Let $m$ and $n$ be positive integers such that $1 < m < n$. Lagrange's Theorem says that, if $G$ is a group of order $n$ and $H$ is a subgroup of $G$ of order $m$, then $m$ is a factor of $n$. As a corollary to the fundamental theorem of finite abelian groups it can be shown that, if $G$ is an abelian group of order $n$, and $m$ is a factor of $n$, then $G$ has a subgroup of order $m$.

The general question is this. Let $G$ be a group of order $n$ and let $m$ be a factor of $n$. When can we say that $G$ contains a subgroup of order $m$? We know that the answer to this question isn't, “Always:” $A_4$ is a group of order 12 and 6 is a factor of 12, but $A_4$ does not have a subgroup of order 6.

Much of the seminal work on this question was done by the Norwegian mathematician Ludwig Sylow (1832 – 1918). His results are collectively known as the “Sylow theorems.”

**Theorem 1 (Sylow's Existence Theorem):** Let $G$ be a finite group of order $n$. If, for some prime $p$ and some positive integer $k$, $p^k$ is a factor of $n$, then $G$ has a subgroup of order $p^k$.

**Proof:** If $G$ is abelian, then the result follows from the fundamental theorem of finite abelian groups.

In the nonabelian case, the proof is by induction on $n$. The result is satisfied vacuously when $n = 1$ or when $n$ is prime (in which case the only factors of $n$ are 1 and $n$), or when $n = 4$. Moreover, the only nonabelian group of order 6 is $D_3$, and it has both a subgroup of order 2 and a subgroup of order 3. Thus, let $n \geq 8$, and assume, for any $n'$, $1 \leq n' < n$, that if $G'$ is a (nonabelian) group of order $n'$ and if, for some prime $p$ and some positive integer $k'$, $p^{k'}$ is a factor of $n'$, then $G'$ has a subgroup of order $p^{k'}$.

Let $G$ be a nonabelian group of order $n$ and suppose that, for some prime $p$ and some $k \in \mathbb{Z}^+$, $p^k$ is a factor of $n$. To complete the proof, we must show that $G$ has a subgroup of order $p^k$. This is obvious if $n = p^k$, so assume that $p^k$ is a proper factor of $n$.

Consider the class equation

$$|G| = |C| + \sum |[x]|$$

where $C$ is the center of $G$. If, for some $x \in G - C$, $p^k$ is a factor of $|C_x|$, then we can apply the induction hypothesis with $G' = C_x$ and $k' = k$ to assert that $G'$ has a subgroup of order $p^{k'}$. Since any subgroup of $G'$ is also a subgroup of $G$, we are done in this case.
Thus, we may assume that, for all \( x \in G - \mathcal{C} \), \( p^k \) is not a factor of \( |\mathcal{C}_x| \). Consider such an \( x \), and consider the relation:

\[
|[x]| |\mathcal{C}_x| = |G|
\]

Since \( p^k \) is a factor of \( |G| \) but is not a factor of \( |\mathcal{C}_x| \), \( p \) must be a factor of \( |[x]| \) for every \( x \in G - \mathcal{C} \). It follows from the class equation that \( p \) is a factor of \( \mathcal{C} \).

Since \( \mathcal{C} \) is abelian, \( \mathcal{C} \) contains a cyclic subgroup of order \( p \), call it \( H \), and let \( h \) generate \( H \). Since \( H \leq \mathcal{C} \), we have that

\[
ghg^{-1} = h
\]

for any \( g \in G \) and any \( h \in H \). Thus, \( H \triangleleft G \).

Let \( G' = G/H \). Then \( p^{k-1} \) is a factor of \( |G'| \). Thus, we may apply the induction hypothesis to \( G' \), with \( k' = k - 1 \), to assert that \( G' \) has a subgroup \( H' \) of order \( p^{k-1} \), say

\[
H' = \{ H, Hx_2, \ldots, Hx_{p^{k-1}} \}
\]

We claim that

\[
K = H \cup Hx_2 \cup \cdots \cup Hx_{p^{k-1}}
\]

is a subgroup of \( G \) of order \( p^k \). It is clear that \( |K| = p^k \), since each right coset of \( H \) in \( G \) contains \( p \) elements, and distinct right cosets are disjoint.

