

The Sylow Theorems
 Anna Marie Bohmann
 Massachusetts Institute of Technology

This paper gives a proof of the Sylow theorems using the concept of a group acting on a set. It is the tangible outcome of an eight week program at the University of Minnesota under the direction of Professor Paul Garrett. During this course I studied basic group theory, and the following is meant to illustrate both that knowledge, and my newly acquired practical knowledge of \TeX .

The Sylow theorems were originally published in 1872 by the Norwegian mathematician Peter Ludvig Mejdell Sylow (1832–1918). These theorems give information about the subgroups of finite groups, and in a sense provide a partial converse to Lagrange’s theorem.

The action of a group G on a set X is a map $G \times X \rightarrow X$ given by $(g, x) \rightarrow g \cdot x$ for $g \in G, x \in X$, with the following properties:

- i. $e \cdot x = x, \forall x \in X$
- ii. $(g_1 g_2) \cdot x = g_1(g_2 \cdot x), \forall x \in X$

The orbit O_x of a point x in X is defined by

$$O_x = \{y \in X : g \cdot x = y, \text{ for some } g \in G\}$$

and the stabilizer G_x by

$$G_x = \{g \in G : g \cdot x = x\}$$

For each x, G_x is a subgroup of G :

Given $x \in X, e \in G_x$ since $e \cdot x = x$, by the definition of group action; if $g \in G, x = e \cdot x = (g^{-1}g) \cdot x = g^{-1}(g \cdot x) = g^{-1} \cdot x$

First, some general results about group actions:

Theorem 1. *Let G be a finite group and X a set acted on by G . If $x \in X$, then $|O_x| = [G : G_x]$, meaning the order of the orbit of a point is equal to the index of its stabilizer in the group.*

Proof: Define a bijection $\phi : O_x \rightarrow G/G_x$. Let $y \in O_x$, so $y = g \cdot x$ for some $g \in G$. Then $\phi(y) = gG_x$. We must show this is well defined, meaning $\phi(y)$ is unique for each y . If $\exists h \in G$ such that $y = h \cdot x$ in addition to $y = g \cdot x$, $g \cdot x = h \cdot x$, or $x = g^{-1}h \cdot x$, so $g^{-1}h \in G_x$ and thus $h \in gG_x$ or $hG_x = gG_x$.

To prove the mapping is one-to-one: Assume $\phi(y_1) = \phi(y_2)$. Then $\exists g_1, g_2$ such that $y_1 = g_1 \cdot x$ and $y_2 = g_2 \cdot x$, and also $g_1G_x = g_2G_x$, so there exists $g \in G_x$ such that $g_2 = g_1g$. Then $y_2 = g_2 \cdot x = g_1g \cdot x = g_1 \cdot x = y_1$, and the map is one-to-one.

To prove the mapping is onto, it suffices to note that given a left coset gG_x , if $g \cdot x = y, \phi(y) = gG_x$. Since there is a bijection between O_x and G/G_x , their orders must be equal.

Define an equivalence relation on X : $x \sim y$ if and only if $y = g \cdot x$ for some $g \in G$. Now verify this is an equivalence relation:

- i. $x \sim x$ since $x = e \cdot x, \forall x \in X$
- ii. $x \sim y \Leftrightarrow y \sim x$ since $y = g \cdot x \Leftrightarrow g^{-1} \cdot y = x$
- iii. $x \sim y$ and $y \sim z \Rightarrow x \sim z$, since $y = g \cdot x$ and $z = h \cdot y \Rightarrow z = hg \cdot x$

Since this is an equivalence relation, it partitions the set X :

If $x, y \in X$ and $O_x \cap O_y \neq \emptyset$, then $O_x = O_y$. Suppose $z \in O_x \cap O_y$. Then $z \sim x$ and $z \sim y$. Thus $x \sim y$ and $y \sim x$. $x \sim y \Rightarrow O_y \subset O_x$ and $y \sim x \Rightarrow O_x \subset O_y$, so $O_x = O_y$.

