5/28

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

$$\varphi : G \to \mathrm{Aut}(X) \quad (= \mathrm{Perm}(X)).$$
$$g \mapsto (\varphi_g : X \to X)$$

Equivalently, an action is a function

$$G \times X \to X$$
$$(a, x) \mapsto a * x$$

satisfying two axioms

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

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

Today: G acts on itself by conjugation

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

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:

$$Z(h) = \text{Stab}(h) := \{g \in G : ghg^{-1} = h\}$$
$$= \{g \in G : gh = hg\} \leq G.$$

Note that Stab(h) is a (probably non-normal) subgroup of G.

↓

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

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

and then by Lagrange we have

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

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

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

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

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

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

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

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

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, 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

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

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

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

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
- {rotate $\pm 2\pi/3$ around face} size 20
- {rotate π around edge} size 15
- {rotate $\pm 2\pi/5$ around vertex} size 12
- {rotate $\pm 4\pi/5$ around vertex} size 12

Class Equation

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

Now suppose we have a normal subgroup.

$$1 \lneq N \ntrianglelefteq I.$$

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