

Introduction

This short note proves the Sylow theorems via a fundamental counting lemma about fixed points of finite p -group actions on sets. Nothing new is here, but we do show a slight extension on the Sylow Count theorem for arbitrary p -subgroups of a finite group G , which is not usually covered in these oft-presented theorems.

LEMMA 1 (Fundamental Lemma): *If a finite p -group P acts on a set X with fixed points X^P , then*

$$|X| \equiv |X^P| \pmod{p} \quad (1)$$

Proof. The orbit-stabilizer theorem shows any orbit of size larger than 1 is the index of a proper subgroup of P , hence has size 0 (mod p). Since $|X|$ is the sum of orbit sizes, we are done. $\square$

Sylow Subgroups

Recall that a Sylow p -subgroup of G is a p -subgroup of G such that p does not divide $[G : P]$. We start by focusing on p -elements.

THEOREM 2 (Cauchy): *If $|G|$ is divisible by p , then G has an element of order p .*

Proof. Consider the subset $X \subset G^p$ given by $X = \{(g_1, \dots, g_p) \mid g_1 \cdots g_p = 1\}$. Let the group $R = \langle (1, 2, \dots, p) \rangle \subset S_p$ act on X via rotation. Since p divides $|R|$ and $|X| = |G|^{p-1}$, [Lemma 1](#) shows $|X^P| \equiv 0 \pmod{p}$. But $X^P = \{(g, \dots, g) \mid g^p = 1\}$, which contains $(1, \dots, 1)$. Thus there is another element $g \in G$ with $g^p = 1$. $\square$

Now we show that, using Cauchy's theorem as a base case, we can iteratively build larger p -subgroups of G .

PROPOSITION 3: *If $H \leq G$ is a p -subgroup of G , and $[G : H]$ is divisible by p , then $[N_G(H) : H]$ is divisible by p .*

Proof. Consider the action of H on the right cosets of H in G . Note that a coset Hg is fixed by this action precisely when $H \subset H^g$; that is, when $g \in N_G(H)$. By [Lemma 1](#), we have

$$[N_G(H) : H] \equiv [G : H] \equiv 0 \pmod{p}$$

$\square$

COROLLARY 4 (Sylow Development): *If $P \leq G$ is a p -subgroup of G and p divides $[G : P]$, then there exists a subgroup $P \leq Q \leq N_G(P)$ with $[Q : P] = p$.*

Proof. By [Proposition 3](#), $N_G(P)/P$ has order divisible by p , and then by [Theorem 2](#) there is a subgroup $\bar{Q} \leq N_G(P)/P$ of order p . But this corresponds to a subgroup $P \leq Q \leq N_G(P)$ with $[Q : P] = p$. $\square$

COROLLARY 5 (Sylow Existence): *If p^m divides $|G|$, then G has a subgroup of order p^m .*

Proof. Cauchy's theorem gives a subgroup P of order p . Iteratively using [Corollary 4](#), we can create a subgroup of order p^m from one of order p^{m-1} as long as p^m divides $|G|$. $\square$

We turn next to counting all the Sylow subgroups of G .

PROPOSITION 6: *If $P \leq G$ is a Sylow p -subgroup of G , and p^m divides $|G|$, then the number of subgroups of order p^m in G is congruent (mod p) to the number of subgroups of order p^m in P .*

Proof. Let P act on the set $X = \{H \leq G \mid |H| = p^m\}$ via conjugation. Note that if $H \in X^P$, then P normalizes H , and so $PH = HP$ is a p -subgroup of G . But $P \leq PH$ and $[G : P]$ (hence $[PH : P]$) is coprime to p , so it must be that $PH = P$; that is, $H \triangleleft P$. Obviously, every normal subgroup of P of order p^m is in X^P , and so we see that

$$X^P = \{H \triangleleft P \mid |H| = p^m\}$$

Now let P act via conjugation on $Y = \{H \leq P \mid |H| = p^m\}$. We see that $X^P = Y^P$, and thus by [Lemma 1](#) we have

$$|X| \equiv |X^P| = |Y^P| \equiv |Y| \pmod{p}$$

$\square$

COROLLARY 7: *The number n_p of Sylow p -subgroups of G is such that $n_p \equiv 1 \pmod{p}$.*