Therefore, if X is finite,

$$|X| = \sum_{i=1}^n |O_{x_i}| \tag{1}$$

where each x_i is contained in a distinct orbit.

Now consider the action of G on itself by *conjugation*: $(g, x) \rightarrow gxg^{-1}$. The *center* of G is

$$Z_G = \{x : xg = gx, \forall g \in G\}$$

which is the set of all fixed points under conjugation.

Z_G is the union of all trivial orbits (i.e. those with order 1), since for every $x \in X, O_x \ni x$, so $|O_x| = 1$ implies $gxg^{-1} = x, \forall g \in G$. Thus, equation 1 becomes

$$|G| = |Z_G| + \sum_{i=1}^k |O_{x_i}|$$

where each x_i is in a distinct nontrivial orbit. Now by Theorem 1, this becomes the *class equation*:

$$|G| = |Z_G| + \sum_{i=1}^k [G : G_{x_i}]$$

The next theorem provides information on the elements of an abelian group.

Cauchy's Theorem. *Let G be a finite abelian group and p a prime that divides $|G|$. Then G has an element of order p .*

Proof (by induction on order of G).

If $|G| = 1$, the theorem is obviously true. Let $|G| = n$, and assume the theorem holds for all groups with orders less than n . G must have elements of prime order, since if $|x| = qm$, where q is prime, $|x^m| = q$.

Let $x \in G$ have order q . Assume $q \neq p$, and construct $\langle x \rangle$. Since every subgroup of an abelian group is normal, $G/\langle x \rangle$ is also an abelian group. The order of this group is n/q , which is divisible by p , and so by the induction hypothesis, $G/\langle x \rangle$ contains an element $y\langle x \rangle$ of order p . Thus $(y\langle x \rangle)^p = \langle x \rangle$, meaning $y^p \in \langle x \rangle$, so either $y^p = e$ or $|y^p| = q$, in which case $|y^q| = p$, since $y^{p^q} = y^{q^p} = e$.

Cauchy's theorem is actually true for any finite group, not just abelian ones, but this generalization can be regarded as a special case of the first Sylow theorem, and the proof in the general case is so similar to the proof of the latter theorem that it seems excessive to prove them both.

Sylow Theorem 1. *Let G be a finite group and p a prime so that p^r divides $|G|$. Then G contains a subgroup of order p^r .*

Proof (by induction on order of G).

If $|G| = 1$, the theorem is obvious. Suppose $|G| = n$, and the theorem holds for all groups with order less than n . Apply the class equation:

$$|G| = |Z_G| + \sum_{i=1}^k [G : G_{x_i}]$$

There are two cases:

Case 1: Suppose p does not divide $[G : G_{x_i}]$ for some i . Then, by Lagrange's Theorem, $|G| = |G_{x_i}|[G : G_{x_i}]$. Since p^r divides $|G|$, p^r divides $|G_{x_i}|$, and (using the fact that $[G : G_{x_i}]$ is nontrivial), we apply the induction hypothesis to G_{x_i} .

Case 2: Suppose p divides $[G : G_{x_i}]$ for all i . Since $p^r \mid |G|$, by the class equation, $p \mid |Z_G|$. Thus Z_G contains an element g of order p , by Cauchy's Theorem. Consider $\langle g \rangle$, the group generated by g , and the factor group $G/\langle g \rangle$, whose order is n/p , which is divisible by p^{r-1} . Thus, by the induction hypothesis, $G/\langle g \rangle$ contains a subgroup \bar{H} of order p^{r-1} . By the homomorphism $\phi : G \rightarrow G/N$, this has the form $H/\langle g \rangle$ for some $H \in G$, and so $|\bar{H}| = p^{r-1} = |H|/p$, implying $|H| = p^r$.

To prove the second and third Sylow theorems, we have to define a specific type of subgroup and a new group action.

Definition: Let G be a finite group, p a prime and p^r the highest power of p dividing the order of G . Any subgroup of G of order p^r is a *Sylow p -subgroup* of G .

