Recall:

Thm. (First Sylow Theorem) If p is prime and $p^r \mid |G|$, then $\exists$ subgroup $H \leq G$ s.t. $|H| = p^r$.

Prop ① Fix any subgroups $H, K \leq G$, with $H \curvearrowright \mathcal{G}$ by conjugation. Then $|\mathcal{O}_K^H| = [H : N(K) \cap H]$.

Prop ② If $P \leq G$ is a Sylow p-subgroup and $x \in N(P)$ satisfies $|x| = p^k$, for some k, then $x \in P$.

We want to prove:

Thm (Second Sylow Theorem) For any prime p and finite group G, the Sylow p-subgroups of G are pairwise G-conjugate.

i.e., the Sylow p-subgroups of G constitute a single orbit of the action $G \curvearrowright \mathcal{G}$.

(Proof.)

Claim. $\forall$ Sylow p-subgroup $P \leq G$, $p \nmid |\mathcal{O}_P|$

(Proof of claim)

$$\text{Prop ①} \Rightarrow |\mathcal{O}_P| = [G : N(P) \cap G] = [G : N(P)].$$

$$\text{Lagrange: } [G : N(P)] \cdot |N(P)| = |G|$$

OTOH, $|G| = |P| \cdot m$, with $p \nmid m$.

from def'n of Sylow p-subgroups

So $[G : N(P)] \cdot |N(P)| = |P| \cdot m$.

Since $P \le N(P)$, $|P| \mid |N(P)|$, so divide both sides by $|P|$:

$$[G:N(P)] \cdot \frac{|N(P)|}{|P|} = m.$$

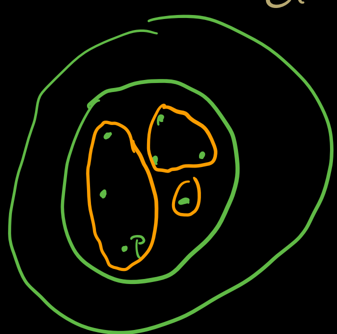
$$p \nmid m \Rightarrow p \nmid [G:N(P)] \Rightarrow p \nmid |\mathcal{O}_P|. \qquad \square$$

Now consider Sylow p-subgroups $P, Q \le G$.

We WTS: $Q \in \mathcal{O}_P$.

$Q \le G \Rightarrow Q \curvearrowright \mathcal{G}$

By an exercise, $\mathcal{O}_P$ is partitioned by Q-conjugacy classes.



Prop (1) $\Rightarrow |\mathcal{O}^Q_{P'}| = [Q : N(P') \cap Q]$.

So $|\mathcal{O}^Q_{P'}|$ divides $|Q| = p^n$, for any $P' \in \mathcal{O}_P$.

$\therefore |\mathcal{O}^Q_{P'}| = p^k$, for some $0 \le k \le n$.

If $k \ge 1$ for every P', then $p \mid |\mathcal{O}^Q_{P'}|$, for every P', and thus $p \mid |\mathcal{O}_P|$. $\divideontimes$

So $\exists\, P' \in \mathcal{O}_P$ s.t. $|\mathcal{O}^Q_{P'}| = p^0 = 1$.

<u>Exercise</u>. Use Prop (2) to show that $P' = Q$.

Then $Q \in \mathcal{O}_P$, so P and Q are G-conjugate. ∎

The proof of the second Sylow theorem tells us a lot about the number of Sylow p-subgroups.

<u>Thm</u> (Third Sylow Theorem) Let G be a finite group, let p be a prime with $p \mid |G|$. If n_p denotes the # of Sylow p-subgroups of G. Then

(i) $n_p \equiv 1 \pmod{p}$;

(ii) $n_p \mid |G|$.

(Proof.) Conclusion (ii) follows from the second Sylow theorem:

$n_p = |\mathcal{O}_P|$, for some Sylow p-subgroup.

So $n_p = [G : N(P)] = |G| / |N(P)|$ divides $|G|$.

Conclusion (i) follows from the proof of Sylow 2:

Recall that the orbits of $Q \curvearrowright \mathcal{G}$ partition $\mathcal{O}_P$, with

$$|\mathcal{O}_Q^Q| = 1 \quad \& \quad |\mathcal{O}_{P'}^Q| = p^k,\ k \geq 1,$$

for $P' \neq Q \in \mathcal{O}_P$.

$$\text{So } n_p = |\mathcal{O}_P| = |\mathcal{O}_Q^Q| + \sum_{\substack{\text{other} \\ Q\text{-orbits}}} |\mathcal{O}_{P'}^Q|$$

$$= 1 + \sum_{\substack{\text{other} \\ Q\text{-orbits}}} p^{k_i}.$$

Since each $k_i \geq 1$, reducing mod p gives

$$n_p \equiv 1 \pmod{p}. \qquad \blacksquare$$

Examples/Applications

Ex. We can now classify all groups of order 99.

Write $99 = 3^2 \cdot 11$.

By Sylow 3: $n_3 \equiv 1 \pmod 3$

$\hookrightarrow n_3 = 1, \cancel{4}, \cancel{7}, \cancel{10}, \cancel{13}, \ldots$

& $n_3 \mid 99$

So $n_3 = 1$

Similarly, $n_{11} \equiv 1 \pmod{11}$ & $n_{11} \mid 99 \Rightarrow n_{11} = 1$.

Let H = unique Sylow 3-subgroup

K = unique Sylow 11-subgroup.

Sylow 2: Conjugating H by any $g \in G$ gives a Sylow 3-subgroup. Since $n_3 = 1$, $gHg^{-1} = H$.

So $H \trianglelefteq G$ is normal.

Similarly, K is normal.

$n_p = 1$
$\Downarrow$
the unique Sylow p-subgroup is normal

Both normal $\Rightarrow HK = KH$.

$|H| = 3^2 = 9$ & $|K| = 11 \Rightarrow |H \cap K| = 1$

So $HK \leq G$ is a subgroup of order $|H| \cdot |K| = 99$.

So $G = HK \cong H \times K$.

$|K| = 11 \Rightarrow K \cong \mathbb{Z}_{11}$

$|H| = 9 \Rightarrow H \cong \mathbb{Z}_3 \times \mathbb{Z}_3$ OR $\mathbb{Z}_9$.

So there are exactly two groups of order 99:

$$\mathbb{Z}_9 \times \mathbb{Z}_{11} \quad ; \quad \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{11}.$$

No non-abelian group of order 99.

__Thm.__ If $|G| = pq$, with $p \neq q$ prime, then G is not simple.
Moreover, if $q \not\equiv 1 \pmod{p}$, then G is cyclic.

(Proof.) WLOG, $p < q$.

Sylow 3: $n_q = qk + 1$; $n_q \mid pq$.

$\therefore n_q = 1 \Rightarrow \exists!\ Q \leq G$ with $|Q| = q$

$\hookrightarrow Q$ is normal.

$\therefore G$ is not simple.

Now $\oint q \not\equiv 1 \pmod{p}$.

Sylow 3: $n_p = pk + 1$ and $n_p \mid pq$.

$\Rightarrow n_p \mid q$

Since q is prime, this means

$n_p = 1$ ✓ OR $n_p = q$

$\Downarrow$

$q \equiv 1 \pmod{p}$, by Sylow 3. ✗

So we get $P \leq G$ normal, with $|P| = p$.

Already have $Q \leq G$, with $|Q| = q$.

By same argument as above,

$$G = PQ \cong P \times Q \cong \mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq}. \qquad \blacksquare$$