date: wednesday, february 7, 2024

Third Sylow Theorem

Recall: If $|G|=p^r m$ with $p \nmid m$, then any subgroup P of G with $|P|=p^r$ is a Sylow p-subgroup.

First Sylow Theorem => a Sylow p-subgroup always exists

(Third Sylow Theorem) Let G be a group with $p \mid |G|$ (p is a prime). If n_p = number of distinct Sylow p-subgroups

1) $n_p \equiv 1 \bmod p$
2) $n_p \mid |G|$

eg. Show that any group G with $|G|=45=3^2 \cdot 5$ has exactly one Sylow 5-subgroup.

By 3rd Sylow theorem,

1) $n_5 \in \{1,6,11,16,21,26,31,36,41\}$
2) $n_5 \in \{1,3,5,9,15,45\}$

So $n_5=1$ (only number in both sets)

Last Class: If P is the only Sylow p-subgroup of G, then P is normal.

In any group G with $|G|=45$, the Sylow 5-subgroup is normal.

Recall: G is simple if it has no normal subgroups.

Corollary: No simple groups of order 45.

"Ingredients"

Lemma: Let H and K be subgroups of G. The number of distinct H conjugates of K is $[H : N(K) \cap H]$.

Lemma ②: Suppose $|x| = p^a$ and $xPx^{-1} = P$ for some Sylow p-subgroup. Then $x \in P$.

Proof (Third Sylow Theorem)

Let $\mathcal{S} = \{P = P_1, P_2, \ldots, P_k\}$ be all the distinct Sylow p-subgroups. We want $n_p = k$. Can make $\mathcal{S}$ into a P-set via action

$$P \times \mathcal{S} \to \mathcal{S}$$
$$(x, P_i) \mapsto xP_ix^{-1} \quad (*)$$

Note $xP_ix^{-1} \in \mathcal{S}$ by the Second Sylow Theorem since any two Sylow subgroups related by conjugation. Since $(*)$ is a group action, $\mathcal{S}$ is partitioned by the orbits.

If $P = P_1$, orbit of $P = \mathcal{O}_P = \{xPx^{-1} \mid x \in P\} = \{P\}$.

If $P_i \neq P_1$, orbit of $P_i = \mathcal{O}_{P_i} = \{xP_ix^{-1} \mid x \in P\}$.

$$|\mathcal{O}_{P_i}| = \text{number of distinct } P\text{-conjugates of } P_i$$
$$= [P : N(P_i) \cap P] = \frac{|P|}{|N(P_i) \cap P|} = p^{a_i} \text{ with } a_i \geq 0$$

In addition, if $P_i \neq P_1$, then $|\mathcal{O}_{P_i}| > 1$ because if $\{xP_ix^{-1} \mid x \in P\} = \{P_i\}$, ie. $xP_ix^{-1} = P_i$ for all $x \in P$. But Lemma ② then forces $P_1 = P_i$ so

$$|\mathcal{O}_{P_i}| = p^{a_i} \text{ with } a_i \geq 1.$$

To summarize, we have partition

$$\mathcal{S} = \mathcal{O}_P \cup \mathcal{O}_{P_2} \cup \cdots \cup \mathcal{O}_{P_t} \leftarrow \text{distinct orbits}$$

So

$$|\mathcal{S}| = |\mathcal{O}_P| + |\mathcal{O}_{P_2}| + \cdots + |\mathcal{O}_{P_t}| = 1 + p^{a_2} + p^{a_3} + \cdots + p^{a_3}.$$

So $n_p = |\mathcal{S}| \equiv 1 \bmod p$.

At the same time, $\mathcal{S}$ is a G-set via action.

$$G \times \mathcal{S} \to \mathcal{S}$$
$$(g, P_i) \mapsto gP_ig^{-1}$$

For any $P \in \mathcal{S}$, orbit under this action is

$$\mathcal{O}_P = \{gPg^{-1} \mid g \in G\} \leftarrow \text{using } 2^{nd} \text{ Sylow theorem}$$

So

$$|\mathcal{O}_P| = [G : N(P) \cap G] = [G : N(P)] = \frac{|G|}{|N(P)|}.$$

So $|N(P)||\mathcal{O}_P| = |G|$.

But $n_p = |\mathcal{O}_P|$, so $n_p \mid |G|$. $\square$

$\boxed{\text{Applications}}$:

Recall: If $|G|=p$ (a prime), then $G \simeq \mathbb{Z}_p$.

Theorem: Suppose $|G|=pq$ with p,q prime and $p<q$. Then G has a unique Sylow q-subgroup (so G is not simple). In addition, if $q \not\equiv 1 \bmod p$, then $G \simeq \mathbb{Z}_{pq}$.

eg. $|G|=77=7\cdot 11$
$11 \not\equiv 1 \bmod 7$ so $G \simeq \mathbb{Z}_{77}$.

<u>Proof</u>
We need n_q = number of distinct Sylow p-subgroups. So $n_q \in \{1, p, q, pq\}$. Note $q \equiv 0 \bmod p$ and $pq \equiv 0 \bmod q$. And $p \equiv p \bmod q$ since $p<q$. So $n_q = 1$ <– only one Sylow q-subgroup.
Now count n_p = number of Sylow p-subgroup if $q \not\equiv 1 \bmod p$. So $n_p \in \{1, q, p, pq\}$. Note $p \equiv 0 \bmod p$ and $pq \equiv 0 \bmod p$. Given $q \not\equiv 1 \bmod p$. So $n_p = 1$.
To summarize, we have a Sylow q-subgroup Q and a Sylow p-subgroup P with $|Q|=q$ and $|P|=p$.
Claim: G is the internal direct product of P and Q.
Need to check:
- $Q \cap P = \{e\}$
- $QP = G$
- $qp = pq$ for all $p \in P, q \in Q$ (use fact P and Q are normal)

So $G \simeq Q \times P \simeq \mathbb{Z}_q \times \mathbb{Z}_p \times \mathbb{Z}_{pq}$ since $\gcd(p,q)=1$.

$\square$

eg. If $|G|=15=3\cdot 5$, we have $3<5$ and $5 \not\equiv 1 \bmod 3$ so $G \simeq \mathbb{Z}_{15}$.