# 10 The Sylow Theorems and Applications

The textbook proof of Sylow's Theorems is the rather classic proof, using indcution and exploiting the class equation. Here we give an alternative proof, elementary and combinatoric in nature, due to Wielandt (Archive der Mathematik 10 (1959), 401–402). There are many other proofs of this result. For a finite group $G$, Sylow's Theorems guarantee the existence of subgroups of all prime-power orders dividing the order of $G$. This can be viewed as a kind of partial converse to Lagrange's Theorem. First recall a result from our homework, which guarantees the existence of subgroups of prime order for all primes dividing $|G|$:

**Theorem 10.1 Cauchy's Theorem** *Let $G$ be a finite group and $p$ a prime dividing the order of $G$. Then $G$ contains an element of order $p$.*

**Definition 10.2** *Let $G$ be a finite group, $p$ a prime, and write $|G| = p^a m$, $(p, m) = 1$. A $p$-subgroup of $G$ (i.e. a subgroup of order a power of $p$) of order $p^a$ is a* Sylow $p$-subgroup of $G$.

**Theorem 10.3 (Sylow)** *Let $G$ be a finite group, $p$ a prime, $|G| = p^a m$, $(p, m) = 1$. Then*

1. *every $p$-subgroup of $G$ is contained in a subgroup of order $p^a$ (and hence, since $\{1\}$ is a $p$-subgroup, Sylow $p$-subgroups exist);*

2. *if $n_p$ denotes the number of Sylow $p$-subgroups, then $n_p \equiv 1 \pmod{p}$ and $n_p$ divides $m$;*

3. *any two Sylow $p$-subgroups are conjugate in $G$ (and hence also isomorphic).*

*Proof.* First we show existence of Sylow $p$-subgroups. Let $\mathcal{S}$ denote the set of all subsets of $G$ with exactly $p^a$ elements, and let $G$ act on $\mathcal{S}$ by left multiplication. Notice $|\mathcal{S}| = (p^a m)!/[p^a!(p^a m - p^a)!]$. We claim that this is not divisible by $p$. We have

$$|\mathcal{S}| = \frac{p^a m(p^a m - 1)\cdots(p^a m - p^a + 1)}{1 \cdot 2 \cdots (p^a - 1)p^a} = m \prod_{i=1}^{p^a - 1} (\frac{p^a m - i}{i}).$$

Consider $\frac{p^a m - i}{i}, 1 \leq i < p^a$. If $p^j$ divides $i$ then $j < a$ and $p^j$ divides $p^a m - i$. If $p^j$ divides $(p^a m - i)$, then $j < a$ and $p^j$ divides $(p^a m - i)$. Therefore $p$ does not divide any of the factors $\frac{p^a m - i}{i}$ and so does not divide $|\mathcal{S}|$. This implies there is some orbit of $\mathcal{S}$ under the action of $G$ which has order not divisible by $p$. Call it $\mathcal{S}_1$. Let $X \in \mathcal{S}_1$ and consider $[G : G_X] = |\mathcal{S}_1|$. Then $p$ does not divide this index, so $p^a$ divides $|G_X|$. Now $X$ is a subset of $G$ with exactly $p^a$ elements. Choose $x \in X$. Then $|\{gx \mid g \in G_X\}| = |G_X|$. Since $G_X$ stabilizes $X$, we must have $gx \in X$ for all $g \in G_X$. Therefore $|G_X| \leq p^a = |X|$. Thus $|G_X| = p^a$, and we have found a Sylow $p$-subgroup.

