Theorem (Sylow I)**.** *Let G be a finite group. Suppose that $p^m \mid |G|$ but $p^{m+1} \nmid |G|$ for some prime p. Then G has a subgroup of order p^m.*

The following combinatorial proof is due to Helmut Wielandt who published the result in the journal Archiv der Matematik, Vol 10 (1959), which proves a more general result and also constructs the desired p-subgroup.

First we prove a lemma:

Lemma. *Let $n = p^\alpha m$. It follows that $p^r \mid m$ but $p^{r+1} \nmid m$ if and only if $p^r \mid \binom{p^\alpha m}{p^\alpha}$ but $p^{r+1} \nmid \binom{p^\alpha m}{p^\alpha}$.*

Proof. Recall that $\binom{n}{k} = \frac{n!}{k!(n-k)!}$.

We have

$$\begin{aligned}\binom{p^\alpha m}{p^\alpha} = \frac{(p^\alpha m)!}{(p^\alpha)!(p^\alpha m - p^\alpha)!} &= \frac{(\cancel{p^\alpha} m)(p^\alpha m - 1)\cdots(p^\alpha m - k)\cdots(p^\alpha m - p^\alpha + 1)\cancel{(p^\alpha m - p^\alpha)!}}{(\cancel{p^\alpha})(p^\alpha - 1)\cdots(p^\alpha - k)\cdots(1)\cancel{(p^\alpha m - p^\alpha)!}} \\ &= m\left(\frac{(p^\alpha m - 1)\cdots(p^\alpha m - k)\cdots(p^\alpha m - (p^\alpha - 1))}{(p^\alpha - 1)\cdots(p^\alpha - k)\cdots(1)}\right).\end{aligned}$$

We wish to show that the largest power of p dividing $\binom{p^\alpha m}{p^\alpha}$ is p^r.

Let $1 \le k < p^\alpha$. First suppose that $p^s \mid p^\alpha - k$. It follows that $s < \alpha$. By the division algorithm, write $p^s q = p^\alpha - k$ for some integer q; equivalently, $p^\alpha = p^s q + k$. Observe that

$$\begin{aligned}p^\alpha m - k &= p^\alpha m - k - p^\alpha + p^\alpha \\ &= p^\alpha m - k - p^\alpha + (p^s q + k) \\ &= p^\alpha m - p^\alpha + p^s q = p^s(q + p^{\alpha - s}(m-1)),\end{aligned}$$

meaning that $p^s \mid p^\alpha m - k$ as well. We show conversely that if $p^s \mid p^\alpha m - k$ then $p^s \mid p^\alpha - k$. Suppose by way of contradiction that $s \ge \alpha$, so that $p^\alpha \mid p^s$, and by transitivity of divisibility, that $p^\alpha \mid p^\alpha m - k$. But $p^\alpha \mid p^\alpha m$, so that because p is prime it follows that $p^\alpha \mid k$ which is impossible since $1 \le k < p^\alpha$. Hence $s < \alpha$ in this case also. Again use the division algorithm to write $p^s q = p^\alpha m - k$; equivalently, $p^s q + k = p^\alpha m$. It follows that

$$\begin{aligned}p^\alpha - k &= p^\alpha - k - p^\alpha m + p^\alpha m \\ &= p^\alpha - k - p^\alpha m + (p^s q + k) \\ &= p^\alpha - p^\alpha m + p^s q = p^s(q - p^{\alpha - s}(m-1)),\end{aligned}$$

so that $p^s \mid p^\alpha - k$.

We conclude then that the any powers of p dividing a term $p^\alpha - k$ found in the denominator of

$$\frac{(p^\alpha m - 1)\cdots(p^\alpha m - k)\cdots(p^\alpha m - (p^\alpha - 1))}{(p^\alpha - 1)\cdots(p^\alpha - k)\cdots(1)} \quad \left(\text{equal to } \binom{p^\alpha m - 1}{p^\alpha - 1} \in \mathbb{Z}\right)$$

are the same as those dividing the corresponding term $p^\alpha m - k$ found in the numerator. Therefore all of the powers of p found in the fraction cancel out, meaning that powers of p divide $\binom{p^\alpha m}{p^\alpha}$ if and only if they divide m.

Let the largest power of p dividing m be p^r. It follows that $p^r \mid m$ but $p^{r+1} \nmid m$ if and only if $p^r \mid \binom{p^\alpha m}{p^\alpha}$ but $p^{r+1} \nmid \binom{p^\alpha m}{p^\alpha}$. $\square$

The next part of the proof involves proving a more general result:

Theorem. *If p is prime and $p^\alpha \mid |G| = p^\alpha m$ for a finite group G, then G has a subgroup of order p^α.*

Proof. We construct a desired subgroup H of order p^α.

