So far we have been looking at action of groups on graphs. This setup an interesting correspondence between the two objects.

Now we will consider some interesting actions on groups themselves

One of the consequences we are aiming for are the Sylow theorems which talks about subgroups of a given finite group.

For this we begin with the class equation.

Suppose $G \curvearrowright X$, $|G|, |X| < \infty$.

Now we can write

$$X = \bigsqcup_{i=1}^{n} O(x_i)$$ as a union

of distinct orbits.

Now. we have $|Stab(x_i)||O(x_i)| = |G|$

So we have decomposed $|X|$ as a sum of factors of G.

① $G \curvearrowright G$ by multiplication

$O(x) = G \quad \forall x \in G.$

So the class equation is boring.

② **conjugation**: $c: G \times G \longrightarrow G.$

given by $C(g, x) = g x g^{-1}$

Fix, x, $x \longrightarrow c(g, x) = g x g^{-1}$

from G to itself. is an automorphism.

$$\left[\begin{aligned} id_G &\to id_G, \\ g_2 g_3 &\to g_1 g_2 g_3 g_1^{-1} \\ &= g_1 g_2 g_1^{-1} g_1 g_3 g_1^{-1} \\ &= c(g_1, g_2) c(g_1, g_3) \end{aligned}\right]$$

$x^{-1} \to c(g, x^{-1}) = (c(g, x))^{-1}$

Let $C_x = O_c(x) = \{gxg^{-1} : g \in G\}$

C_x is called the conjugacy class of x.

$\mathrm{Stab}_G(x)$ is called the centralizer of x — $Z(x) = \{g : gxg^{-1} = x\} = \{g : \underline{gx = xg}\}$

So we have $|C_x||Z(x)| = |G|$

and $\displaystyle\sum_{C \text{ conjugacy class}} |C| = |G|$

↳ Class equation for G.

$Z(G) = \displaystyle\bigcap_{x \in G} Z(x) = \{ g \in G : xg = gx \text{ for all } x \in G\}$

$Z(G) = G \Leftrightarrow$ group is abelian

Examples: Abelian groups $|C_x| = 1$ for all $x \in G$

$|G| = 1 + 1 + 1 + \cdots + 1 + 1$

Dihedral Group $D_6 = \{1, x, x^2, y, yx, yx^2\}$

$yx = x^{-1}y$.

$\Rightarrow yx = x^2y$

$\Rightarrow yxy^{-1} = x^2$

$\{x, x^2\}$

$x \cdot yx^{-1} = yx^{-2} = yx \cdot \quad xyxx^{-1} = yx^2$

Conjugacy classes are $\{1\}$, $\{x, x^2\}$ and $\{y, yx, yx^2\}$

Class equation $|D_6| = 1+2+3$

p - prime

A group is called a p group is $|G| = p^e$ for some e.

Prop: Every finite p-Group has a non-trivial center

Proof: By the class equation

$$p^e = |G| = \sum_{C \to \text{conjugacy classes}} |C|$$

for some e.

$$= 1 + \sum_{\substack{C \text{ conjugacy classes} \\ C \neq \{Id_G\}}} |C|$$

conjugacy class of identity

$\# 1^s = |Z(G)|$

If $|Z(G)| = 1$ then the sum consists of terms of the order p^k, $k \geq 1$. Then the sum is $1 \bmod p$ but this is impossible.

Observe

Every group of prime order is abelian.

Proof: If G is such a group and $x \in G, x \neq id_G$

$\Rightarrow \langle x \rangle \mid |G| \Rightarrow \langle x \rangle = G.$

$\Rightarrow$ G is cyclic and hence is abelian.

Prop:

Every group of order p^2 is abelian. (p - prime)

Proof:

It is enough to prove $Z(G) = G$.

Suppose not! then $|Z(G)| = p$.

Take $x \notin Z(G)$

Then $x \in Z(x)$ and $Z(G) \subset Z(x)$

$\Rightarrow \quad Z(x) = G.$

$\Rightarrow \quad Z(x) = G$ for all $x \in G \setminus Z(x)$

But $Z(x) = G$ for all $x \in G$ as well.

$\Rightarrow \quad Z(G) = G.$

Prop: p - prime G - group
$|G| = p^2$ then $G \simeq \mathbb{Z}/p^2\mathbb{Z}$
or $G \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$

Proof! order of an element in $G \setminus \{id_G\}$
is p or p^2.

If there is an element of order p^2
then $G \simeq \mathbb{Z}/p^2\mathbb{Z}$.

Now suppose every such element has order p.

Take $x \in G$. and $y \in G \setminus \langle x \rangle$

Then $\langle y \rangle \cap \langle x \rangle = \{id_G\}$. &

and since its abelian $xy = yx$.

Thus $\langle y \rangle \langle x \rangle$ is a subgroup of G. of order $> p$

$\Rightarrow \langle y \rangle \langle x \rangle = G$.

$\Rightarrow G \simeq \langle x \rangle \times \langle y \rangle \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$

(If $H_1, H_2 < G$, $H_1 H_2 = H_2 H_1$ $H_1 \cap H_2 = \{id_G\}$ then $H_1 H_2 \simeq H_1 \times H_2$.
Take $\phi : H_1 \times H_2 \to H_1 H_2$ given by $\phi(h_1, h_2) = h_1 h_2$
Injectivity follows from $H_1 \cap H_2 = \{id_G\}$.)

Theorem (Cauchy) G group $|G| < \infty$, p prime and $p \mid |G|$. Then G contains an element of order p.

Proof: Suppose not. We will proceed by induction on $|G|$. We already know this if $|G| = p$.

Now we know this fact in case $|G| \leq n-1$ for some n.

Let $|H| = n$ and $p \mid n$.

Assume that the order of all elements are prime to p. [Otherwise there is a subgroup $\cong \mathbb{Z}/t\mathbb{Z}$ where $p \mid t$ and gives an element of prime order.]

Case ① H has a proper normal subgroup G.

$|G| \mid |H|$ if $p \mid |G|$ we are done by induction if not $p \mid |H|/|G| = |H/G|$

Thus there exists $h \in H$ such that

$$(\bar{h})^p = id_{H/G}.$$

Let $\operatorname{ord}(h) = r$.

$\Rightarrow \quad (\bar{h})^r = id_{H/G} \Rightarrow p \mid r$.

$\Rightarrow \operatorname{ord}(h^{r/p}) = p$.

Case (ii) G has no proper normal subgroup.

and G has no proper subgroup of order divisible by p.

$\Rightarrow$ for all x.

if $|C_x| = 1 \qquad Z(x) = G$.

if $|C_x| > 1 \qquad Z(x) \underset{\neq}{\leq} G$

$\Rightarrow p \nmid Z(x)$

$\Rightarrow p \mid |C_x|$

By the Class equation

$$|G| = \sum_{C \text{ conjugacy class}} |C|$$

If $|C| \neq 1$ then $p \mid |C|$

$\Rightarrow p \mid (\#1\text{'s in class equation}) = |Z(G)|$

Contradicts
assumption.