\dfrac{|G|}{|C_G(g_i)|} = \dfrac{p^\alpha}{p^{k_i}} = p^{\alpha - k_i} \geq p$ ($\alpha - k_i > 0$)

So, $p \mid \dfrac{|G|}{|C_G(g_i)|}$ for all $i$.

Thus, $p$ divides

$$|G| - \sum_{i=1}^{r} \frac{|G|}{|C_G(g_i)|} = |Z(G)|.$$

($|G| = p^\alpha$; $\dfrac{|G|}{|C_G(g_i)|} = p^{\alpha - k_i} \geq p$)

So, $|Z(G)| \geq p > 1$. ∎

**Theorem:** Let $G$ be a group with $|G| = p^2$ where $p$ is prime. Then $G$ is abelian.

**Proof:** (from Herstein: Topics in Algebra)

To show $G$ is abelian we show $Z(G) = G$.

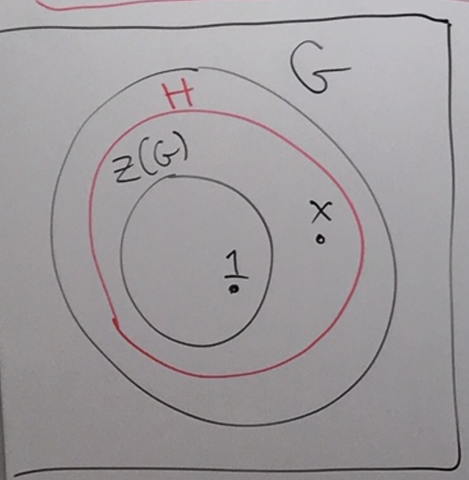
From the previous theorem, $|Z(G)| > 1$.

By Lagrange, since $Z(G) \leq G$, we know $|Z(G)| \mid |G|$.

So, $|Z(G)| = p$ or $|Z(G)| = p^2$.

We will rule out $|Z(G)| = p$ and that will imply that $|Z(G)| = p^2$ or $Z(G) = G$.

Suppose $|Z(G)| = p$. Then $Z(G) \neq G$.




Pick some $x \in G$ with $x \notin Z(G)$.

Let

$$H = C_G(\{x\}) = \{g \in G \mid gx = xg\}.$$

Then $H \leq G$.

Also, $Z(G) \leq H$.

And $x \in H$.

So, $|H| \geq p+1$.

But $|H| \mid |G|$ by Lagrange, so $|H| = p^2$.

(only divisors of $|G| = p^2$ are $1, p, p^2$)

So, $H = G$.

So, $gx = xg$ for all $g \in G$.

Then, $x \in Z(G)$.

This is ridiculous! [Reducto ad absurdum]

So, $|Z(G)| \neq p$.

Thus, $|Z(G)| = p^2$ and so $G = Z(G)$.

Q.E.D.

Test 2

currently

Tues. Nov 5

move to

Tues. Nov 12