The proofs of the Sylow Theorems depend on the equivalence relation on the elements of a group.

Definition. For a group $G$, two elements $a, b \in G$ are conjugate if there is $x \in G$ such that $b = x^{-1}ax$. You will recognize that the map $g \rightarrow x^{-1}gx$ for $g \in G$ is an inner automorphism of $G$.

Theorem 9.19. Conjugacy is an equivalence relation on $G$. We then speak of the conjugacy classes which are pairwise disjoint or identical, and whose union is $G$.

For $a$ an element of a finite group $G$, how big is the conjugacy class that contains $a$? We find the answer in a special subgroup of $G$.

Definition. For an element $a$ in a group $G$, the centralizer of $a$ is $C(a) = \{ g \in G : ga = ag \}$.

Theorem 9.20. If $G$ is a group and $a \in G$, then $C(a)$ is a subgroup of $G$.

Theorem 9.21. Let $G$ be a finite group and $a \in G$. Then the number of elements in the conjugacy class of $a$ is equal to the index $[G : C(a)]$ which divides $|G|$.

For a finite group $G$, if $C_1, C_2, \ldots, C_t$ are the distinct conjugacy classes of elements of $G$, then

$$G = C_1 \cup C_2 \cup \cdots \cup C_t.$$  

Since the distinct conjugacy classes are mutually disjoint, we have

$$|G| = |C_1| + |C_2| + \cdots + |C_t|.$$  

If we choose one element $a_i$ in each conjugacy class $C_i$, then by Theorem 9.21 we have $|C_i| = [G : C(a_i)]$, so that

$$|G| = [G : C(a_1)] + [G : C(a_2)] + \cdots + [G : C(a_t)].$$  

This is known as the class equation of the finite group $G$, and is the basic tool used in the proofs of the Sylow Theorems.

There is another version of the class equation we will use shortly that depends on $Z(G)$, the center of $G$.

Theorem. For a finite group $G$, if $C_1, C_2, \ldots, C_r$ are the conjugacy classes of $G$ for which $|C_i| \geq 2$, then

$$|G| = |Z(G)| + |C_1| + |C_2| + \cdots + |C_r|.$$
Proof. For elements $c$ and $x$ of $G$, we have $cx = xc$ if and only if $x^{-1}cx = c$.
Now $c \in Z(G)$ if and only if $cx = xc$ for all $x \in G$.
Thus $c \in Z(G)$ if and only if $c$ has exactly one conjugate, namely itself.
This implies that $Z(G)$ is the union of all of the one-element conjugacy classes of $G$. □

Theorem 9.27. If $G$ is a group of order $p^n$ for a positive prime $p$ and some $n \geq 1$, then $|Z(G)| = p^k \geq 2$.
Proof. Since $Z(G)$ is a subgroup of $G$, we have $|Z(G)| = p^k$ for some $0 \leq k \leq n$ by Lagrange’s Theorem.

From the class equation for $G$, we know that
$$|Z(G)| = |G| - |C_1| - |C_2| - \cdots - |C_r|,$$
where $|C_i| \geq 2$ and $|C_i|$ divides $|G|$ by Theorem 9.21.
Since $|G| = p^n$, each $|C_i|$ is divisible by $p$.
Since $|G|$ is also divisible by $p$, the class equation implies that $p$ divides $|Z(G)|$.
Therefore $|Z(G)| = p^k$ for some $1 \leq k \leq n$. □

Corollary 9.28. For a positive prime $p$ and an integer $n > 1$, there are no simple groups of order $p^n$.
Proof. Suppose $|G| = p^n$ for a positive prime $p$ and an integer $n > 1$.
The center $Z(G)$ is a normal subgroup of $G$.
If $Z(G) \neq G$, then $G$ is not simple.
So suppose $Z(G) = G$, so that $G$ is abelian.
If $G$ were simple, then by Theorem 8.25 the group $G$ would be isomorphic to $Z_q$ for some positive prime $q$, and hence $|G| = q$.

