Lecture 20 Class equation and applications

<u>Lagrange's theorem</u>: If $H \leq G$, G finite, then $|H| \,\big|\, |G|$.

<u>Corollary</u>: if $|G| = p$, a prime, then $G \cong \mathbb{Z}_p$.

<u>Proof</u>: Take $g \in G$, $g \neq e$ then $\langle g \rangle \leq G$ so $|\langle g \rangle| \,\big|\, p$ so $|\langle g \rangle| = p$ so $\langle g \rangle = G$. Thus G is cyclic.

<u>Corollary</u>: Any two groups of order p (p prime) are isomorphic.

A general problem is to try to figure out how many nonisomorphic groups there are of a given order. One tool is the <u>class equation</u>.

Recall G acts on G by conjugation $g \cdot h = ghg^{-1}$.
The orbits are the <u>conjugacy classes</u> $[h]$
The stabilizer of $h \in G$ is the <u>centralizer</u> $Cent(h) = \{g \mid gh = hg\}$
The <u>center</u> is $Z(G) = \{g \mid gh = hg \text{ for all } h\}$.

Observe $g \in Z(G) \iff Cent(g) = G$.
By orbit stabilizer theorem: $|[g]| = \dfrac{|G|}{|cent(g)|}$.

$$g \in Z(G) \iff |[g]| = 1$$

<u>Class equation</u> Assume G is finite. Then

$$|G| = |Z(G)| + \sum_{\substack{\text{conj. classes} \\ [g] \subseteq G \setminus Z(G)}} \frac{|G|}{|Cent(g)|}$$

<u>Proof</u> conjugacy classes are a partition of G. $|Z(G)|$ counts the classes of size one, the other term counts the rest. $\blacksquare$

Ex $G = S_3 \quad Z(S_3) = \{e\}$

$|G| = 6$

$[(12)] = \{(12), (13), (23)\}$
$\mathrm{cent}((12)) = \{e, (12)\}$
$[(123)] = \{(123), (132)\}$
$\mathrm{cent}((123)) = \{e, (123), (132)\}$

$$|Z(S_3)| + \frac{|S_3|}{|\mathrm{Cent}((12))|} + \frac{|S_3|}{|\mathrm{cent}((123))|} = 1 + \frac{6}{2} + \frac{6}{3} = 1+3+2 = 6$$

Some applications:

Proposition: If $|G| = p^n$, p prime, then $Z(G) \neq \{e\}$
(there exist nontrivial elements in the center)

Proof If $g \notin Z(G)$ then $|\mathrm{Cent}(g)|$ divides $|G| = p^n$ and is less than p^n so $\frac{|G|}{|\mathrm{Cent}(g)|}$ is also divisible by p.

So in the class equation, p divides $|G|$ and p divides $\sum_{\substack{\text{conj classes} \\ [g] \subseteq G \setminus Z(G)}} \frac{|G|}{|\mathrm{cent}(g)|}$. So p divides $|Z(G)|$. Since $|Z(G)| \geq 1$, $|Z(G)|$ is at least p. ∎

Proposition: If $|G| = p^2$, (p prime), then either $G \cong \mathbb{Z}_{p^2}$ or $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$.

Proof If G is cyclic, $G \cong \mathbb{Z}_{p^2}$ and we are done.
So suppose G is not cyclic. Then any nonidentity element has order p: If $g \neq e$, $\langle g \rangle \mid p^2$ and $|\langle g \rangle| < p^2$ so $|\langle g \rangle| = p$.
By previous theorem, we can find $g_1 \in Z(G)$, $g_1 \neq e$.
then $\langle g_1 \rangle \cong \mathbb{Z}_p$. Now take $g_2 \in G \setminus \langle g_1 \rangle$.
then $\langle g_2 \rangle \cong \mathbb{Z}_p$.
Because $g_1 \in Z(G)$, g_1 and g_2 commute.

