Lec 9/11

Wednesday, September 11, 2019 11:32

Sylow Theorems (partial converse to Lagrange theorem

Lemma if $G$ is finite abelian and $p$ is a prime dividing $|G|$, then $G$ contains an element of order $p$.

Pf induction on $|G|$. If $|G|=1$, the lemma holds.

Assume the lemma holds $\forall$ abelian gp of order $<|G|$.

let $1 \neq a \in G$. if $r = |a|$ is div by $G$, then $b = a^{\frac{r}{p}} \in G$ has order $p$.

If $p \nmid r$, then $G/\langle a \rangle$ has order $|G|/r < |G|$, and $|G|/r$ is divisible by $p$. So $G/\langle a \rangle$ has an element $\bar{b} = b\langle a \rangle$ of order $p$.

Suppose $s = |b|$. Then $(\bar{b})^s = (b\langle a \rangle)^s = b^s \langle a \rangle = \langle a \rangle = \bar{1}$.

So $p \mid s$, meaning $b^{s/p} \in G$ has order $p$. $\square$

Theorem (Sylow I) If $p$ is a prime & $p^k$ (w/ $k \in \mathbb{Z}_{\geq 0}$) divides $|G|$, then $G$ contains a subgroup of order $p^k$.

proof induct on $|G|$ again. for $k=0$, it's true, suppose $k>0$ By the class equation,

$$|G| = |Z(G)| + \sum [G : C(y_i)].$$

- If $p \mid |Z(G)|$, then by the lemma,

  $Z(G)$ contains an element $z$ of order $p$.

  Since $\langle z \rangle \trianglelefteq G$, $G/\langle z \rangle$ is a gp, w/ size $|G|/p < p$.

  Hence, by induction, $G/\langle z \rangle$ contains a subgroup

  of order $p^{k-1}$, call it $H/\langle z \rangle$ where $H \leq G$ contains $\langle z \rangle$.

  So $|H| = |H/\langle z \rangle| \cdot |\langle z \rangle| = p^{k-1} \cdot p = p^k$.

- Suppose $p \nmid |Z(G)|$. Then $p \nmid [G : C(y_j)]$ for some $j$.

  So $p^k \mid |C(y_j)|$. Since $\underbrace{|C(y_j)| < |G|}_{\text{since o.w. } y_j \in Z(G)}$, $C(y_j)$ contains

  a subgp of order $p^k$, by induction. $\square$

<u>Def</u> Let $p^m$ be the max'l power of prime $p$ dividing $|G|$.

Then a subgp of $G$ of order $p^m$ is called a

<u>Sylow p-subgroup of G</u>.

By Sylow 1, these subgroups exist.

Consider $\Lambda$, the set of all subgps of $G$.

$G \curvearrowright \Lambda$ by conjugation.

If $H \in \Lambda$, then $\mathrm{Stab}\, H = \underbrace{N_G(H)}_{\substack{\text{normalizer of} \\ H \text{ in } G}} = \{ g \in G \mid gH = Hg \}$.

The orbit $\mathcal{O}_H = \{ aHa^{-1} \mid a \in G \}$ has

cardinality $|\mathcal{O}_H| = [G : \mathrm{Stab}\, H] = [G : N_G(H)]$.

Let $G$ be finite, let $\Pi \subset \Lambda$ be the set of all sylow $p$-subgroups of $G$.

$G \circlearrowright \Pi$ as a restriction of $G \circlearrowright \Lambda$.

Let $\Sigma$ be one of the $G$-orbits in $\Pi$.

$G \circlearrowright \Pi$ restricts to a transitive action $G \circlearrowright \Sigma$.

Let $P \in \Pi$. Then the transitive action $G \circlearrowright \Sigma$ restricts to an action $P \circlearrowright \Sigma$.

<u>Theorem</u> (Sylow II)

1. $\Sigma = \Pi$ (so $G \circlearrowright \Pi$ is transitive)

   i.e. any two sylow $p$-subgps are conjugate

2. $|\Pi|$ divides $[G : P]$, where $P$ is any Sylow $p$-subgp.

And $|\Pi| \equiv 1 \mod p$.

③ Any $\underbrace{p\text{-subgp}}_{\substack{\text{having order} \\ p^r \leq p^m}}$ of $G$ is contained in some Sylow $p$-subgp.

<u>Lemma</u> Let $P \leq G$ be a sylow $p$-subgp let $H \leq G$ of order $p^j$ s.t. $H \subseteq N_G(P)$.

Then $H \leq P$.

<u>Pf</u> Since $P \trianglelefteq N_G(P)$ and $H \leq N_G(P)$, $HP \leq N_G(P)$.

So by an isomorphism thm, $HP/P \cong H/H \cap P$.

so $|HP|/|P| = |H|/|H \cap P|$. So $|HP|/|P|$ is a power of $p$, so $|HP|$ is a power of $p$,

So it must be $p^m = |P|$. So $HP = P$, and $H \leq P$ □

<u>Corollary</u>: $P$ is the unique Sylow $p$-subgp of $N_G(P)$.

<u>Proof of Sylow II</u> The action $P \circlearrowright \Sigma$ decomposes $\Sigma$ into $P$-orbits.

Suppose $P \in \Sigma$. Then $\{P\}$ is one orbit of $P \circlearrowright \Sigma$.

warning: many different things are called P!

Moreover, $\{P\}$ is the only $P$-orbit of size 1. all other orbits have size $p^s$ for some $s \in \mathbb{Z}_{>0}$.

<u>pf</u> Suppose $\{P'\}$ is another 1-element orbit. Then $P \leq N_G(P')$, so $P = P'$.

Any orbit has size $|P|/|\mathrm{Stab}\, Q|$, which divides $|P|$.

So $|\Sigma| \equiv 1 \mod p$.

We claim $\Sigma = \Pi$, so $|\Pi| \equiv 1 \mod p$ and $\underbrace{|\Pi| \text{ divides } [G:P]}_{\text{Orbit-stabilizer Thm}}$. $= [G : \mathrm{Stab}\, P]$, $P \leq \mathrm{Stab}\, P$.

Suppose $\Pi \neq \Sigma$. Then $\exists\, P \in \Pi \setminus \Sigma$. The $P$-orbits on $\Sigma$ all have sizes equal to a positive power of $p$ (by lemma).

So $|\Sigma| \equiv 0 \mod p$, a contradiction. So $\Sigma = \Pi$.

For part ③, let $H$ be a $p$-subgp of $G$, consider $H \curvearrowright \Pi$.

The $H$-orbits in $\Pi$ have sizes that are powers of $p$.

but $|\Pi| \equiv 1 \mod p$, so there is an $H$-orbit of size 1,

meaning $H \leq N_G(P)$, so $H \leq P$ by the lemma. $\square$