**Exercise:** Show that \( K \) is a subgroup of \( G \).

This completes the proof.

---

**Definition 1:** Let \( G \) be a finite group and let \( p \) be a prime factor of \( |G| \). If \( k \in \mathbb{Z}^+ \) is such that \( p^k \) is a factor of \( |G| \) but \( p^{k+1} \) is not a factor of \( |G| \), then any subgroup of \( G \) of order \( p^k \) is called a \( p \)-**Sylow subgroup** of \( G \).

---

**Example 1:** Let \( G \) be a nonabelian group of order 12. Since \( 12 = 2^2 \cdot 3 \), we know by Theorem 1 that \( G \) contains a subgroup of order 4 and a subgroup of order 3. Any subgroup of \( G \) of order 4 is a 2-Sylow subgroup, whereas any subgroup of order 3 is a 3-Sylow subgroup.

Any 3-Sylow subgroup of \( G \) is cyclic. In the case of

\[
D_6 = \langle r, s \mid |r| = 6, |s| = 2, s \neq r^3, sr = r^5s \rangle
\]

there is a unique 3-Sylow subgroup — \( \{ e, r^2, r^4 \} \) — and this subgroup is a normal subgroup of \( D_6 \). Contrast this with the situation for

\[
A_4 = \langle a, b \mid |a| = 3, |b| = 2, aba = ba^2b \rangle
\]
Here, there are four Sylow 3-subgroups:

\[
\langle a \rangle = \{e, a, a^2\} \quad \langle ab \rangle = \{e, ab, ba^2\} \\
\langle ba \rangle = \{e, ba, a^2b\} \quad \langle aba \rangle = \{e, aba, a^2ba^2\}
\]

None of these is a normal subgroup; in fact, each one is conjugate to \( H = \langle a \rangle \), since

\[
\langle ab \rangle = a^2ba\langle a \rangle a^2ba, \quad \langle ba \rangle = aba^2\langle a \rangle aba^2, \quad \langle aba \rangle = b\langle a \rangle b
\]

A 2-Sylow subgroup is either cyclic or is isomorphic to the Klein four-group (that is, \( \mathbb{Z}_2 \times \mathbb{Z}_2 \)). Neither \( D_6 \) nor \( A_4 \) contains an element of order 4; hence, for these two groups, any 2-Sylow subgroup is isomorphic to the Klein four-group.

For \( D_6 \), there are three 2-Sylow subgroups, namely,

\[
\{e, r^3, s, r^3s\}, \quad \{e, r^3, rs, r^4s\}, \quad \{e, r^3, r^2s, r^5s\}
\]

None of these is a normal subgroup; in fact, each one is conjugate to \( K = \{e, r^3, s, r^3s\} \):

\[
\{e, r^3, rs, r^4s\} = r^5Kr \quad \text{and} \quad \{e, r^3, r^2s, r^5s\} = rKr^5
\]

On the other hand, for \( A_4 \), there is a unique 2-Sylow subgroup, namely,

\[
N = \{e, aba^2, a^2ba, b\}
\]

and this subgroup is a normal subgroup of \( A_4 \).

**Exercise:** Recall that there is a third nonabelian group of order 12, namely,

\[
T = \langle a, b \mid |a| = 6, |b| = 4, a^3 = b^2, ba = a^5b \rangle
\]

Show that \( T \) has:

(a) a unique 3-Sylow subgroup, which is a normal subgroup of \( T \);

(b) three distinct 2-Sylow subgroups, each isomorphic to \( \mathbb{Z}_4 \).