But $|G| = p^n$ for a positive prime $p$ and $n > 1$, a contradiction. □

Corollary 9.29. If $G$ has order $p^2$ for a positive prime $p$, then $G$ is abelian and $G$ is isomorphic to $Z_{p^2}$ or to $Z_P \oplus Z_P$.
Proof. With $|G| = p^2$ for a positive prime $p$, we have that $|Z(G)| = p$ or $p^2$ by Theorem 9.27.

If $|Z(G)| = p^2$, then $Z(G) = G$, and $G$ is abelian.
If $|Z(G)| = p$, then as $Z(G)$ is normal, the quotient group $G/Z(G)$ has order $p^2/p = p$.
This means that $G/Z(G)$ is cyclic, so by Theorem 8.13, the group $G$ is abelian.

With $G$ being abelian, the Fundamental Theorem of Finite Abelian Groups implies that $G$ is isomorphic to $Z_{p^2}$ or $Z_{p} \oplus Z_{p}$.

Example. By Corollary 9.29, a group of order $9 = 3^2$ is abelian and isomorphic to $Z_9$, or $Z_3 \oplus Z_3$. □
We can extend the result of the Corollary from groups of order \( pq \) to some groups of order \( p^2 q \).

**Theorem 9.30.** Let \( p \) and \( q \) be distinct positive primes such that \( q \nmid 1 \pmod{p} \), i.e., \( q \neq 1 + pt \), and \( p^2 \nmid 1 + qt \), i.e., \( p^2 \neq 1 + qt \). If \( G \) is a group of order \( p^2 q \), then \( G \) is abelian and isomorphic to \( \mathbb{Z}_{p^2 q} \) or \( \mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_q \).

**Example.** A group of order \( 1573 = 11^2 \cdot 13 \) has \( p = 11 \) and \( q = 11 \) which satisfy \( 13 \equiv 2 \pmod{11} \) and \( 11^2 = 121 \equiv 4 \pmod{13} \).

So any group of order 1573 is abelian and isomorphic to \( \mathbb{Z}_{1573} \) or \( \mathbb{Z}_{11} \oplus \mathbb{Z}_{11} \oplus \mathbb{Z}_{13} \).

The dihedral groups are a collection of finite nonabelian groups, and account for some of the nonabelian groups of finite order.

**Theorem 9.32.** The dihedral group \( D_n \) is a group of order \( 2n \) generated by a rotation \( r \) and a reflection \( d \) where \( |r| = n \), \( |d| = 2 \), and \( dr = r^{-1}d \).

**Theorem 9.33.** If a group \( G \) has order \( 2p \) for an odd positive prime \( p \), then \( G \) is isomorphic to the cyclic group \( \mathbb{Z}_{2p} \) or the dihedral group \( D_p \).

**Examples.** (a) By Theorem 9.32, a group of order \( 10 = 2 \cdot 5 \) is isomorphic to \( \mathbb{Z}_{10} \) or \( D_5 \).

(b) By Theorem 9.32, a group of order \( 14 = 2 \cdot 7 \), is isomorphic to \( \mathbb{Z}_{14} \) or \( D_7 \).

**Theorem 9.34.** If \( G \) is a group of order 8, then \( G \) is isomorphic to one of \( \mathbb{Z}_8 \), \( \mathbb{Z}_4 \oplus \mathbb{Z}_2 \), \( \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \), \( D_4 \), or the quaternion group \( Q \).

**Theorem 9.35.** If \( G \) is a group of order 12, then \( G \) is isomorphic to one of \( \mathbb{Z}_{12} \), \( \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \), \( A_4 \), \( D_6 \), or the group \( T \) generated by elements \( a, b \) that satisfy \( |a| = 6 \), \( b^2 = a^3 \), \( ba = a^{-1}b \).