# THE SYLOW THEOREMS

## 1. Group Actions

An **action** of a group $G$ on a set $S$ is a map

$$G \times S \longrightarrow S, \quad (g, x) \longmapsto gx$$

such that

- The action is associative,
$$(g\tilde{g})x = g(\tilde{g}x) \quad \text{for all } g, \tilde{g} \in G \text{ and } x \in S.$$
- The group identity element acts trivially,
$$1_G x = x \quad \text{for all } x \in S.$$

Some examples:

- Every group $G$ acts on itself by left-translation,
$$G \times G \longrightarrow G, \quad (g, \tilde{g}) \longmapsto g\tilde{g}.$$
- Let $G$ be a group and let $H$ be subgroup, not necessarily normal. Then $G$ acts on the coset space $G/H$ by left-translation,
$$G \times G/H \longrightarrow G/H, \quad (g, \tilde{g}H) \longmapsto g\tilde{g}H.$$
This example specializes to the previous one when $H$ is trivial.
- Every group $G$ acts on itself by left-conjugation
$$G \times G \longrightarrow G, \quad (g, \tilde{g}) \longmapsto g\tilde{g}g^{-1}.$$
- Every group $G$ acts on the set of its subgroups by left-conjugation,
$$G \times \{\text{subgroups}\} \longrightarrow \{\text{subgroups}\}, \quad (g, H) \longmapsto gHg^{-1}.$$
- The symmetric group $G = S_n$ by definition acts on the set $S = \{1, 2, \cdots, n\}$. However, a little care is required here, since to make the action obey the associative rule we must compose permutations from right to left.
- The dihedral symmetry group $D_n$ of the regular $n$-gon in the plane acts on the set of vertices of the $n$-gon, and it acts on the set of edges of the $n$-gon, and it acts on the set of **flags** of the solid, where a flag is a pair
$$(\text{vertex, edge})$$
such that the vertex lies in the edge.
- Let $G$ be a rotation group of a Platonic solid. Then $G$ acts on the set of vertices of the solid, and $G$ acts on the set of edges of the solid, and $G$ acts on the set of faces of the solid, and $G$ acts on the set of flags
$$(\text{vertex, edge, face}), \quad \text{vertex} \subset \text{edge} \subset \text{face}$$
of the solid.
- Let $V$ be any vector space over a field $k$. The group of $k$-linear automorphisms of $V$ acts on $V$.

Let a group $G$ act on a set $S$. Define a binary relation $\sim_G$ on $S$,

$$x \sim_G \tilde{x} \quad \text{if } \tilde{x} = gx \text{ for some } g \in G\}.$$

Immediately, $\sim_G$ is an equivalence relation. Thus it partitions $S$ into mutually disjoint **orbits**,

$$S = \bigsqcup \mathcal{O}_x, \qquad \mathcal{O}_x = \{gx : g \in G\}.$$

Consequently we have a counting formula

$$|S| = \sum |\mathcal{O}_x|, \quad \text{sum over disjoint orbits.}$$

Each set-element $x \in S$ has a corresponding **isotropy subgroup** in $G$,

$$G_x = \{g \in G : gx = x\}.$$

Isotropy subgroups need not be normal but the conjugate of one isotropy subgroup is another,

$$gG_xg^{-1} = G_{gx}.$$

Each isotropy coset $gG_x$ takes $x$ to $gx$, and distinct cosets $gG_x$ and $\tilde{g}G_x$ take $x$ to distinct values. Thus we have the **orbit–stabilizer formula**,

$$|\mathcal{O}_x| = |G/G_x|,$$

and the counting formula becomes

$$|S| = \sum_{\mathcal{O}_x} |G/G_x|, \quad \text{sum over disjoint orbits.}$$

## 2. A Preliminary Abelian Group Lemma

**Lemma 2.1** (Cauchy)**.** *Let $G$ be a finite abelian group, and let $p \mid |G|$ where $p$ is prime. Then $G$ contains an element—and therefore a subgroup—of order $p$.*

The lemma is immediate granting the structure theorem for finite abelian groups, but we prove it from first principles.