Applying Sylow's Existence Theorem with \( k = 1 \), we obtain the following corollary.

**Corollary 2 (Cauchy's Theorem):** Let \( G \) be a finite group and let \( p \) be a prime such that \( p \) is a factor of \( |G| \). Then \( G \) has an element of order \( p \).

In previous work, we alluded to the idea of conjugate subgroups. Formally, let \( G \) be a group and let \( H \) and \( K \) be subgroups of \( G \). We say that \( K \) is conjugate to \( H \) if

\[
K = gHg^{-1}
\]

for some element \( g \in G \). Just as “conjugacy” of elements is an equivalence relation on \( G \), conjugacy of subgroups is an equivalence relation on the set of subgroups of \( G \).
**Exercise:** For any group $G$, show that “conjugacy” is an equivalence relation on the set of subgroups of $G$.

To prove Sylow’s other theorems, we introduce the idea of a group $G$ acting on a set $S$. Let $G$ be a group, let $S$ be a set, and let $\pi$ be a homomorphism from $G$ to the group $S(S)$ of all permutations of $S$. That is, the function $\pi$ associates, with any given element $g \in G$, a permutation $\pi_g$ of $S$, and the function $\pi$ has the following property:

$$\pi_{hg}(s) = \pi_h(\pi_g(s))$$

for any two elements $g, h \in G$. Then we say that $G$ acts on $S$ through $\pi$, or, more simply, that $G$ acts on $S$. Note that, if $G$ acts on $S$ through $\pi$, then

$$\pi(G) = \{\pi_g \mid g \in G\}$$

is a subgroup of the group of all permutations of $S$.

Let $G$ act on $S$ (through $\pi$). Define the relation $\sim$ on $S$ by

$$s \sim t \iff \pi_g(s) = t \text{ for some } g \in G$$

**Exercise:** Show that $\sim$ is an equivalence relation on $S$.

**Definition 2:** For $s \in S$, the equivalence class containing $s$ under the equivalence relation $\sim$ is called the orbit of $s$ and is denoted by $O(s)$ or by $\text{orb}(s)$. Also, the stabilizer of $s$ is the subset of $G$ denoted by $\text{stab}(s)$ and defined by

$$\text{stab}(s) = \{g \mid \pi_g(s) = s\}$$

**Exercise:** Show that $\text{stab}(s)$ is a subgroup of $G$.

Technically, both the orbit of $s$ and the stabilizer of $s$ depend on the group $G$ and the function $\pi$, and so we might denote them by

$$O_{G,\pi}(s) \quad \text{and} \quad \text{stab}_{G,\pi}(s)$$

respectively. However, whenever we use these terms, the group $G$ and the function $\pi$ under consideration will always be clear, so we can use the simpler notation of the definition.

**Example 2:** Any group $G$ acts on itself through “conjugacy.” That is, let $G$ be a group, and define $\pi : G \to S(G)$ by $\pi(g) = \pi_g$, where
\[ \pi_g(x) = gxg^{-1} \]

Then \( \pi_g \) is a permutation of \( G \) — in fact, \( \pi_g \) is an automorphism of \( G \).

**Exercise:** Verify that \( \pi_g \) is an automorphism of \( G \). As a corollary, it follows that

conjugate subgroups of \( G \) are isomorphic.

For this “action,” and for a given element \( s \) of \( G \),

\[ \mathcal{O}(s) = \{ gsg^{-1} \mid g \in G \} = [s] \] is the conjugacy class of \( s \)

Also,

\[ \text{stab}(s) = \{ g \mid gsg^{-1} = s \} = \{ g \mid gs = sg \} = C_G(s) \]

that is, \( \text{stab}(s) \) is the centralizer of \( x \). Note that, by Theorem 7 in *Abelian Groups*, if \( G \) is finite, then

\[ |\mathcal{O}(s)| = [s] = |G : C_G(s)| = |G : \text{stab}(s)| \]

\[ \square \]