Now let $\mathcal{P}$ denote the set of all conjugates of some Sylow $p$-subgroup $P$ in $G$. Then $P$ acts on $\mathcal{P}$ by conjugation. The number of elements in an orbit must be a power of $p$: $[P : P_x] = |\mathcal{O}_x|$. We claim that $P$ is the only element in $\mathcal{P}$ with a singleton orbit. If $\mathcal{O}_{P_1} = P_1$, then $P_1 \lhd \langle P, P_1 \rangle$, so $PP_1$ is a subgroup of order $|P||P_1|/|P \cap P_1| = p^a$, so $P = PP_1 = P_1$. Thus $|\mathcal{P}| \equiv 1 \pmod{p}$. Also $|\mathcal{P}| = [G : N_G(P)]$ and $m = [G : P] = [G : N_G(P)][N_G(P) : P]$, so $|\mathcal{P}|$ divides $m$. We will be done if we can show that any $p$-subgroup of $G$ is contained in some group in $\mathcal{P}$ (for then any Sylow $p$-subgroup will be conjugate to $P$, and every $p$-subgroup will be contained in a Sylow $p$-subgroup).

Let $P'$ be a $p$-subgroup of $G$. Suppose $P'$ is not contained in some conjugate of $P$. Let $P'$ act on $\mathcal{P}$ by conjugation. Then there can be no singleton orbits or, as before, $P'P_1$ would be a subgroup of order greater than $p^a$, a contradiction. That says all $P'$-orbits in $\mathcal{P}$ have order a power of $p$, and are not 1. That implies $|\mathcal{P}| \equiv 0 \pmod{p}$, a contradiction. Thus $P'$ is contained in some $P_1 \in \mathcal{P}$.

**Corollary 10.4** *$G$ contains subgroups of order $p^i$, $1 \leq i \leq a$, and any subgroup of order $p^i$ is a normal subgroup of some subgroup of order $p^{i+1}$, $1 \leq i \leq a - 1$.*

**Theorem 10.5** *1. If $N_G(P) \leq H \leq G$, then $N_G(H) = H$. In particular, $N_G(N_G(P)) = N_G(P)$.*

*2. If $N \lhd G$ then $P \cap N$ is a Sylow $p$-subgroup of $N$ and $PN/N$ is a Sylow $p$-subgroup of $G/N$.*

*Proof.* For (1), suppose $x \in N_G(H)$. Since $P \leq H \lhd N_G(H)$, we have $xPx^{-1} \leq H$. Then $P, xPx{-}1$ are Sylow $p$-subgroups of $H$, so there exists

$h \in H$ such that $xPx^{-1} = hPh^{-1}$, which implies $x^{-1}h \in N_G(P) \leq H$, and so $x \in H$.

For (2), observe that $[N : P \cap N] = [PN : P]$ is prime to $p$, and so since $P \cap N$ is a $p$-subgroup, it must be a Sylow subgroup. The other case is similar: $[G/N : PN/N] = [G : PN]$ is prime to $P$, and $|PN/N| = |P/(P \cap N)|$ is a prime power.

**Applications of Sylow's Theorems:** The bulk of these applications use the Sylow Theorems to show the existence of nontrivial proper normal subgroups, allowing one to show that a group of a given size is not simple. This can often be extended into an argument to show a group of a given size must be solvable, or to show that it must be a "semidirect product", which we will discuss in Chapter 5. These results often allow complete classification of all groups of a given order. Prelim problems in group theory often are along these lines.

1) The quaternion group $Q_8$ is not a subgroup of $S_5$: We know $D_8 \leq S_4 \leq S_5$, and $|D_8| = 8, |S_5| = 120 = 8 \cdot 15$. Therefore, since all Sylow 2-subgroups of $S_5$ must be isomorphic, any subgroup of order 8 must be isomorphic to $D_8$.

