# Sylow Theorems

S. Kumaresan
School of Math. and Stat.
University of Hyderabad
Hyderabad 500046
kumaresa@gmail.com

Proof of all the theorems here is based on Group action, and we will use the following facts.

**Fact 1.** Let $G$ be a group and $H$, a subgroup of $G$. Then $G$ acts transitively on the set $G/H$, left cosets of $H$,where the action is defined as: $g \cdot aH = gaH$. (In fact, all transitive actions arise in this way.)

**Fact 2.** Let $G$ be a group acting on a set $X$. For each $x \in X$, we define $G_x := \{g \in G : gx = x\}$, called the stabilizer of $x$ in $G$. Note that $G_x$ is a subgroup of $G$ for all $x \in X$. Now if $G$ acts transitively on $X$ and if $x$, $y$ in $X$, then their stabilizers are related as follows: if $a \in G$ is such that $ax = y$, then $G_x = aG_y a^{-1}$.

**Fact 3.** Let $G$ be a finite group acting on a finite set $X$. For every point $x$ in $X$ we define $O_x := \{gx \mid g \in G\}$, called the orbit of $x$. Then $|G| = |O_x| \cdot |G_x|$. In other words the cardinality of an orbit divides that of the group $G$.

**Fact 4.** Let $G$ be a finite group acting on a finite set $X$. Then there exist mutually disjoint orbits $\mathcal{O}_1, \ldots, \mathcal{O}_n$ for some $n$ such that $X = \cup_{i=1}^n \mathcal{O}_i$. Hence we have

$$|X| = |\mathcal{O}_1| + |\mathcal{O}_2| + \cdots + |\mathcal{O}_n|.$$

Note that if $x \in \mathcal{O}_i$ is any element then $\mathcal{O}_i = O_x$. So we can also write

$$|X| = |O_{x_1}| + \cdots + |O_{x_n}|, \qquad \text{where } x_i \in \mathcal{O}_i \text{ is any element.}$$

**Theorem 1** (Lagrange's Theorem)**.** If $G$ is a finite group, then the order of a subgroup $H$ divides that of $G$. That is, if $H \leq G$, then $|H|$ divides $|G|$.

**Proof:** Let $H$ be a subgroup of $G$. Then by Fact 1, $G$ acts transitively on $G/H$, the set of left cosets of $H$. Now the stabilizer of the identity coset $eH = H \in G/H$ is given by $G_H = \{g \in G \mid gH = H\} = H$. But then by Fact 3, $|G| = |G_H| \cdot |O_H| = |H| \cdot |O_H|$. Hence $|H|$ divides $|G|$. □

**Theorem 2.** Let $G$ be a group of even oder. Then there exists an element of order 2.

**Proof:** Let $H = \{+1, -1\}$ be the 2-element group with multiplication. We let $H$ act on $G$ as follows: $1 \cdot g := g$ and $-1 \cdot g := g^{-1}$, for all $g \in G$. Using Fact 4 we get

$$|G| = |O_{x_1}| + \cdots + |O_{x_n}|, \text{ for some } x_1, \ldots, x_n \in G.$$

Now we note that for each $x \in G$, the orbit $O_x = \{x, x^{-1}\}$ and if $x = e$, then $O_e = \{e\}$. Therefore,

$$|G| = 1 + \sum_{x_i \neq e} |O_{x_i}|.$$

So, if $|O_{x_i}| = 2$, for all $x_i \neq e$, then $|G|$ is congruent to 1 modulo 2, a contradiction. Hence there exists at least one element $x_j \neq e$ such that $|O_{x_j}| = 1$. This means that $x_j^{-1} = x_j$, or $x_j^2 = e$. Hence,the order of $x_j$ is 2. □

**Remark:** In fact, we established that there exists odd number of elements of order 2.

**Theorem 3** (Cauchy Theorem)**.** Let $G$ be a finite group and $p$ be a prime such that $p$ divides the order of $G$. Then there exists an element $a \in G$ such that order of $a$ is $p$.