**Example 3:** Let \( G \) be a group and let \( S \) denote the set of subgroups of \( G \). Then \( G \) acts on \( S \) through conjugacy. That is, define \( \pi : G \rightarrow S(S) \) by \( \pi(g) = \pi_g \), where \( \pi_g : S \rightarrow S \) is defined by

\[ \pi_g(H) = gHg^{-1} \]

For a fixed subgroup \( H \) of \( G \), its orbit \( \mathcal{O}(H) \) consists of all of the subgroups conjugate to \( H \). Hence, \( \mathcal{O}(H) = \{ H \} \) if and only if \( H \) is a normal subgroup of \( G \). The stabilizer of \( H \) is

\[ \text{stab}(H) = \{ g \mid gHg^{-1} = H \} \]

In this case, \( \text{stab}(H) \) is called the *normalizer* of \( H \) in \( G \) and is denoted by \( N_G(H) \).

In the case when \( G \) is finite, define the function \( f \) from the collection of left cosets of \( N = N_G(H) \) to \( \mathcal{O}(H) \) by

\[ f(xN) = xHx^{-1} \]

Clearly, \( f \) is onto. Furthermore, for any \( x_1, x_2 \in G \),

\[ f(x_1N) = f(x_2N) \iff x_1Hx_1^{-1} = x_2Hx_2^{-1} \]

\[ \iff x_1^{-1}x_1Hx_1^{-1}x_2 = H \]

\[ \iff x_2^{-1}x_1 \in N \]

\[ \iff x_1N = x_2N \]
This shows that $f$ is both well-defined and one-to-one. Therefore,

$$|\mathcal{O}(H)| = |G : N| = |G : \text{stab}(H)|$$

In general, we have the following result.

**Theorem 3 (Orbit-Stabilizer Theorem):** Let $G$ be finite group and let $G$ act on a set $S$ through $\pi$. Then, for any $s \in S$,

$$|\mathcal{O}(s)| = |G : \text{stab}(s)|$$

**Exercise:** Prove the theorem. Hint: Fix $s \in S$ and let $N = \text{stab}(s)$. Define $f$ from the set of left cosets of $N$ in $G$ to $\mathcal{O}(s)$ by

$$f(xN) = \pi_x(s)$$

Show that $f$ is well-defined, one-to-one, and onto. It follows that

$$|\mathcal{O}(s)| = |\text{im}(f)| = |\text{dom}(f)| = |G : \text{stab}(s)|$$

**Corollary 4:** Let $p$ be a prime and let $G$ be a group with order a power of $p$. Let $G$ act on a finite set $S$ through $\pi$, and define the subset $T$ of $S$ by

$$T = \{s \in S \mid \mathcal{O}(s) = \{s\}\}$$

Then

$$|T| \equiv |S| \pmod{p}$$

(that is, $p$ is a factor of $|S| - |T|$).

**Proof:** Since the orbits partition $S$ and $S$ is finite, we can write

$$|S| = |T| + \sum_{s \notin S_0} |\mathcal{O}(s)|$$

$$= |T| + \sum_{s \notin S_0} |G : \text{stab}(s)|$$

by the orbit-stabilizer theorem

Note that each term $|G : \text{stab}(s)|$ in the sum on the right is a multiple of $p$, and hence so is the sum. It follows that $|S| - |T|$ is a multiple of $p$. 
Theorem 5 (Sylow's Conjugacy Theorem): Let $G$ be a finite group and let $p$ be a prime factor of the order of $G$. Then:

1. If $H$ is a subgroup of $G$ such that the order of $H$ is a power of $p$, and $K$ is a $p$-Sylow subgroup of $G$, then $gHg^{-1}$ is a subgroup of $K$ for some $g \in G$.