2) A group of order $p \cdot q^r, q \geq p, r \geq 1$ is never simple. If $q = p$, we have seen that the center is nontrivial, and since the group is not of prime order, it cannot be an abelian simple group. If $q \neq p$, then the Sylow $q$-subgroup is of index $p$, which is the smallest prime dividing the order of the group, so it is a nontrivial proper normal subgroup. Let Q be the Sylow $q$-subgroup, and let $P$ be a Sylow $p$-subgroup. Then by order considerations it is clear that $G = PQ$. When we study semidirect products, we will see that this group is a semidirect product. (Basically, this just means $Q \trianglelefteq G, G = PQ, P \cap Q = \{1\}$). Now suppose $Q$ is cyclic. Then $G$ must be abelian unless $p$ divides $q - 1$: necessarily we have a homomorphism $P \to \mathrm{Aut}(Q)$ (given by conjugation by elements of $P$) since $Q \trianglelefteq G$, and $|\mathrm{Aut}(Q)| = q^{r-1}(q-1)$. If $p$ does not divide $q^r(q-1)$, then the homomorphism is trivial, so $G$ is in fact cyclic of order $pq^r$. If $p$ divides $q-1$, then because $\mathrm{Aut}(Q)$ is cyclic, there is a unique subgroup of $\mathrm{Aut}(Q)$ of order $p$, and the map from $P$ to this subgroup gives rise to a unique (up to isomorphism) nonabelian group of order $pq^r$.

3) Example (2) is a special case of *Burnside's Theorem:* A noncyclic group of order $p^m q^n$ is never simple. The easiest proof of this result involves character theory and is beyond the scope of this course. You may NOT cite Burnside's Theorem for solving homework exercises!!

4) There are no simple groups of orders 12 or 28: For order 12, count the number of Sylow 3-subgroups. By the conditions, there are 1 or 4. If 1, it is normal, so assume there are 4. Then since these groups are of order 3 (prime), they are disjoint except for the identity, so there are $4 \cdot 2 = 8$ elements of order 3. Then there are only 4 elements left, and they must comprise the Sylow 2-subgroup, which is of order 4, and therefore it must be unique and hence normal. For order 28, the number of Sylow 7-subgroups must be a divisor of 4 and congruent to 1 (mod 7), and so must be 1, so the Sylow 7-subgroup is normal.

5) A group of order 28 with a normal subgroup of order 4 is abelian. For as above, the Sylow 7-subgroup $\mathrm{Syl}_7$ is normal. If also the Sylow 2-subgroup $\mathrm{Syl}_2$ is normal, then $G \cong \mathrm{Syl}_7 \times \mathrm{Syl}_2$ which is abelian.

6) There are no simple groups of orders 72 or 300. For $72 = 2^3 3^2$: $n_3 \equiv 1 \pmod 3$ and $n_3$ divides 8, so $n_3 = 1$ or 4. If $n_3 = 1$, then the Sylow 3-subgroup is normal. If $n_3 = 4$, then $n_3 = [G : N_G(P)]$, so $G$ has a subgroup of index 4, and this induces a homomorphism from $G$ onto a transitive subgroup of $S_4$, a group of order 24. Thus the kernel of this homomorphism is a nontrivial proper normal subgroup. For $300 = 5^2 2^2 3$, we have $n_5 = 1$ or 6. If 1, we are done. If $n_5 = 6$, then as above we have a homomorphism from $G$ to a transitive subgroup of $S_6$. Since $|S_6| = 720$ and 300 does not divide 720, this cannot be an injective homomorphism, and the kernel will give the necessary normal subgroup.

7) A group of order 12 with no element of order 2 in its center is isomorphic to $A_4$. First we show that $n_3 = 4$. If $n_3 = 1$, then let $\langle x \rangle$ be the Sylow 3-subgroup, and observe $x$ has at most two conjugates, $x$ and $x^2$. Thus $[G : C_G(x)] \leq 2$, so $|C_G(x)| = 6$ or 12, and thus it contains an element of order 2, say $y$. Let $Q$ be a Sylow 2-subgroup containing $y$. It is of order 4, therefore abelian. Therefore $y$ lies in the center of $\langle Q, x \rangle = G$, contradicting our assumption. Thus $n_3 = 4$. Then there are 8 elements of order 3, as in example (4) above, and the Sylow 2-subgroup is normal. Left multiplication by $G$ on a Sylow 3-subgroup gives a map $G \to S_4$, which is injective since the Sylow 3-subgroup is not normal and is of prime order (and the kernel is the largest normal subgroup in the Sylow 3-subgroup). Therefore $G$ is isomorphic to a subgroup of $S_4$ of order 12, and there is only one.