**Proof:** Assume $|G| = m$. Consider the set

$$X = \{(g_1, g_2, \ldots, g_p) \mid g_i \in G, g_1 \cdot g_2 \cdots g_p = e\}.$$

Note that $(e, e, \ldots, e) \in X$. In fact $|X| = m^{p-1}$, because each $g_i$, $1 \leq i \leq p-1$ can be chosen in $m$ ways, and once we choose $g_1, g_2, \ldots, g_{p-1}$, then $g_p = (g_1 \cdots g_{p-1})^{-1}$ is uniquely determined. Observe that $p$ divides $|X|$, since $p$ divides $m$ and $p - 1 \geq 1$.

Let $H$ be the group generated by the $p$ cycle $\sigma := (1, 2, \ldots, p)$. Then $|H| = p$. There exists a natural action of $H$ on $X$, defined as follows: If $\tau \in H$ and $(g_1, \ldots, g_p) \in X$, then $\tau(g_1, \ldots, g_p) := (g_{\tau(1)}, \ldots, g_{\tau(p)})$. We need to check that for all $x \in X$ and $\tau$ in $H$, $\tau(x) \in X$. (Note that if $G$ is abelian then this is trivial.) Now if $x = (g_1, \ldots, g_p) \in X$, then$g_1 \cdots g_p = e$, hence $g_1 = (g_2 \cdots g_p)^{-1}$. So, $\sigma(g_1, \ldots, g_p) = (g_2, \ldots, g_p, g_1) \in X$, if $g_2 \cdot g_3 \cdots g_p \cdot g_1 = e$. But this is true because $g_2 \cdots g_p \cdot g_1 = (g_2 \cdots g_p) \cdot (g_2 \cdots g_p)^{-1} = e$. Now we write $X = \cup_{i=1}^{n} O_{x_i}$ as the disjoint union of its orbits $O_{x_i}$ for some $x_1, \ldots, x_n \in X$. Therefore

$$|X| = |O_{x_1}| + \cdots + |O_{x_n}|$$

Since the orbit $O_{(e,\ldots,e)} = \{(e, \ldots, e)\}$, we can write

$$|X| = 1 + \sum_{x_i \neq (e,\ldots,e)} |O_{x_i}|$$

Since $|O_{x_i}|$ divides $p$ for each $i$, either $|O_{x_i}| = 1$ or $p$, for $1 \leq i \leq n$. If $|O_{x_i}| = p$, for all $x_i \neq (e, \ldots, e)$, then $|X| \equiv 1 \pmod{p}$, a contradiction to the fact that $p$ divides $|X|$. Hence there exists at least one orbit $O_{x_i}$ for $x_i \neq (e, \ldots, e)$ such that $|O_{x_i}| = 1$. Let us fix one such $x_i = (a_1, \ldots, a_p)$. Then $\sigma(a_1, \ldots, a_p) = (a_2, \ldots, a_p, a_1)$, and hence $(a_1, \ldots, a_p) = (a_2, \ldots, a_p, a_1)$. This implies that $a_1 = a_2$, $a_2 = a_3, \ldots a_p = a_1$. Hence $a_1 = a_2 = \cdots = a_p (= a$ say). But $a_1 \cdots a_p = e$, implies $a^p = e$. □

**Remark:** We note that, as in theorem 2, here too we have proved that the number of elements of order $p$ in $G$ is $\equiv -1(|p|)$.

**Theorem 4** (The Sylow Theorem)**.** Let $G$ be a finite group such that $|G| = p^n m$, where $n \geq 1$ and $(m, p) = 1$. Then

1. There exists a subgroup $H$ of order $p^n$ called the Sylow $p$- subgroup of $G$.

2. Any two Sylow $p$-subgroups are conjugate in $G$. That is if $H$ and $K$ are two Sylow $p$-subgroups of $G$ then $K = gHg^{-1}$, for some $g \in G$.

3. Let $k$ be the number of Sylow $p$-subgroups of $G$, then $k$ is congruent to 1 modulo $p$.

   (For our convenience we will call the statements (1), (2),and (3) as 1st, 2nd and 3rd Sylow theorem.)