2. If $H$ and $K$ are both $p$-Sylow subgroups of $G$, then $H$ and $K$ are conjugate subgroups.

Proof: To prove (1), let $H$ be a subgroup of $G$ such that the order of $H$ is a power of $p$ and let $K$ be a $p$-Sylow subgroup of $G$. Let $S$ be the set of left cosets of $K$ in $G$, and let $H$ act on $S$ through $\pi$, with $\pi : H \to S(S)$ defined by $\pi(h) = \pi_h$, where

$$\pi_h(gK) = hgK$$

Then, by Corollary 4,

$$|T| \equiv |S| \pmod p \to |T| \equiv |G : K| \pmod p$$

Note that, since $K$ is a $p$-Sylow subgroup of $G$, $|G : K| = |G|/|K|$ is not a multiple of $p$. Thus, $|T|$ is not a multiple of $p$. In particular, $|T| > 0$.

Let $g' \in G$ be such that $g'K \in T$. Then $O(g'K) = \{g'K\}$. This means that, for every $h \in H$, $g'K = \pi_h(g'K) = hg'K$. It follows that, for every $h \in H$, $(g')^{-1}hg'K = K$, that is, $(g')^{-1}hg' \in K$. Letting $g = (g')^{-1}$, we have that $gHg^{-1}$ is a subgroup of $K$.

Part 2 now follows easily from part 1. For, if $H$ and $K$ are both $p$-Sylow subgroups of $G$, then, by part 1, $gHg^{-1} \leq K$ for some $g \in G$, and $|gHg^{-1}| = |H| = |K|$. Therefore, $gHg^{-1} = K$, showing that $H$ and $K$ are conjugate subgroups.

Corollary 6: Let $G$ be a finite group and let $p$ be a prime factor of the order of $G$. If $G$ has a unique $p$-Sylow subgroup $N$, then $N$ is a normal subgroup of $G$. Conversely, if $N$ is a $p$-Sylow subgroup of $G$ and $N \triangleleft G$, then $N$ is the unique $p$-Sylow subgroup of $G$.

Theorem 7 (Sylow's Counting Theorem): Let $G$ be a finite group, let $p$ be a prime factor of the order of $G$, and let $s_p$ denote the number of distinct $p$-Sylow subgroups of $G$. Then $s_p$ is a factor of $|G|$ and $s_p \bmod p = 1$.

Proof: Let $K$ be a $p$-Sylow subgroup of $G$. Then, by Theorem 5, part 2,

$$s_p = |G : N_G(K)|$$

showing that $s_p$ is a factor of $G$. Let $S$ be the set of $p$-Sylow subgroups of $G$, and let $K$ act on $S$ through conjugation (as in Example 3). Then, by Corollary 4,
Sylow Theorems

Clearly, $K \in T$, since $KK^{-1} = K$ for any $k \in K$. Suppose $K' \in T$. Then, for any $k \in K$, $kK'k^{-1} = K'$. It follows that $K \leq NG(K')$. Now then, $NG(K') \leq G$, and so both $K$ and $K'$ are $p$-Sylow subgroups of $NG(K')$. But, clearly, $K' \triangleleft NG(K')$. Thus, by Corollary 6, $K'$ is the unique $p$-Sylow subgroup of $NG(K')$. Hence, $K = K'$, and it follows that $|T| = 1$. This shows that $s_p \equiv 0 \pmod{p}$.

Next we present several applications of the Sylow theorems.

**Example 4:** Let $p$ and $q$ be distinct primes and let $G$ be a group of order $p^i q^j$ for some positive integers $i$ and $j$. Show that, if $G$ has a unique $p$-Sylow subgroup $N_1$ and a unique $q$-Sylow subgroup $N_2$, then $G$ is abelian.

**Solution:** Let $p$ and $q$ be distinct primes and let $G$ be a group of order $p^i q^j$ for some positive integers $i$ and $j$. Suppose $G$ has a unique $p$-Sylow subgroup $N_1$ and a unique $q$-Sylow subgroup $N_2$. Then, by Corollary 6, $N_1 \triangleleft G$ and $N_2 \triangleleft G$. Also, $G = N_1 N_2$ and $N_1 \cap N_2 = \{e\}$, where $e$ is the identity of $G$.