Let $\mathcal{M} \subseteq \mathcal{P}(G)$ be the set of all subsets of G with p^α elements. Let $|G| = p^\alpha m$, so that $|M| = \binom{p^\alpha m}{p^\alpha}$. Define a relation $\sim$ on $\mathcal{M}$ by $M_1 \sim M_2$ if there exists a $g \in G$ such that $M_1 = M_2 g$. For $M_1, M_2, M_3 \in \mathcal{M}$, it follows from $M_1 = M_1 1_G$, $M_1 = M_2 g$ is equivalent to $M_2 = M_1 g^{-1}$, and $M_1 = M_2 g$ with $M_2 = M_3 h$ implies $M_1 = M_3 hg$, that $\sim$ is an equivalence relation on $\mathcal{M}$.

Let p^r be the largest power of p which divides m. We claim that there is an equivalence class $\overline{M}$ of elements in $\mathcal{M}/\sim$ such that p^{r+1} does not divide $\left|\overline{M}\right|$. To see this, suppose not; that is, that there are no equivalence classes $\overline{M}$ in $\mathcal{M}$ such that $p^{r+1} \nmid \left|\overline{M}\right|$. Equivalently said, $p^{r+1} \mid \left|\overline{M}\right|$ for every equivalence class $\overline{M}$ of $\mathcal{M}$. Since equivalence classes partition $\mathcal{M}$ (and $\mathcal{M}$ is finite because G is finite), it follows that $p^{r+1} \mid |\mathcal{M}| = \binom{p^\alpha m}{p^\alpha}$. From the previous lemma it follows that $p^{r+1} \mid m$, but this is a contradiction since r was chosen maximally with respect to p^r dividing m.

Let $\overline{M} = \{M_1, M_2, \ldots, M_n\}$ be an equivalence class in $\mathcal{M}$ such that $p^{r+1} \nmid \left|\overline{M}\right| = n \neq 0$. By definition of the relation $\sim$, it follows that for every $g \in G$ and each i, $1 \leq i \leq n$, that $M_i g = M_j$ for some j, $1 \leq j \leq n$. We construct the set $H = \{g \in G \mid M_1 g = M_1\}$, and observe that H is a subgroup of G: The identity $1_G \in H$, and for $a, b \in H$, meaning $M_1 a = M_1 b = M_1$, then $M_1 ab^{-1} = M_1$ so that $ab^{-1} \in H$.

We show first that $n|H| = |G|$. Observe that in the set of right cosets of H in G given by G/H, the equivalence

$$Ha = Hb \iff ab^{-1} \in H \iff M_1 ab^{-1} = M_1 \iff M_1 a = M_1 b$$

motivates a set map from $G/H \to \overline{M}$ where

$$Ha \mapsto M_1 a.$$

This map is a bijection: Suppose that $M_1 a = M_1 b$, which by the above equivalence gives that $Ha = Hb$, so that this map is injective. If $M_j \in \overline{M}$, then there exists $g \in G$ such that $M_j = M_1 g$, then observe that $Hg \mapsto M_1 g = M_j$ so that this map is surjective. Thus $|G/H| = |G|/|H| = \left|\overline{M}\right| = n$, so that $|G| = n|H|$ as desired.

Now we show that $|H| = p^\alpha$. By construction, $p^{r+1} \nmid n = \left|\overline{M}\right|$, and we saw that $n|H| = |G| = p^\alpha m$. With $p^r \mid m$, we have $p^{\alpha+r} \mid p^\alpha m = n|H|$. It follows from the maximality of p^r with respect to dividing m that $p^\alpha \mid |H|$, meaning $p^\alpha \geq |H|$.

For any $m_1 \in M_1$, we have that $m_1 h \in M_1$ for any $h \in H$ since $M_1 m_1 h = M_1 h = M_1$. Hence M_1 must have at least $|H|$ distinct elements, since the multiplication by m_1 is injective, viewed as a map from H to itself. If $h_1 \neq h_2$, then $m_1 h_1 \neq m_1 h_2$ by left cancellation in H. But M_1 is in $\mathcal{M}$, meaning $|M_1| = p^\alpha$. So $|H| \leq p^\alpha$, and combining it with the previous result we find that $|H| = p^\alpha$.

Hence the theorem is proved; furthermore, we have constructed the desired subgroup H. □

Sylow's first theorem comes as a special case of the previous theorem.

Theorem (Sylow I)**.** *Let G be a finite group. Suppose that $p^m \mid |G|$ but $p^{m+1} \nmid |G|$ for some prime p. Then G has a subgroup of order p^m.*

Proof. Take $\alpha = m$ to be maximal with respect to p^α dividing $|G|$ in the previous theorem. □