**Motivation for the proof of the 1st Sylow theorem.** Consider the set $\Sigma = \{S \subseteq G : |S| = p^n\}$. If at all there is a subgroup of order $p^n$ then it has to be in $\Sigma$. Now one can immediately think of an action of $G$ on $\Sigma$ defined as follows: If $g \in G and S \in \Sigma$, then $g \cdot S := \{gs \mid s \in S\}$. If there is a Sylow $p$-subgroup $H$, then $H \in \Sigma$ and its orbits under this action is the set of left cosets, $\{gH \mid g \in G\}$. Hence $|O_H| = m$. This means that $(p, |O_H|) = 1$. This suggests that we should look for an orbit $\mathcal{O}$ such that $p$ does not divide $|\mathcal{O}|$. So, we must prove that there exists an orbit $\mathcal{O}$ such that $p$ does not divide $|\mathcal{O}|$. Fix one such orbit $\mathcal{O}$, and $S \in \mathcal{O}$. Consider the stabilizer $G_S$ of $S$ and call it $H$. Then we prove that $|H| = p^n$.

**Proof of 1st Sylow theorem:** Let us consider the set $\Sigma = \{S \subseteq G : |S| = p^n\}$. Note that $|\Sigma| = \binom{p^n m}{p^n}$. We now claim that

1. $\binom{p^n m}{p^n} \equiv m(|p|)$

2. and $p$ does not divide $\binom{p^n m}{p^n}$.

For the time being let us assume these claims and complete the proof of the theorem. By Fact 4 we can write $\Sigma = \cup_{i=1}^{k} \mathcal{O}_i$, as the disjoint union of its orbits under this action of $G$ and hence $|\Sigma| = \sum_{i=1}^{k} |\mathcal{O}_i|$. Since $p$ does not divide the left hand side, $p$ does not divide the right hand side. This implies that there exists at least one $i$ such that $p$ does not divide $|\mathcal{O}_i|$. We choose one such $\mathcal{O}_i$ and call this orbit $\mathcal{O}$. Fix $S$ in $\mathcal{O}$ and let $H = G_S$, the stabilizer of $S$ in $G$. We will now show that $H$ is a $p$-sylow sub group of $G$. i.e., we will show that $|H| = p^n$.

By Fact 3, we have that $|G| = |G_S| \cdot |\mathcal{O}| = |H| \cdot |\mathcal{O}|$. Since $p^n$ divides $|G|$ and $p$ does not divide $|\mathcal{O}|$, $p^n$ divides $|H|$, hence $|H| \geq p^n$. Next fix $s_0$ in $S$ and let $H$ act on $S$ in a natural way: $(h, s) \mapsto hs$. (Check that this is an action.) Now $H_{s_0} = \{h \in H \mid hs_0 = s_0\} = \{e\}$, since $hs_0 = s_o$ implies $h = e$, by the right cancellation law in the group. Hence $|H| = |H_{s_0}| \cdot |O_{s_0}| = 1 \cdot |O_{s_0}| \leq |S|$, since $O_{s_0} \subseteq S$. So, $|O_{s_0}| \leq |S| = p^n$. Thus $|H| \leq p^n$. It follows that $|H| = p^n$. □

We now prove the claims made in the proof of the theorem.

**Lemma 1.** *If $p$ is a prime and $(m, p) = 1$ then for $n \geq 1$*

1. $\binom{p^n m}{p^n} \equiv m(|p|)$ *and*

2. *$p$ does not divide $\binom{p^n m}{p^n}$.*

**Proof:** Note that (2) follows from (1). To prove (1) consider the polynomial $(1+X)^{p^n m}$ in $\mathbb{Z}_p[X]$. So, $\binom{p^n m}{p^n}$ is the coefficient of of $X^{p^n}$ in the polynomial $(1+X)^{p^n m}$. On the other hand $(1+X)^{p^n m} = (1+X^{p^n})^m$, since $(a+b)^p = a^p + b^p$ in $\mathbb{Z}_p$. Hence the coefficient of $X^{p^n}$ in this case is $\binom{m}{1} = m(|p|)$. Thus $\binom{p^n m}{p^n} \equiv m(|p|)$. □

**Observation 1.** Let us choose an orbit $\mathcal{O}$ such that $p$ does not divide $|\mathcal{O}|$. Fix $S \in \mathcal{O}$ and define $H = G_S$ as defined in the proof of 1st Sylow theorem. Fix $s_0 \in S$, then $h \mapsto hs_0$ is a bijection between $H$ and $S$.(why?) So, $Hs_0 \subseteq S$, but $|Hs_0| = |S| = p^n$. Hence $S = Hs_0$. Thus $S$ actually arises as a right coset of $H$.