To show that $G$ is abelian, it suffices to show that any element $x_1 \in N_1$ commutes with any element $x_2 \in N_2$. Consider the element $x_1 x_2 x_1^{-1} x_2^{-1}$:

\[
    x_1 x_2 x_1^{-1} x_2^{-1} = (x_1 x_2 x_1^{-1}) x_2^{-1} \in N_2 \quad \text{since} \ N_2 \triangleleft G
\]

\[
    x_1 x_2 x_1^{-1} x_2^{-1} = x_1 (x_2 x_1^{-1} x_2^{-1}) \in N_1 \quad \text{since} \ N_1 \triangleleft G
\]

It follows that $x_1 x_2 x_1^{-1} x_2^{-1} = e$, or that $x_1 x_2 = x_2 x_1$. Therefore, $G$ is abelian.

**Example 5:** Let $q$ be an odd prime. Show that, up to isomorphism, there are two groups of order $2q$: $\mathbb{Z}_{2q}$ and $D_q$.

**Solution:** Let $G$ be a group of order $2q$, with $q$ an odd prime. If $G$ is abelian, then it follows from the fundamental theorem of finite abelian groups (FTFAG) that $G \cong \mathbb{Z}_{2q}$.

Suppose $G$ is nonabelian. Let $N$ be a $q$-Sylow subgroup of $G$. Since $|G : N| = 2$, $N$ is a normal subgroup of $G$. By Corollary 6, $N$ is the unique $q$-Sylow subgroup of $G$. It follows that every element in $G - N$ has order 2.

Note that $N$ is cyclic; say, $N = \langle r \rangle$. Let $s \in G - N$. Then $G = N \cup Ns$ and it follows that $r$ and $s$ generate $G$. The question is, What is $sr$?
Since $G$ is not abelian, $sr \neq rs$ and, since $|srs| = |r| = q$, $srs = r^t$ for some $t$, $2 \leq t \leq q - 1$. Now then,

$$r^{t^2} = (r^t)^t = (srs)^t = sr^t s = r$$

Therefore, $t^2 \mod q = 1$, that is, $q$ is a factor of $t^2 - 1$. Note that $t^2 - 1 = (t + 1)(t - 1)$, and $q$ is not a factor of $t - 1$. It follows that $q$ is a factor of $t + 1$. This implies that $t = q - 1$. Therefore,

$$G = \langle r, s \mid |r| = q, |s| = 2, sr = r^{q-1}s \rangle \cong D_q$$

Example 6: Show that the only group of order 15, up to isomorphism, is $\mathbb{Z}_{15}$. In other words, any group of order 15 is cyclic.

Solution: We apply Example 4. Let $G$ be a group of order 15, and let $s_3$ and $s_5$ denote the number of distinct 3-Sylow subgroups and 5-Sylow subgroups of $G$, respectively. By Sylow's counting theorem, we can say that

$$s_3 = 1 \quad \text{and} \quad s_5 = 1$$

Hence, $G$ has a unique 3-Sylow subgroup and a unique 5-Sylow subgroup. It follows from Example 4 that $G$ is abelian, and it follows from (FTFAG) that the only abelian group of order 15, up to isomorphism, is $\mathbb{Z}_{15}$.

Additional Exercise

Let $G$ be a group of order $3q$, with $q$ a prime, $q \geq 3$.

(a) If $q \mod 3 \neq 1$, show that $G \cong \mathbb{Z}_{3q}$.

(b) Otherwise (if $q \mod 3 = 1$), show that there are two groups of order $3q$, up to isomorphism, $\mathbb{Z}_{3q}$, and the nonabelian group $G$ having the presentation

$$G = \langle a, b \mid |a| = q, |b| = 3, ba = a^2b \rangle$$