Sylow Conjugacy

The main idea of the argument in [Proposition 6](#) is useful enough to extract out:

LEMMA 8: *If P is a Sylow p -subgroup of G and $H \leq G$ is a p -subgroup such that $HP = PH$, then $H \leq P$.*

For a subgroup $Q \leq G$, let Q_G be the set of conjugates of Q in G . Note that the orbit-stabilizer theorem shows $|Q_G| = [G : N_G(Q)]$.

THEOREM 9 (Sylow Conjugacy): *The Sylow p -subgroups of G are all conjugate.*

Proof. Let P, Q be two Sylow subgroups of G (not necessarily distinct). Let P act on Q_G via conjugation. Then by [Lemma 8](#), Q_G^P are those conjugates $Q^g \leq P$. However, since $|Q^g| = |P|$, there can be at most one fixed point (P). Because $|Q_G| = [G : N_G(Q)] \not\equiv 0 \pmod{p}$ (because Q is Sylow), [Lemma 1](#) shows $|Q_G^P| \not\equiv 0 \pmod{p}$, and thus $Q_G^P = \{P\}$. This means $P \in Q_G$, so that P and Q are conjugate. $\square$

Combining [Theorem 9](#) and [Corollary 7](#), we have

COROLLARY 10 (Sylow Count): $n_p = [G : N_G(P)] \equiv 1 \pmod{p}$. In particular, n_p divides $|G|/|P|$.

In the proof of [Theorem 9](#), we noted that the only possible fixed point of P acting on Q_G is P itself. What about the other orbits? If $n_p = 1$, there are no other orbits to speak of (and thus P is normal). In the case $n_p > 1$, pick a Sylow p -subgroup Q such that $|P \cap Q|$ is maximized.

THEOREM 11: Choose a Q as described above for P . Then $n_p \equiv 1 \pmod{[P : P \cap Q]}$.

This is of course a strengthening of [Corollary 7](#).

Proof. We again look at the conjugation action of P on Q_G , noting the only fixed point is P . For another $Q^g \in Q_G$, the orbit-stabilizer theorem shows the orbit has size $[P : N_P(Q^g)]$. Now $N_P(Q^g)$ is a p -subgroup of $N_G(Q^g)$, and thus [Lemma 8](#) implies $N_P(Q^g) \leq Q^g$. Thus

$$|N_P(Q^g)| \leq |P \cap Q^g| \leq |P \cap Q|$$

where the last inequality follows from our choice of Q . Since all of these are p -groups, we then have $|N_P(Q^g)|$ actually divides $|P \cap Q|$, so that $[P : P \cap Q]$ divides $[P : N_P(Q^g)]$. In other words, the orbit of Q^g has size divisible by $[P : P \cap Q]$. Since Q_G is the set of Sylow p -subgroups of G , and all orbits except $\{P\}$ have size divisible by $[P : P \cap Q]$, the theorem follows. $\square$

Sylow Count

It's possible to prove a generalization of [Corollary 7](#) directly from [Proposition 6](#), without the results of the previous section.

THEOREM 12: The number of subgroups of order p^m in G , when p^m divides $|G|$, is $1 \pmod{p}$.

To prove this, we need to establish some results on finite p -groups. We will use the following notation: for a group G , $n_G(k)$ is the number of subgroups of G of order p^k . First, if we examine the proof of Cauchy's theorem ([Theorem 2](#)), we see that when p divides $|G|$, the number of elements of order dividing p is actually $0 \pmod{p}$. So if we remove the identity, there are $-1 \pmod{p}$ elements of order p in G , and we need $(p-1) \equiv -1 \pmod{p}$ of them (plus the identity) to form a subgroup of order p . And of course, all non-identity elements of a subgroup of order p are counted in Cauchy's theorem. Because distinct subgroups of order p must intersect only in 1, this establishes the following lemma.