Now let $T \in \mathcal{O}$ be any element, then $T = gS$, for some $g \in G$. Hence $T = gHs_0 = as_0^{-1}Hs_0 = aK$, where $gs_0 = a$ and $K = s_0^{-1}Hs_0$. Thus any element $T$ in $\mathcal{O}$ is of the form $T = aK$, where $K$ is a fixed Sylow $p$-subgroup of $G$ given by $K = s_0^{-1}Hs_0$.

**Observation 2.** In particular if $\mathcal{O}$ is such that $p$ does not divide $|\mathcal{O}|$, then $\mathcal{O}$ is set of left cosets of $K$ and hence we conclude that $|\mathcal{O}| = m$.

### Motivation of the proof of 2nd Sylow theorem

Let $H$ be a Sylow $p$-subgroup of $G$. By Fact 1 the stabiliser of any left coset $aH$ of $H$ under the action of $G$ on the set of all left cosets $G/H$ is a conjugate of $H$. Thus if $S$ is a conjugate of $H$, that is $S{=}gHg^{-1}$ for some $g \in G$. Then $S$ fixes $aH$ for some $a \in G$. By looking at the stabilizer of $aH$ for all $a \in G$ we get all conjugates of $H$. Thus if we want to prove that any Sylow $p$-sbugroup $S$ is a conjugate of $H$, we must prove that $S$ fixes $aH$ for some $a \in G$. Proof of this fact follows from the following lemma.

**Lemma 2.** *Let $G$ be a $p$ group such that $|G| = p^n$ and $X$ be a finite set on which $G$ acts. Define the set $X^G = \{x \in X \mid gx = x, \text{ for all } g \in G\}$. Then $|X| \equiv m(|p|)$ where $m = |X^G|$.*

**Proof:** By Fact 4 we have

$$|X| = \sum_{i=1}^{m} |O_{x_i}| \text{ for some } x_1, \dots, x_n \in X.$$

Since $|O_{x_i}|$ divides $p^n$, $|O_{x_i}| = p^k$, for some $0 \leq k \leq n$. But $|O_{x_i}| = 1$ iff $x_i \in X^G$. This implies that $|X^G| = \sum_{x_i \in X^G} |O_{x_i}|$. Hence,

$$|X| = \sum_{i=1}^{m} |O_{x_i}| = \sum_{x_i \in X^G} |O_{x_i}| + \sum_{x_i \notin X^G} |O_{x_i}| = |X^G| + \sum_{x_i \notin X^G} |O_{x_i}|.$$

Since $p$ divides $|O_{x_i}|$ for $x_i \neq X^G$, implies that $p$ divides $\sum_{x_i \notin X^G} |O_{x_i}|$. Hence $|X| \equiv m(|p|)$. □

**Ex. 3.** Using the above lemma prove

1. Cauchy theorem and
2. the center of group $G$, $Z(G) = \{g \in G \mid ga = ga \text{ for all } a \in G\}$ is non trivial, if $G$ is a group of a prime power.

### Proof of 2nd Sylow theorem:

Let $H$ and $S$ be two Sylow $p$-subgroups of $G$. Let $S$ act on $X = G/H$ by restricting the standard action of $G$ on $X = G/H$. By Lemma 2, $|X| = m \equiv |X^S|(|p|)$. Since $(p, m) = 1$, it follows that $X^S \neq$. This means that there exists $x = aH$ in $X$ such that $saH = aH$ for all $s \in S$. In other words the stabiliser of $aH$ for the standard action of $G$ on $G/H$ is $S$. Since this action of $G$ on $G/H$ is transitive, the stabilisers of $H$ and $aH$ are conjugate. This proves that $S = aHa^{-1}$. □

**Proof of 3rd Sylow theorem:** Let $k$ be the number of Sylow $p$-subgroups of $G$. Under the action of $G$ on $\Sigma$ (as defined in the proof of 1st Sylow theorem) either $p$ divides the order of an orbit or it does not. We break the orbits of $G$ in $\Sigma$ into two classes. Let $\{\mathcal{O}_i\}_{i=1}^r$ be the collection of orbits such that $p$ does not divide $|\mathcal{O}_i|$ and $\{T_j\}_{j=1}^l$ be the collection of orbits such that $p$ divides $|T_j|$. We claim that $k = r$.

