# Sylow Theorems

<u>Remark:</u> Let $G$ act on $X$ via $*$:

$$*: G \times X \longrightarrow X$$

If $H$ is a subgroup of $G$, then we can restrict the function $*$ to $H \times X$ to get a function (which we also denote by $*$)

$$*: H \times X \longrightarrow X$$

This function $*: H \times X \to X$ satisfies the axioms of an action of $H$ on $X$ and is called the <u>restriction to $H$</u> of the action of $G$ on $X$. For every $x \in X$, we have

$$\mathrm{stab}_H(x) = \{h \in H : h * x = x\} = \mathrm{stab}_G(x) \cap H$$

<u>Lemma:</u> Let $G$ be a finite group and let $P$ be a $p$-subgroup of $G$ (this means $P$ is a $p$-group and a subgroup of $G$). Then

$$[N_G(P) : P] \equiv [G : P] \mod p$$

<u>proof:</u> Consider the action of $G$ on $G/P$ by left multiplication.

$$* \; G \times G/P \to G/P$$
$$g * hP = ghP$$

Restrict this action to ~~[illegible]~~ an action of $P$ on $G/P$:

$$P \times G/P \to G/P$$
$$a * gP = agP$$

Lets calculate the fixed points:

$$
\begin{aligned}
(G/P)^P &= \{gP \in G/P : \forall a \in P,\ a * gP = gP\} \\
&= \{gP \in G/P : \forall a \in P \quad agP = gP\} \\
&= \{gP \in G/P : \forall a \in P \quad (ag)^{-1} g \in P\} \\
&= \{gP \in G/P : \forall a \in P \quad g^{-1} a g \in P\} \\
&= \{gP \in G/P : g \in N_G(P)\} \\
&= N_G(P)/P
\end{aligned}
$$

By a previous corollary, $|X^G| \equiv |X| \bmod p$ when a finite group $G$ acts on a finite set $X$. Applying the here gives

$$[G:P] = |G/P| \equiv |(G/P)^P| = |N_G(P)/P| = [N_G(P):P] \mod p. \quad \square$$

<u>Cor</u>: Let $G$ be a finite group and let $P$ be a $p$-subgroup of $G$ such that $p$ divides $[G:P]$. Then $p$ divides $[N_G(P):P]$.

<u>Thm</u>: (Sylow's First Theorem) Let $G$ be a finite group of order $n$ and let $p$ be a prime number. Write $n = p^a m$ with $a \geq 0$ and $p \nmid m$. If $P$ is a subgroup of $G$ of order $p^b$ with $0 \leq b < a$, then there exists a subgroup $\tilde{P}$ of $G$ of order $p^{b+1}$ such that $P \triangleleft \tilde{P}$.

<u>proof</u>: Let $P$ be a subgp of $G$ of order $p^b$ with $1 \leq b < a$. Then $[G:P] = |G|/|P| = p^a m / p^b = p^{a-b} m$ so $p$ divides $[G:P]$. Then by the corollary, $p$ divides $[N_G(P):P] = |N_G(P)/P|$. Hence by Cauchy's theorem, $N_G(P)/P$ has a subgroup of order $p$. By the correspondence theorem, this subgroup must be of the form $\tilde{P}/P$ for some subgp $\tilde{P}$ of $G$ such that $P \subseteq \tilde{P}$. Further, $\tilde{P} \subseteq N_G(P)$ since $\tilde{P}/P \subseteq N_G(P)/P$, so $P$ is a normal subgroup of $\tilde{P}$.

We have that

$$|\tilde{P}| = [\tilde{P}:\{1\}] = [\tilde{P}:P][P:\{1\}] = |\tilde{P}/P| \cdot |P| = p \cdot p^b = p^{b+1}. \quad \square$$

<u>Cor</u>: Let $G$ be a finite gp of order $n$ and let $p$ be a prime. If $p^b$ divides $n$, then $G$ has a subgroup of order $p^b$.