*Proof.* If $G$ contains an element whose order is a multiple of $p$ then we are done. So suppose that $G$ contains no such element, and let

$$n = \text{lcm}\{\text{order of } g : g \in G\}.$$

Thus $p \nmid n$. We will show that

$$|G| \mid n^k \quad \text{for some } k.$$

To see this, take any $b \neq 1$ in $G$, and note that $\langle b \rangle$ is a proper subgroup of $G$ since $p \nmid |\langle b \rangle|$ but $p \mid |G|$. On the other hand, $|\langle b \rangle| \mid n$. In the quotient group $G/\langle b \rangle$ we also have $(g\langle b \rangle)^n = 1$ for all elements $g\langle b \rangle$, and so the lcm of the orders of the elements of $G/\langle b \rangle$ divides $n$. Now by induction on the group order, $|G/\langle b \rangle| \mid n^{k-1}$ for some $k$, i.e., $|G|/|\langle b \rangle| \mid n^{k-1}$ for some $k$, and thus

$$|G| \mid |\langle b \rangle| \, n^{k-1} \mid n^k.$$

The display contradicts the fact that $p \mid |G|$, and so the supposition that $G$ has no element whose order is a multiple of $p$ is untenable. □

## 3. Sylow Theorems: the Existence Theorem

Let a finite group $G$ act on itself by conjugation,

$$g(\tilde{g}) = g\tilde{g}g^{-1}, \quad g, \tilde{g} \in G.$$

Then the counting formula becomes the **class formula**,

$$|G| = |Z(G)| + \sum_{|\mathcal{O}_x|>1} [G : G_x],$$

where the sum is over non-singleton conjugacy classes in $G$ and the isotropy subgroup $G_x$ is the **normalizing subgroup** of $x$,

$$G_x = \{g \in G : gxg^{-1} = x\}.$$

When the conjugacy class of $x$ is a non-singleton, $G_x$ is a proper subgroup of $G$.

Also, if $G$ acts on a subset $S$ of its subgroups $H$ by conjugation then the class formula becomes

$$|S| = \sum_{\mathcal{O}_H} [G : G_H],$$

where now the isotropy subgroup $G_H$ is the normalizing subgroup of the subgroup $H$,

$$G_H = \{g \in G : gHg^{-1} = H\}.$$

**Definition 3.1.** *Let $G$ be a finite group, and let $p \mid |G|$ where $p$ is prime. Then a* **$p$-Sylow subgroup** *of $G$ is a subgroup of order $p^n$ where $p^n \parallel |G|$.*

**Theorem 3.2.** *Let $G$ be a finite group, and let $p \mid |G|$ where $p$ is prime. Then there exists a $p$-Sylow subgroup of $G$.*

*Proof.* The proof is by induction on the order of $G$. The base case where $|G| = p$ is clear. If $G$ contains a subgroup $H$ whose index in $G$ is coprime to $p$ then we are done by induction. So assume that $p \mid [G : H]$ for every proper subgroup $H$ of $G$.

Let $G$ act on itself by conjugation,

$$(g, x) \longmapsto gxg^{-1}.$$

As above, the class formula is

$$|G| = |Z(G)| + \sum_{|\mathcal{O}_x|>1} [G : G_x].$$

In the sum, since $|\mathcal{O}_x| > 1$ for each $x$, also $G_x$ is a proper subgroup of $G$ for each $x$. Thus, counting modulo $p$ shows that $p \mid |Z(G)|$. By the preliminary abelian group lemma, there exists some $a \in Z(G)$ having order $p$. The order-$p$ subgroup $\langle a \rangle$ is normal in $G$ since $a$ is central. Because $p^{n-1} \parallel |G/\langle a \rangle|$, induction gives a $p$-Sylow subgroup $\widetilde{K}$ of $G/\langle a \rangle$. Let

$$K = f^{-1}(\widetilde{K}) \quad \text{where} \quad f : G \longrightarrow G/\langle a \rangle \text{ is the canonical map.}$$