If $H$ is a Sylow $p$-subgroup of $G$ then $H \in \Sigma$ and the orbit of $H$ is the left cosets of $H$. So, $|O_H| = m$, hence $p$ does not divide $|O_H|$. This means that $O_H = \mathcal{O}_i$ for some $1 \le i \le r$ . This proves that $k \le r$. We now claim that $r \le k$. First notice that each $\mathcal{O}_i$ is the set of left cosets of a Sylow $p$ subgroup. If $H_i \in \mathcal{O}_i$ is the Sylow $p$-subgroup, then $H_i = H_j$ iff $i = j$. For, otherwise $GH_i = GH_j$ and hence $\mathcal{O}_i = \mathcal{O}_j$, which is a contradiction. This proves that $k = r$. Now we have

$$|\Sigma| = \sum_{i=1}^{k} |\mathcal{O}_i| + \sum_{j=1}^{l} |T_j| = km + tp.$$

Since $p$ does not divide $|\mathcal{O}_i|$ but $|\mathcal{O}_i|$ divides $p^n m$ it follows that $|\mathcal{O}_i| = m$. Hence $|\Sigma| \equiv mk(|p|)$. But by Lemma 1, $|\Sigma| = \binom{p^n m}{p^n} \equiv m(|p|)$. Hence these two together imply that $k \equiv 1(|p|)$. □

**2nd proof of 3rd Sylow theorem:**

Let $X$ be the set of all Sylow subgroups of $G$. Fix $H \in X$ and let $H$ act on $X$ by conjugation, that is $(h, S) \mapsto hSh^{-1}$. (Why is this an action?) By Lemma 2, $|X| \equiv |X^H|(|p|)$. First notice that $H \in X^H$. So, it is enough to prove that $|X^H| = 1$. That is if $S \in X^H$ then $S = H$. Let $S \in X^H$, then

$$hSh^{-1} = S \qquad \text{for all } h \in H. \tag{1}$$

This implies that $hS = Sh$, for all $h \in H$ and hence $HS = SH$. Now let $T = HS$. We claim that $T$ is a subgroup of $G$. For $h_1s_1, h_2s_2 \in T$, $(h_1s_1)(h_2s_2)^{-1} = h_1h_1s_2^{-1}h_2^{-1} = h_1h_2^{-1}h_2s_1s_2^{-1}h_2^{-1} = (h_1h_2^{-1}) \cdot (h_2s_1s_2^{-1}h_2^{-1}) \in T$, since $h_1h_2^{-1} \in H$ and $h_2s_1s_2^{-1}h_2^{-1} \in S$, by Eq 1. Also $S$ is a normal subgroup of $T$: for $h_1s_1 \in T$ and $s \in S$, $h_1s_1s(h_1s_1)^{-1} = h_1s_1ss_1^{-1}h_1^{-1} \in S$, by Eq 1. But $|S| = |H| = p^n$ and hence $H$ and $S$ are Sylow $p$-subgroups of $T$. This implies that they are conjugate in $T$ by 2nd Sylow theorem. But $S$ is normal in $T$ and hence $H = S$. Thus $|X^H| = 1$, hence $|X| = k \equiv 1(|p|)$, by Lemma 2. □

**Ex. 4.** Let $G$ be a finite group and $p$, the smallest prime such that $p$ divides the order of $G$. Then any subgroup of $G$ of index $p$ is normal.

**Ex. 5.** Prove that a group of the order 35 is cyclic.

**Ex. 6.** Prove that a group of the order 500 is not simple, that is, it has a non trivial normal subgroup.

**Ex. 7.** If $G$ is a group of the order $p^n$, then there exists a subgroup of order $p^i$, for $1 \le i \le n$ and subgroup of the order $p^i$ is normal normal in a subgroup of the order $p^{i+1}$.

**Ex. 8.** Prove that a group of the order $p^n$ is solvable.

**Ex. 9.** If $p$ and $q$ are primes such that $p$ does not divide $q - 1$, then a group of order $pq$ is isomorphic to $\mathbb{Z}_{pq}$.