Lec 9/10

Monday, September 10, 2018 11:30

p prime $r, m \in \mathbb{Z}_{>0}$.

then $\binom{mp^r}{p^r} \equiv m \pmod p$

<u>Idea:</u> If $G \curvearrowright X$ and $|G| = p^r$ then X = disjoint union of orbits.

$\forall$ orbit $\mathcal{O}$, $|\mathcal{O}|$ divides $|G| = p^r$, i.e. $|\mathcal{O}| = 1$ or div. by p.

$|X| \equiv$ # of orbits of size 1 $\pmod p$

$= |X^G|$

$= \{x \in X \mid g \cdot x = x \ \forall g \in G\}$

Special Case – $G \curvearrowright G$ by conjugation: $g \cdot x := gxg^{-1}$.

Fixed pts: $\{x \in G \mid gxg^{-1} = x \ \forall g \in G\} =: Z(G)$ center of group.

If $|G| = p^r$ then $|Z(G)|$ is divisible by p.

It's a subgroup, so $|Z(G)| = p^s$ for some $1 \leq s \leq r$.

Note: $Z(G) \trianglelefteq G$ and $Z(G)$ is abelian.

"Inductive arguments": G: size $p^r \rightsquigarrow G/Z(G)$: size p^{r-s}

since $s \geq 1$, this is $< r$.

"Base case" : $\mathbb{Z}/p\mathbb{Z}$

Hölder program:

Prop: If $|G| = p^r$ then there exists a chain of normal subgroups

$$\{e\} = Z_0 \trianglelefteq Z_1 \trianglelefteq Z_2 \trianglelefteq \cdots \trianglelefteq Z_k = G \quad \text{such that}$$

Z_ℓ / Z_ℓ is abelian for every ℓ.

Proof by induction on r, where $|G| = p^r$.

Base case: $r = 0$, nothing to prove ✓

Induction Hyp: Prop is true $\forall$ groups of size p^t, $t < r$.

Induction step: $|G| = p^r$. Take $Z_1 = Z(G)$. $\pi : G \longrightarrow \underbrace{G/Z(G)}_{\text{admits a chain}}$ $\bar{G}$

$$\{\bar{e}\} \trianglelefteq \bar{Z}_2 \trianglelefteq \cdots \trianglelefteq \bar{Z}_j = \bar{G}.$$

april snow

refer to 3rd 4 4th iso thm.

We know $\left\{ \begin{array}{c} \text{normal subgps in} \\ G/N \end{array} \right\} \xleftrightarrow[\text{everything!}]{\text{Preserves}} \left\{ \begin{array}{c} \text{normal subgps in } G \\ \text{Containing } N \end{array} \right\}$

$\trianglerighteq \{e\}$ $\square$

Ex: $|D_8| = 2^3$. $Z(D_8) = \{e, r^2\}$. Chain is

$$\{e\} \trianglelefteq \langle r^2 \rangle \trianglelefteq D_8$$

$$D_8/\langle r^2\rangle = \langle s, r \mid \underbrace{r^2=e}, s^2=e, \underbrace{srs=r^{-1}}_{r^{-1}=r^3=r} \rangle \text{ is abelian.}$$

Program to understand finite groups.

$$n = p_1^{k_1} \cdots p_\ell^{k_\ell} .$$

Theorems to prove:

Let G be a finite group, $|G| = n$. Let p be a prime and write $n = p^r m$ w/ $p \nmid m$.

<u>Theorem</u> (Sylow) : There is a subgroup $S \leq G$ with $|S| = p^r$.

<u>Proof</u> $G \circlearrowright X :=$ all subsets of G w/ cardinality p^r.

$$\underset{g}{\in} \cdot \underset{\{x_1, \dots, x_{p^r}\}}{\in} := \{g \cdot x_1, \dots, g \cdot x_{p^r}\}.$$

① $|X| = \binom{p^r \cdot m}{p^r} \equiv m \pmod p$ (not 0 mod p).

② If $H = \{h_1, \dots, h_{p^r}\} \in X$ then $g \in \mathrm{Stab}_G(H) \iff \{g \cdot h_1, \dots, g \cdot h_{p^r}\}$

i.e. $g h_1 = h_i$ so $g = h_i h_1^{-1}$.

So $\mathrm{Stab}_G(H) \subseteq \{e, h_2 h_1^{-1}, \dots, h_{p^r} h_1^{-1}\}$ so $|\mathrm{Stab}_G(H)| \leq p^r$.

Let $\mathcal{O}$ be a G-orbit with $|\mathcal{O}|$ not div. by p $\left(|X| = \sum_{\mathcal{O}:\text{ orbit}} |\mathcal{O}|\right)$ not div. by p so one exists.

pick $H \in \mathcal{O}$. then $|\mathrm{Stab}_G(H)| = \dfrac{|G|}{|\mathcal{O}|} = p^r \cdot m_1 \leq p^r$ ($|G| = p^r m$; $|\mathcal{O}|$ not div by p)

no div by p

So $\mathrm{Stab}_G(H)$ is the subgroup we're looking for.

<u>Definition</u>: a group H is said to be a p-group if $|H| = p^r$ for some r.

Sylow p-Subgroup of G is a subgroup P which is a p-group and p does not divide $\frac{|G|}{|P|}$.

<u>Theorem</u> If $\begin{matrix} H \leq G \\ P \leq G \end{matrix}$ are two p-groups & P is a sylow p-subgp, then $\exists g \in G$ s.t. $\underbrace{H \subset gPg^{-1}}$. (In particular, $H = gPg^{-1}$ if H is a sylow p-subgp).

$\hookrightarrow Hg \subset gP \longleftrightarrow h \cdot gP = g \cdot P \quad \forall h \in H$

<u>Proof</u> $\underset{H}{\circlearrowleft} X = \underbrace{G/P}$: $h \cdot (\sigma P) = h\sigma P$.

has $m = \frac{p^r \cdot m}{p^r}$ elements ($\neq 0 \mod p$)

H ← p-group.

So $|X| \equiv |\overset{\text{\# of fixed pts}}{X^H}| \neq 0 \pmod p$

$\Rightarrow \exists$ some $g \cdot P \in X$ s.t. $h \cdot gP = gP$.

$\mathrm{Syl}_p(G)$ = set of all Sylow p-subgps of G.

Sylow theorems

<u>part 1</u>: $\mathrm{Syl}_p(G) \neq \emptyset$ if $p \mid |G|$.

<u>part 2</u>: $\circlearrowleft G$ is transitive

<u>part 3</u>: if $n_p = \#\mathrm{Syl}_p(G)$, then $n_p \equiv 1 \mod p$, (so $n_p \mid m$ where $|G| = p^r m$)

\

<u>part 3</u>: if $n_p = \# Syl_p(G)$, then $n_p \equiv 1 \mod p$, $\left(\text{so } n_p \mid m \text{ where } |G| = p^r m \right)$.