Math 122 Monday, October 31

G acts on a set $S = \bigcup O_s$ disjoint union of orbits $O_s = G/G_s$ as a set

If G and S are finite $\#S = \sum_{\text{orbits}} \#G/\#G_s$ counting formula

application: G acts on $S=G$ by conjugation $g(s) = gsg^{-1} = s'$
O_s = conjugacy class of s G_s = centralizer of s

Class formula $\#G = \sum_{\substack{\text{conj. classes}\\ \text{of } G}} \#G/\#G_s$

When is $G_s = G$? For all $g \in G$, $gsg^{-1} = s \iff gs = sg \iff s$ commutes with all $g \in G$
$\iff s \in Z(G) =$ center of $G \triangleleft G$.

In this case, $O_s = \{s\}$. $\#O_s = 1 = \#G/\#G_s$: G

In all other cases, $\#O_s > 1$ is a proper divisor of $\#G$.

$$\#G = \sum_{\substack{\text{orbits of}\\ S \text{ in } Z(G)}} 1 + \sum_{\substack{\text{orbits of}\\ S \notin Z(G)}} \#G/\#G_s \;(\leftarrow \text{divisor of } \#G > 1) = \#Z(G) + \sum_{s \text{ not central}} \#G/\#G_s$$

If G is abelian, $Z = G$, every conjugacy class has one element, and class formula $\Rightarrow \#G = \#G$.

defn A finite group G is a p-group (p a prime) if $\#G = p^n$.

ex: $\mathbb{Z}/p\mathbb{Z}$, $\mathbb{Z}/p^n\mathbb{Z}$, $\mathbb{Z}/2 \times \mathbb{Z}/2$ Klein-4 group
non-abelian ex: D_4 = dihedral group of order 8.

Thm Any p-group has a non-trivial center $Z \neq \{e\}$.

Note: $G = S_3$ of order $6 = 2 \cdot 3$ has a trivial center.

Pf: If $|Z| = 1$ then the class equation gives $\#G = 1 + \sum \#G/\#G_s$ where the terms in the sum are proper divisors of $\#G = p^n$. So $p^n = 1 + \sum p^i$. But then the left hand side is $0 \bmod p$ while the right hand side is $1 \bmod p \Rightarrow\Leftarrow$. So $|Z| > 1$.

Cor Any p-group G of order p^n, $n > 1$ has a non-trivial normal subgroup $H \triangleleft G$.

Pf: We know $\{e\} \subsetneq Z \subset G$. If $Z \neq G$ take $H = Z$. If $G = Z$ then G is abelian and any non-trivial $H \subset G$ is normal. Clear that such H exists: let $g \in G$. Either $\langle g \rangle \subsetneq G$ or $\langle g \rangle = G$ but $\langle g^p \rangle \subsetneq G$.

$n=1$ $\#G=p \Rightarrow G$ is cyclic so isomorphic to $\mathbb{Z}/p\mathbb{Z}$ generated by any $g\neq e$.

<u>Thm</u> Any group of order p^2 is abelian

Pf: We know $Z\neq\{e\}$. Z a subgroup $\Rightarrow \#Z=p$ or $\#Z=p^2$, in which case $G=Z$, which is what we want. Assume $\#Z=p$, $\{e\}\subset Z\subset G$. Choose $g\in G, g\notin Z$ and consider the centralizer G_g of g. $G\supset G_g\supset Z\cup\{g\}\supsetneq Z$, so as G_g is a subgroup $\Rightarrow \#G_g=p^2 \Rightarrow G_g=G$. But then $g\in Z$, a contradiction. Hence $Z=G$.

Can show that either $G\simeq\mathbb{Z}/p^2\mathbb{Z}$ ($\exists g$ of order p^2) or $G\simeq\mathbb{Z}/p\mathbb{Z}+\mathbb{Z}/p\mathbb{Z}$.

What about G of order p^3? Can have: abelian: $\mathbb{Z}/p^3\mathbb{Z}$ some g of order p^3
$\mathbb{Z}/p^2+\mathbb{Z}/p$ some g of order p^2, none of order p^3
a vector space of dim 3 over $\mathbb{Z}/p \rightsquigarrow \mathbb{Z}/p+\mathbb{Z}/p+\mathbb{Z}/p$ every $g\neq e$ of order p.

Can also have <u>non-abelian</u> G of order p^3. Must have $\#Z=p$ or p^2. If $\#Z=p^2$ then G/Z has order $p \Rightarrow G/Z$ is cyclic $\Rightarrow$ (by midterm) G is abelian $\Rightarrow \#Z=p^3$. So must have $\#Z=p \Rightarrow \#(G/Z)=p^2$. By above G/Z must <u>not</u> be cyclic! So $Z\simeq\mathbb{Z}/p\mathbb{Z}$, $G/Z\simeq\mathbb{Z}/p\mathbb{Z}+\mathbb{Z}/p\mathbb{Z}$. Class equation $p^3=p+\sum_{\text{conj. classes}}|G|/|G_g| \leftarrow$ order p^2 as contains g and Z. So $p^3=p+\sum p$. Number of conjugacy classes is $(p^3-p)/p=p^2-1$.

Ex. $G\subset GL_3(\mathbb{Z}/p\mathbb{Z})$ $G=\left\{\begin{pmatrix}1&a&c\\0&1&b\\0&0&1\end{pmatrix}\right\}$ order p^3 $Z=\left\{\begin{pmatrix}1&0&c\\0&1&0\\0&0&1\end{pmatrix}\right\}$

$G/Z=\{(a,b)\in\mathbb{Z}/p+\mathbb{Z}/p\}$. If $p>2$ all elements $g\neq e$ in G have order p.
If $p=2$ get two elements of order 4 and $G=D_4$.

<u>Challenge</u>: There is a non-isomorphic non-abelian group of order p^3 ($p>2$) which contains elements of order p^2.

<u>Sylow Thms</u> Assume $\#G=p^n\cdot m$ with $\gcd(m,p)=1$ [m is prime to p]. Then
1) G contains a subgroup H of order p^n.
(H is as unique as possible as $H'=gHg^{-1}$ has same order for all $g\in G$)
2) Any two subgroups H and H' of order p^n are <u>conjugate</u> in G.

So $\#G=12=2^2\cdot3 \Rightarrow \exists$ subgroups of order 3 and 4.
$\#G=60=2^2\cdot3\cdot5 \Rightarrow \exists$ subgroups of order 4, 3, and 5

Remark on the conjugacy action of G on $\{$subgroups of $G\}$. Generally if G acts on S then G acts on $P(S)=\{$all subsets $T\subset S\}$. One invariant of elements of O_T is $\#T$. Another invariant might come from the structure of S. $\{$subgroups of $G\}\subset P(S)$ $g(T)=gTg^{-1}=T'$ is another subgroup. What is $G_H=\{g\in G: gHg^{-1}=H\}$?