<u>proof</u>: This follows from induction on $b$ using the previous thm. $\square$

**Def**: Let $G$ be a group of order $n$ and let $p$ be a prime. Write $n = p^a m$ where $a \geq 0$ and $p \nmid m$. Every subgroup of $G$ of order $p^a$ is called a Sylow p-subgp of $G$. The set of Sylow p-subgroups of $G$ is denoted by $Syl_p(G)$. By the first Sylow theorem, $Syl_p(G) \neq \phi$. Note that also by the first Sylow theorem every p-subgroup of $G$ is contained in a Sylow p-subgroup of $G$.

**Remark**: Let $G$ be a finite group and $H \subseteq G$ a subgp. For all $g \in G$, the map

$$\begin{aligned} H &\longrightarrow gHg^{-1} \\ h &\longmapsto ghg^{-1} \end{aligned}$$

is a bijection. Therefore $|H| = |gHg^{-1}|$. Hence $G$ acts on the set of Sylow p-subgps of $G$: If $P \subseteq G$ is a Sylow p-subgp, then $|gPg^{-1}| = |P|$, so $gPg^{-1}$ is also a Sylow p-subgp. We will exploit this action later.

**Example** $G = Sym(3)$, $|G| = 6 = 2 \cdot 3$

$Syl_2(G) = \{ \langle(12)\rangle, \langle(23)\rangle, \langle(13)\rangle \}$

$Syl_3(G) = \{ \langle(123)\rangle \}$

$Syl_p(G) = \{ \{id\} \}$ if $p \geq 5$

**Theorem** (Sylow's $2^{nd}$ Theorem) Let $G$ be a finite group. Any two Sylow $p$-subgps of $G$ are conjugate.

proof: Let $P, Q \in Syl_p(G)$ be two Sylow $p$-subgps of $G$. Consider the action of $P$ on $G/Q$ via left multiplication.

$$*: P \times G/Q \longrightarrow G/Q$$
$$a * bQ = abQ$$

~~Then~~ Considering fixed points, we have

$$|G/Q^P| \equiv |G/Q| \mod p$$

Since $Q$ is a Sylow $p$-subgroup, $p$ does not divide $|G/Q|$. Hence $|G/Q|$ is not $0$, so $|G/Q^P| \geq 1$. Let $aQ \in G/Q^P$.

~~Then for all $g \in P$, we have that~~

~~$gaQ \neq aQ$~~

~~so $(ga)^{-1}a = a^{-1}ga \notin Q$.~~

We claim that $aQa^{-1} = P$.

~~Let $x \in aQa^{-1}$. Then $x = aqa^{-1}$ for some $q \in Q$~~

Let $g \in P$. Then $gaQ = aQ$, so $a^{-1}ga \in Q$. Then $g \in aQa^{-1}$. Hence $P \subseteq aQa^{-1}$. Since $|P| = |aQa^{-1}|$, $P = aQa^{-1}$.

# Sylow Theorems Cont.

**Prop:** Let $G$ be a group and let $H$ and $K$ be finite subgroups of $G$. Then
$$|HK| = \frac{|H|\cdot|K|}{|H\cap K|}$$

**proof:** Consider the function
$$f : H \times K \longrightarrow HK$$
$$f(h,k) = hk$$

$f$ is surjective by construction. We claim that for all $b \in HK$, if $b = hk$, where $h \in H$, $k \in K$, then
$$f^{-1}(b) = \{(hx, x^{-1}k) : x \in H \cap K\}$$

Show inclusion both ways. Let $x \in H\cap K$, then
$$f((hx, x^{-1}k)) = hxx^{-1}k = hk = b$$

so $(hx, x^{-1}k) \in f^{-1}(b)$.

Let $(z,w) \in f^{-1}(b)$. Then $zw = b = hk$. Let $x = h^{-1}z = kw^{-1}$. Then $x \in H\cap K$, and $(z,w) = (hx, x^{-1}k)$. Therefore we've show that $f^{-1}(b) = \{(hx, x^{-1}k) : x \in H\cap K\}$.

