Sylow's Theorem: Proofs

We begin with the following special case of Sylow's Theorem:

Theorem (Cauchy's theorem): Suppose that prime \( p \) divides \( |G| \).

Then \( G \) has an element of order \( p \).

Proof:

Consider the set \( X \) consisting of sequences \( (a_1, a_2, \ldots, a_p) \) such that \( a_1 \cdot a_2 \cdot \ldots \cdot a_p = e \). We want to see that \( X \) contains an element of the form \( (a, a, a, \ldots, a) \) for some \( a \in G \), \( a \neq e \).

Observe that \( \mathbb{Z}_p \) acts on \( X \) by cyclic permutations, i.e.,

\[
(a_1, a_2, \ldots, a_p) \mapsto (a_{p-1}, a_p, a_1, a_2, \ldots, a_{p-2})
\]

since if \( xy = e \) in a group \( \Rightarrow y = x^{-1} \) in particular \( yx = e \).

So if \( (a_1, \ldots, a_p) \in X \) then \( (a_p, a_1, \ldots, a_{p-1}) \in X \) as well.

Observe as well that \( a_1, a_2, \ldots, a_p \) can be any choice of elements of \( G \) and then \( a_p = (a_1 \ldots a_{p-1})^{-1} \). So

\[
|X| = |G|^{p-1}
\]

An element of \( X \) is either fixed under the \( \mathbb{Z}_p \)-action or is an orbit.

at size \( q \).
Thus \( |X| = n + kp \)

Since \( p \) divides \( n \), \( |X| - kp = \left( \sum_{e=1}^{p} - kp \right) \) and \( n \neq 1 \), \((e, e, \ldots, e) \in X \),

\[ \Rightarrow X \text{ has a fixed point different than } (e, \ldots, e). \]

\[ \Rightarrow \exists (a, \ldots, a) \in X \not\in aP. \]

\[ \Rightarrow \exists a \in G \text{ of order } p. \quad \square \]

Proof of 1st Sylow Theorem:

Proof by induction on \( n \).

Base case: \( n = 1 \) is Cauchy's Theorem, already proved.

Suppose \( \exists H \leq G, \quad |H| = p^m \). We want to show there is a subgroup of order \( p^{m+1} \).

Consider the action of \( H \) on the set of cosets:\n
Hash on \( G/H \) by:

\[ g \cdot (aH) = gaH, \quad g \in H, \quad aH \in G/H. \]

Orbit-Stabilizer \( \Rightarrow \)

\[ \text{Orbit } \sim |H \cdot (aH)| = \left| H/\text{stab}(aH) \right| \]

\( \Rightarrow \left| H \cdot (aH) \right| \mid \text{stab}(aH) \mid = |H| = p^m \)

\( \Rightarrow \) either \( |H \cdot (aH)| = 1 \) or \( p \) divides \( |H \cdot (aH)| \).
Orbits form a partition of $G/H$, so:

$$|G/H| = \sum_{\text{orbits}} |H \cdot (aH)| = \sum \text{# of sizes 1} + \sum \text{orbits of size 2}$$

$$M = \text{# of orbits of size 1}$$

$$\Rightarrow m = |G/H| - \sum_{\text{orbits of size 2}} |H \cdot (aH)|$$

$p$ divides $(G/H)$

$$= |G|/p - m \quad \text{and since } p \nmid |G|, \quad \text{we have that } p \nmid m.$

Therefore $m$ is divisible by $p$.

Since $H \cdot (eH) = \mathbb{G}/H$, $m \neq 1$ and therefore there exists $aH \neq H$ with $|H \cdot (aH)| = 1$.