Since the canonical map is $p$-to-1, it follows that $K$ is a $p$-Sylow subgroup of $G$. $\square$

## 4. Sylow Theorems: the Further Results

**Definition 4.1.** *Let $G$ be a finite group, and let $p \mid |G|$ where $p$ is prime. Then a $p$-**subgroup** of $G$ is a subgroup of order $p^n$ where $p^n \mid |G|$.*

**Theorem 4.2.** *Let $G$ be a finite group.*
(1) *Every $p$-subgroup of $G$ is contained in a $p$-Sylow subgroup.*
(2) *All $p$-Sylow subgroups of $G$ are conjugate.*
(3) *The number of $p$-Sylow subgroups is 1 modulo $p$ and divides $|G|$.*

*Proof.* Let $S$ denote the set of $p$-Sylow subgroups of $G$, a nonempty set by the previous theorem. Let $G$ act on $S$ by conjugation. Let $P$ denote some $p$-Sylow subgroup of $G$, let $S_o$ denote its orbit, and let $G_P$ denote the normalizer of $P$. Since $G_P$ contains $P$,

$$|S_o| = [G : G_P] \text{ is coprime to } p.$$

To prove (1), let $H$ be a nontrivial $p$-subgroup of $G$. Then $H$ acts by conjugation on $S_o$, and

$$|S_o| = \sum_{P'} [H : H_{P'}],$$

summing over one $p$-Sylow subgroup from each $H$-suborbit of the $G$-orbit of the $p$-Sylow subgroup $P$. Since $|S_o|$ is coprime to $p$ and each $[H : H_{P'}]$ is a $p$-power, some suborbit is a singleton. That is, $H \subset G_{P'}$ for some $P'$, making $HP'$ a subgroup of $G$. Also, $P'$ is normal in $HP'$, and so the second isomorphism theorem of group theory gives

$$HP'/P' \cong H/(H \cap P').$$

The quotient group on the left side of the display has order coprime to $p$ because $P'$ is a $p$-Sylow subgroup, while the quotient group on the right side has $p$-power order because $H$ is a $p$-subgroup. Thus both quotient groups are trivial. That is, $H \subset P'$, i.e., $H$ is contained in a $p$-Sylow subgroup as desired.

To prove (2), let $H$ in the proof of (1) be any $p$-Sylow subgroup. The proof of (1) shows that $H$ is a subgroup of a conjugate of $P$, and so $H$ is the entire conjugate of $P$ since their orders are equal. Note that now we have $S_o = S$.

To prove (3), recall that $S$ is the set of $p$-Sylow subgroups of $G$, so that $|S|$ is the number of $p$-Sylow subgroups. Let the $p$-Sylow subgroup $P$ act on $S$ by conjugation. To show that $|S| = 1 \text{ mod } p$, write

$$|S| = \sum_{P'} [P : P_{P'}],$$

summing over one $P'$ from each $P$-orbit. Each term in the sum is 1 or a $p$-power. The $P$-suborbit of $\{P\}$ is itself, so one term in the sum is 1. Any other $p$-Sylow subgroup $P' \neq P$ has a nontrivial orbit, for otherwise $P$ normalizes $P'$, making $PP'$ a subgroup of $G$ whose order is divisible by too high a power of $p$. Hence the rest of the terms in the sum are nontrivial $p$-powers. Thus $|S| = 1 \bmod p$.

As for the last statement, the equality displayed at the beginning of the proof is now

$$|S| = [G : G_P],$$

and the right side divides $|G|$. □

The proofs of Theorem 3.2 and Theorem 4.2 are a *tour de force* for group actions.