Now we claim that $|f^{-1}(b)| = |H\cap K|$. This is true because if $(hx, x^{-1}k) = (hy, y^{-1}k)$ for $x,y \in H\cap K$, then $x = y$.

We now know that $f$ is a surjective function and for all $b \in HK$, $|f^{-1}(b)| = |H\cap K|$. Therefore
$$|H\times K| = |HK|\cdot|H\cap K|$$

which implies that

$$|HK| = \frac{|H|\cdot|K|}{|H\cap K|}$$

since $|H\times K| = |H|\cdot|K|$. $\square$

<u>Theorem</u> (Sylow's Third Theorem): $G$ - finite group of order $n$. $p$ - prime number. Write $n = p^a m$, $p\nmid m$ and let $n_p(G) = |Syl_p(G)|$ be the number of Sylow $p$-subgroups of $G$. Then

$$n_p(G) \equiv 1 \mod p \quad \text{and} \quad n_p(G) \text{ divides } m$$

<u>proof</u>: By Sylow's 2nd theorem, the conjugation action of $G$ on $Syl_p(G)$ is transitive:

$$\begin{aligned} *: G \times Syl_p(G) &\to Syl_p(G) \\ (g, P) &\mapsto gPg^{-1} \end{aligned}$$

Therefore $|Syl_p(G)| = |orb(P)|$ for any $P \in Syl_p(G)$. Then by the orbit stabiliser thm.

$$|orb(P)| = |G| / |stab(P)|$$

Now observe that $stab(P) = \{g \in G : gPg^{-1} = P\} = N_G(P)$. Hence

$$n_p(G) = |Syl_p(G)| = [G : N_G(P)]$$

Finally we have that since $P \subseteq N_G(P)$,

$$m = [G:P] = [G:N_G(P)][N_G(P):P] = n_p(G)[N_G(P):P]$$

So $n_p(G)$ divides $m$.

Now we show that $n_p(G) \equiv 1 \bmod p$.
Let $P \in Syl_p(G)$ and consider the action

$$\begin{aligned} *: P \times Syl_p(G) &\longrightarrow Syl_p(G) \\ (a, Q) &\longmapsto aQa^{-1} \end{aligned}$$

Since $P$ is a $p$-group,

$$n_p(G) = |Syl_p(G)| \equiv |Syl_p(G)^P| \bmod p$$

We claim that $Syl_p(G)^P = \{P\}$, so $|Syl_p(G)^P| = 1$ and we would be done with the proof. Let $Q \in Syl_p(G)^P$. This means that for all $a \in P$, $aQa^{-1} = Q$. Then $P$ normalizes $Q$ ($P \subseteq N_G(Q)$), so $PQ$ is a subgroup of $G$. We have by the previous proposition that

$$|PQ| = \frac{|P| \cdot |Q|}{|P \cap Q|}$$

So $|PQ|$ is a power of $p$. We have that $P \subseteq PQ$, so $|PQ|$ must be $p^a$ since $p^a$ is the largest power of $p$ dividing $|G|$ and $|P| = p^a$. Hence $P = PQ$. Similarly $Q = PQ$, so $P = Q$. $\square$

<u>Remark</u>: $\cancel{|Syl_p(G)| = 1 \text{ iff}}$ $Syl_p(G) = \{P\}$ if and only if $P$ is a normal subgroup of $G$ because all Sylow $p$-subgroups are conjugate. Therefore Sylow's 3rd theorem gives us a way to prove the existence of normal subgroups by proving that $n_p(G) = 1$ for some $p$.

Example: Let $G$ be a group such that $|G| = 100$. We will use Sylow's 3rd theorem to show that $G$ has a normal subgroup of size 25. We have.

$$100 = 5^2 \cdot 2^2 = 25 \cdot 4$$

Then $n_5(G) \equiv 1 \mod 5$ and $n_5(G)$ divides 4

Hence $n_5(G)$ must be 1, so there is only one Sylow 5-subgroup of $G$. This Sylow 5-subgroup must then be normal, and it has size 25.