For any $aH$ such that $|H \cdot (aH)| = 1$ we have:

$$H = \text{stab}(aH) = \{ h \in H \mid h \cdot aH = aH \}$$

$$= \{ h \in H \mid a^*ha = H \}$$

$$= \{ h \in H \mid a^*ha \in H \}.$$

$$\Rightarrow a \in N(H).$$

So

$$N(H) = \bigcup_{aH \in [H \cdot aH]} aH$$

$$\Rightarrow m = \frac{|N(H)|}{|H|} \Rightarrow p \text{ divides } \frac{|N(H)|}{|H|}$$

$$\Rightarrow \exists \text{ element of order } p,$$

by Cauchy's theorem.
Let \( aH \in N(H)/H \) be an element of \( H \)-conjugacy.

Writing \( \pi: N(H) \to N(H)/H \) for the quotient homomorphism, we have

\[
\pi^{-1}(\langle aH \rangle) = \bigcup_{bH \in \langle aH \rangle} nbH \quad \text{and} \quad |\pi^{-1}(\langle aH \rangle)| = p|H|
\]

(by Lagrange's theorem)

\[
\Rightarrow \pi^{-1}(\langle aH \rangle) = p^{n-1} = p^n.
\]

\[ \square \]

Proof of 2nd Sylow Theorem:

Let \( P \leq G \) be a \( p \)-Sylow subgroup, \( H \leq G \) a \( p \)-group

\( (|H| = p^k \text{ for some } k) \)

Let \( X = \{ gPg^{-1} | g \in G \} \) and let \( G \) act on \( X \) by conjugation. Observe that (by def of \( X \)) the action is transitive.

Also we have \( Syl_b(P) = N(P) \) (by def), so

\[
|X| = \left| \frac{|G|}{|N(P)|} \right| \quad \text{not divisible by } p \quad \text{(why?)}. 
\]

Now consider the action of \( H \) on \( X \), by conjugation. The orbits of this action are a partition of \( X \), so
\[ |X| = \sum_{\text{orbit}} |H \cdot (gP_0)| = \sum_{\text{orb}} \frac{|H|}{|\text{stab}_H(gP_0)|} \]

Therefore, there must be at least one \( H \).

Let \( gP_0 \) have site-1 orbit. Then \( H = \text{Stab}_H(gP_0) = N_G(gP_0) \cap H \).

\[ \Rightarrow H \leq N_G(gP_0) = gN_G(P)g^{-1} \Rightarrow g^{-1}Hg \leq N_G(P). \]

Now, since \( P \leq N_G(P) \), \( P \leq (g^{-1}Hg)P \leq N_G(P) \), by Diamond isomorphism theorem:

\[ |(g^{-1}Hg)P| = \frac{|g^{-1}Hg||P|}{|g^{-1}Hg \cap P|} \]

which is a proper df.

If \( (g^{-1}Hg)P \neq P \), then \( (g^{-1}Hg)P \) is a subgraph of \( G \), of a higher prime power than \( |P| \), but \( |P| \) is \( p \)-Sylow so this can't happen. So \( (g^{-1}Hg)P = P \Rightarrow g^{-1}Hg \leq P. \)
Proof of 3rd Sylow theorem: If there is 1 p-Sylow subgroup, we're done.

Let \( X \) be the set of p-Sylow subgroups, \( P, Q \in X \) distinct subgroups.

From the previous proof (with \( Q = H \)), we know

\[
Q \cap N_G(P) = \text{Stab}_Q(P) \neq Q \quad \text{(else } Q \leq N_G(P) \text{ so )}
\]

\[
Q \leq P \quad \times \quad Q \neq P
\]

So no orbit has size 1, except \( Q \cdot Q = Q \).

Every other orbit has size a positive power of \( p \), so

\[
|X| = mp + 1
\]

\[
\Rightarrow \quad n_p = |X| = 1 \mod p.
\]

Since \( G \) acts transitively on \( X \) we have

\[
|X| = |G/N_G(P)|.
\]

Since \( P \leq N_G(P) \) where

\[
\frac{|G|}{|P|} = \frac{|G/N_G(P)|}{|N_G(P)/P|} = |X| \cdot \left( \frac{|N_G(P)|}{|P|} \right)
\]

\[
\Rightarrow \quad n_p = |X| \quad \text{divides} \quad \frac{|G|}{|P|}.
\]