8) There are no simple groups of order $120 = 2^3 \cdot 3 \cdot 5$. If it were simple, $n_5 = 6$, and since $G$ can have no nontrivial proper subgroups, the map $G \to S_6$ must be injective. Then $G \cap A_6$ is normal in $G$ since $A_6 \lhd S_6$. Because $G$ is simple, we have $G \cap A_6 = \{1\}$ or $G$. It can't be 1 (why? –

think about any subgroup of $S_n$ intersected with $A_n$). Then $[A_6 : G] = 3$, so $A_6$ has a subgroup of index 3. This gives rise to a nontrivial homomorphism $A_6 \to S_3$, which means $A_6$ has a nontrivial proper normal subgroup. This is a contradiction, since $A_6$ is simple.

9) If $|G| = 60$, then if $n_5 > 1$, $G$ is simple. If $G$ is simple, then $n_2 = 5, n_3 = 10, n_5 = 6$, and $G \cong A_5$. These results are proved in the text at the end of §4.5.

10) If $|G| = pqr$, $p \leq q \leq r$ primes, then $G$ is not simple. We have already seen this in the case that $p, q, r$ are not distinct primes, except when $|G| = p^2q, p < q$. Let $Q$ be a Sylow $q$-subgroup. If $Q$ is not normal, then $n_q = p^2$, since we cannot have $p \equiv 1 \pmod{q}$, because $p < q$. Each Sylow $q$-subgroup contains $q-1$ elements of order q, and they must be disjoint except for the identity. This gives $p^2q - p^2$ elements of order $q$, so the remaining $p^2$ elements must comprise the Sylow $p$-subgroup, which must be unique and hence normal.

Now suppose $p < q < r$. Then $n_r = pq$ or 1, since $n_r \equiv 1 \pmod{r}$. If $n_r = pq$, there are $pq(r-1) = pqr - pq$ distinct elements of order $r$. Now if $n_q > 1$, then $n_q > p$, giving more than $p(q-1) = pq - p$ elements of order $q$, which leaves less than $p$ elements in the group, which is impossible, since there must be at least $p-1$ elements of order $p$ and the identity. Thus $n_q = 1$ and $G$ is not simple.

11) If $|G| = 8p^n$, $p$ an odd prime, then $G$ is solvable. We have $n_p \equiv 1 \pmod{p}$ and $n_p$ divides 8, so either the Sylow $p$-subgroup $P$ is normal in $G$ or $n_p = 4, p = 3$, or $n_p = 8, p = 7$. If $P$ is normal in $G$, then since $P$ is solvable (it is a $p$-group) and $G/P$ has order 8, hence solvable, we know $G$ is solvable.

If $n_p = 4, p = 3$, then we have a map from $G$ to a transitive subgroup of $S_4$; let $K$ be the kernel. Then since 4 divides $|G/K|$, we have $|G/K| = 4, 8, 12, 24$ and $|K| = 2 \cdot 3^n, 3^n, 2 \cdot 3^{n-1}, 3^{n-1}$. $G/K$ is solvable as all subgroups of $S_4$ are, and $K$ is solvable as, in each possible case, the Sylow 3-subgroup of $K$ is normal in $K$.

If $n_p = 8, p = 7$, then induct on $n$. If $n = 1$, then $|G| = 56$. By counting elements, there are $8 \cdot 6 = 48$ elements of order 7, leaving 8 elements for the Sylow 2-subgroup, which must then be unique and hence normal. In general, we have a map $G \to S_8$, where $G$ maps onto a transitive subgroup of $S_8$ of order dividing $|G| = 8 \cdot 7^n$. Thus the order of the image divides 56, and cannot be $1, 2, 4, 7$ as these do not correspond to transitive subgroups of $S_8$. Thus the image is of order $8, 14, 28, 56$, all of which imply the image is

solvable, and the kernel is of order $7^n, 4 \cdot 7^{n-1}, 2 \cdot 7^{n-1}, 7^{n-1}$. All of these are solvable (for the middle two, the Sylow 7-subgroup is normal). Thus $G$ is solvable.