

Review of 561/562.

Last Time :

- Groups of Automorphisms
- Group Actions
- Orbit-Stabilizer Theorem
- Free, Transitive, Regular Actions

Recall : An action of group G on set X is a group homomorphism

$$\begin{aligned} \varphi : G &\rightarrow \text{Aut}(X) (= \text{Perm}(X)) \\ g &\mapsto (\varphi_g : X \rightarrow X) \end{aligned}$$

Equivalently, an action is a function

$$\begin{aligned} G \times X &\rightarrow X \\ (a, x) &\mapsto a * x \end{aligned}$$

satisfying two axioms

- $\forall x \in X, 1 * x = x$
- $\forall a, b \in G, x \in X, (ab) * x = a * (b * x)$

$$[\text{Equivalence : } a * x = \varphi_a(x)]$$

Today: G acts on itself by conjugation

$$\begin{aligned} G \times G &\longrightarrow G \\ (g, h) &\longmapsto g * h := ghg^{-1} \end{aligned}$$

Exercise: Check that this is an action.

Notation: Given $h \in G$, the orbit is called the conjugacy class of h :

$$C(h) = \text{orb}(h) := \{ ghg^{-1} : g \in G \} \subseteq G$$

and the stabilizer is called the centralizer of h :

$$\begin{aligned} Z(h) = \text{stab}(h) &:= \{ g \in G : ghg^{-1} = h \} \\ &= \{ g \in G : gh = hg \} \subseteq G. \end{aligned}$$

Note that $\text{stab}(h)$ is a (probably non-normal) subgroup of G .



Now suppose G is finite. By the Orbit-Stabilizer Theorem we have a bijection

$$G/Z(h) \leftrightarrow C(h)$$

and then by Lagrange we have

$$|G|/|Z(h)| = |C(h)|$$

Note that $|C(h)| = 1 \Leftrightarrow |Z(h)| = |G|$
 $\Leftrightarrow h \in Z(G)$

where $Z(G) = \{h \in G : gh = hg \forall g \in G\}$
is the center of G .

If we write G as the disjoint union of conj. classes (orbits) then we have

$$G = \bigsqcup_i C(h_i)$$

$$|G| = \sum_i |C(h_i)|$$

$$= \underbrace{1 + 1 + \dots + 1}_{|Z(G)| \text{ times}} + \sum_{C(h_i) \neq 1} |C(h_i)|$$

$$|G| = |Z(G)| + \sum_{C(h_i) \neq 1} |C(h_i)|$$

This last is called the "class Equation" of G .

Application: Let p be prime. Then every group of order p^2 is abelian.

Proof: Let $|G| = p^2$ and consider the class equation

$$|G| = |Z(G)| + \sum_{C(h_i) \neq 1} |C(h_i)| \quad (*)$$

Since $|C(h_i)|$ divides p^2 we must have $|C(h_i)| = 1, p, \text{ or } p^2$. If $|C(h_i)| \neq 1$ we have $|C(h_i)| = p$ or p^2 . In particular, p divides $|C(h_i)|$.

Since p divides every term on the right side of

$$|Z(G)| = |G| - \sum_{C(h_i) \neq 1} |C(h_i)|,$$

p also divides $|Z(G)|$. Hence

$$|Z(G)| = p \text{ or } p^2$$

If $|Z(G)| = p^2$ then $G = Z(G)$ and we're done. Otherwise, if $|Z(G)| = p$ then

$$|G/Z(G)| = |G|/|Z(G)| = \frac{p^2}{p} = p$$

and hence $G/Z(G)$ is cyclic, i.e. the cosets of $Z(G)$ have the form

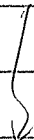
$$Z(G), gZ(G), g^2Z(G), \dots, g^{p-1}Z(G)$$

for some $g \in G$. But then every element of G has the form

$$g^k z$$

for some $k \in \mathbb{N}$ and $z \in Z(G)$, and all such elements commute.

Hence G is abelian.



Another Application: Proving that a group is simple.

We say G is simple if it has no nontrivial normal subgroup.

If $N \trianglelefteq G$, note that N is a union of conjugacy classes.

Let $I =$ group of rotational symmetries of a regular icosahedron

$$I \leq SO(3)$$

The conjugacy classes are

- | | |
|---|---------|
| • $\{1\}$ | size 1 |
| • $\left. \begin{array}{l} \text{rotate } \pm 2\pi/3 \text{ around face} \\ \text{rotate } \pi \text{ around edge} \end{array} \right\}$ | size 20 |
| • $\left. \begin{array}{l} \text{rotate } \pm 2\pi/5 \text{ around vertex} \\ \text{rotate } \pm 4\pi/5 \text{ around vertex} \end{array} \right\}$ | size 12 |
| • $\left. \begin{array}{l} \text{rotate } \pm 2\pi/5 \text{ around vertex} \\ \text{rotate } \pm 4\pi/5 \text{ around vertex} \end{array} \right\}$ | size 15 |
| • $\left. \begin{array}{l} \text{rotate } \pm 2\pi/5 \text{ around vertex} \\ \text{rotate } \pm 4\pi/5 \text{ around vertex} \end{array} \right\}$ | size 12 |

Class Equation

$$60 = 1 + 20 + 15 + 12 + 12.$$

Now suppose we have a normal subgroup.

$$1 \subsetneq N \subsetneq I.$$

Then $N = \{1\} \cup$ other conj. classes

i.e. $|N| = 1 +$ some of $\{20, 15, 12, 12\}$

and $|N|$ divides $|I| = 60$.

This is impossible.



Hence I is simple. This is the smallest nonabelian simple group