LEMMA 13: *In a finite group G with order divisible by p , $n_G(1) \equiv 1 \pmod{p}$.*

Consider now any proper subgroup $H < P$, for P a finite p -group. From [Proposition 3](#), we see that $H < N_P(H)$ is proper as well. Together with [Corollary 4](#), we have

LEMMA 14: *Every maximal subgroup $M < P$ has index p and is normal.*

We'd like to count the number of maximal subgroups in P . Unfortunately, the usual conjugation action tells us nothing, because they're all normal. So instead we work in a suitable quotient of P with large automorphism group. Let $M_1, \dots, M_n$ be the maximal subgroups of P . For each, P/M_i is a group of order p : a one-dimensional vector space over $\mathbb{F}_p$. Thus if $\Phi(P) = \bigcap M_i$, $V = P/\Phi(P)$ embeds in an n -dimensional vector space over $\mathbb{F}_p$, and hence is such a vector space itself (just not necessarily of dimension n). Also, maximal subgroups of V correspond with maximal subgroups of P . So it will be enough to count them in V .

Assume V has dimension d . We define the set

$$X_V = \{(v_1, \dots, v_{d-1}) \in V^{d-1} \mid \dim(\langle v_1, \dots, v_{d-1} \rangle) = d-1\}$$

of linearly independent lists from V of length $d-1$. If $\mathcal{M} = \{M \leq V \mid \dim(M) = d-1\}$ is the set of maximal subgroups (subspaces), there is a surjective map $f : X_V \rightarrow \mathcal{M}$ given by

$$(v_1, \dots, v_{d-1}) \mapsto \langle v_1, \dots, v_{d-1} \rangle$$

For a fixed $M \in \mathcal{M}$, note that $f^{-1}(M) = X_M$, the set of bases of M . Since $|X_M|$ only depends on $\dim(M)$, we see that $|f^{-1}(M)| = |f^{-1}(N)|$ for all $M, N \in \mathcal{M}$, and hence

$$|\mathcal{M}| = \frac{|X_V|}{|X_M|} = \frac{\prod_{i=0}^{d-2} (p^d - p^i)}{\prod_{i=0}^{d-2} (p^{d-1} - p^i)} = \frac{p^d - 1}{p - 1}$$

Going back to our original P , we've shown

LEMMA 15: If $|P/\Phi(P)| = p^d$, then the number of maximal subgroups of P is $\frac{p^d-1}{p-1} \equiv 1 \pmod{p}$.

Proof of Theorem 12. By Proposition 6, we can assume G is a p -group. We prove by induction on m that if p^m divides $|G|$, then $n_G(m) \equiv 1 \pmod{p}$. The base case is Lemma 13. So let $P_1, \dots, P_s$ be the subgroups of order p^m in G , and $Q_1, \dots, Q_t$ those of order p^{m+1} , assuming by induction that $s \equiv 1 \pmod{p}$. Construct an $s \times t$ matrix A where

$$a_{ij} = \begin{cases} 1 & P_i \leq Q_j \\ 0 & \text{otherwise} \end{cases}$$

For a fixed j , the sum $\sum a_{ij}$ is the number of maximal subgroups of Q_j , which is $1 \pmod{p}$ by Lemma 15. For a fixed i , the sum $\sum a_{ij}$ is the number of subgroups that contain P_i as a maximal subgroup. Since all of these are then in $N_G(P_i)$ by Lemma 14, this is the same as counting subgroups of order p in $N_G(P_i)/P_i$, and that is also $1 \pmod{p}$ by Lemma 13. Hence

$$t \equiv \sum_j \sum_i a_{ij} = \sum_i \sum_j a_{ij} \equiv s \equiv 1 \pmod{p}$$

□