Define a new group action of a subgroup $H \in G$ on the set \mathcal{H} of subgroups of G : if $h \in H$, and P is a subgroup, $(h, P) \rightarrow hPh^{-1}$.

Then the orbit of P is

$$O_P = \{K \in \mathcal{H} : hPh^{-1} = K, \text{ for some } h \in H\}$$

which is the set of all subgroups conjugate to P in G .

The stabilizer of P in H is

$$H_P = \{h \in H : hPh^{-1} = P\}$$

which is $N(P) \cap H$, where $N(P) = \{g \in G : gPg^{-1} = P\}$ is the normalizer of P in G . Thus, for this action, theorem 1 gives $|O_P| = [H : N(P) \cap H]$

Lemma. Let P be a Sylow p -subgroup of a finite group G and let x have as its order a power of p . If $x^{-1}Px = P$, then $x \in P$.

Proof. $x \in N(P)$, and the cyclic subgroup $\langle xP \rangle \subset N(P)/P$ has a power of p as its order. There exists $H \subset N(P)$ such that $H/P = \langle xP \rangle$. $|H| = |P||\langle xP \rangle|$, so $|H|$ is also a power of p . But P is a Sylow p -subgroup contained in H , and their order of P is the largest power of p dividing $|G|$, so $H = P$. Thus, H/P is the trivial subgroup, so $xP = P$, and $x \in P$.

Now the two remaining Sylow Theorems.

Sylow Theorem 2. Let G be a finite group and p a prime dividing $|G|$. Then all Sylow p -subgroups of G are conjugate.

Proof. Let P be a Sylow p -subgroup and suppose $|G| = p^r m$, and $|P| = p^r$. Let

$$O_P = \{P = P_1, P_2, \dots, P_k\}$$

be the set of conjugates of P in G . From above, $k = [G : N(P)]$. Now,

$$|G| = |N(P)||[G : N(P)] = |N(P)|k$$

and since $p^r \mid |N(P)|$, p does not divide k .

Given Q , another Sylow p -subgroup of G , we must show that $Q \in O_P$. Consider the above action of Q on each P_i . These form a partition of O_P , and the size of the partition of each P_i is $[Q : N(P_i) \cap Q]$. By Lagrange's Theorem, this must divide $|Q| = p^r$. Thus the number of equivalence classes of each P_i must be a power of p . But $p \nmid k$, so one P_i , say P_j , must contain only one equivalence class. In other words, $xP_jx^{-1} = P_j$ for all $x \in Q$, and thus by the lemma, $P_j = Q$.

Sylow Theorem 3. *Let G be a finite group and let p be a prime dividing the order of G . Then the number of Sylow p -subgroups is congruent to $1 \pmod{p}$ and divides $|G|$.*

Proof. Let P be a Sylow p -subgroup acting on the set of Sylow p -subgroups $\mathcal{P} = \{P = P_1, P_2, \dots, P_k\}$ by conjugation. As shown in the proof of Sylow Theorem 2, the only P -conjugate of P is P itself, and the orders of the other conjugacy classes are some power of p . $|\mathcal{P}|$ is the sum of positive powers of p and 1, so $|\mathcal{P}| \equiv 1 \pmod{p}$.

Suppose G acts on $|\mathcal{P}|$ by conjugation. Since all Sylow p -subgroups are conjugate, there is only one orbit under this action, so for $P \in \mathcal{P}$, $|\mathcal{P}| = \text{order of } P = [G : N(P)]$. But $[G : N(P)]$ must divide $|G|$, so the number of Sylow p -subgroups must divide $|G|$.

Bibliography:

Clarke, Allan. *Elements of Abstract Algebra*. New York: Dover Publications, Inc., 1984.

Ehrlich, Gertrude. *Fundamental Concepts of Abstract Algebra*. Boston, MA: PWS-KENT Publishing Company, 1991.

Gallian, Joseph A. *Contemporary Abstract Algebra*. Lexington, MA: D. C. Heath and Company, 1986.

Judson, Thomas W. *Abstract Algebra: Theory and Applications*. Boston, MA: PWS Publishing Company, 1994.