Next we claim $\langle g_1\rangle \cap \langle g_2\rangle = \{e\}$. In fact,

$$|\langle g_1\rangle \cap \langle g_2\rangle| \text{ divides } |\langle g_2\rangle| = p.$$

So either $|\langle g_1\rangle \cap \langle g_2\rangle| = 1$, and $\langle g_1\rangle \cap \langle g_2\rangle = \{e\}$ as desired.
or $|\langle g_1\rangle \cap \langle g_2\rangle| = |\langle g_2\rangle|$ and $\langle g_1\rangle \cap \langle g_2\rangle = \langle g_2\rangle$;
then $g_2 \in \langle g_1\rangle$ contrary to the construction.
So $\langle g_1\rangle \cap \langle g_2\rangle = \{e\}$

Then $\langle g_1\rangle\langle g_2\rangle$ is a subgroup of G isomorphic to $\mathbb{Z}_p \times \mathbb{Z}_p$ (recognition theorem for direct products.) But $|G| = p^2$, so

$$G = \langle g_1\rangle\langle g_2\rangle \cong \mathbb{Z}_p \times \mathbb{Z}_p. \qquad \blacksquare$$

<u>Proposition</u> If $|G| = p^n$, p prime, $n > 1$, then there is a nontrivial proper normal subgroup N : $\{e\} \subsetneq N \subsetneq G$.
Furthermore, N can be chosen so that every subgroup $H \leq N$ is normal in G.

<u>Proof</u> If G is non abelian, $Z(G)$ is a proper subgroup.
By the first proposition, $Z(G)$ is nontrivial.
Also $Z(G)$ is always a normal subgroup of G and any subgroup of $Z(G)$ is normal in G.

It remains to consider the case of G abelian.
In that case every subgroup is normal.
Let $g \in G$, $g \neq e$. Then $|\langle g\rangle| = p^s$ for some $1 \leq s \leq n$.
If $s < n$, we take $N = \langle g\rangle$.
If $s = n$, then g^p has order p^{n-1}, so we take $N = \langle g^p\rangle$. $\blacksquare$

<u>Corollary</u> If $|G|=p^n$, p prime, there is a sequence of normal subgroups

$$\{e\} = G_0 \subsetneqq G_1 \subsetneqq G_2 \subsetneqq \cdots \subsetneqq G_{n-1} \subsetneqq G_n = G$$

such that $|G_i|=p^i$.

<u>Proof</u>: Induction on n. If $n=1$, $G \cong \mathbb{Z}_p$ and the conclusion is true.

Suppose the conclusion holds for all groups of order p^k, $k<n$. Let G be a group of order p^n. Use proposition to find nontrivial proper normal $N \leq G$, such that every subgroup of N is normal in G. Then $|N| = p^k$ for some $k<n$, and $|G/N| = p^{n-k}$, $n-k<n$.

By induction, there are subgroups

$$\{e\} = G_0 \leq G_1 \leq \cdots \leq G_k = N \quad |G_i|=p^i \quad \text{all } G_i \lhd G.$$

and

$$\{e\} = \overline{G}_0 \leq \overline{G}_1 \leq \cdots \leq \overline{G}_{n-k} = G/N \quad |\overline{G}_j| = p^j \text{ all } \overline{G}_j \lhd G/N.$$

Define $G_{i+k} = \pi^{-1}(\overline{G}_i)$ where $\pi : G \to G/N$ is the quotient map. Then these subgroups are normal in G and $|G_{i+k}| = |\overline{G}_i|\,|N| = p^{i+k}$

Then

$$\{e\} \leq G_0 \leq G_1 \leq \cdots \subseteq \underset{\substack{\| \\ N}}{G_k} \leq \underset{\substack{\| \\ \pi^{-1}(\overline{G}_1)}}{G_{k+1}} \leq \cdots \leq G_n = G$$

is the desired sequence. ∎