

**Abstract**

We discuss the nuances of the conjugation action in groups, and use it to prove the Sylow theorems. We then use the Sylow theorems to classify the nature of groups of a particular order.

**Introduction to Conjugation**

Every transitive left-action of a group on a set  $S$  is, up to isomorphism, left-multiplication on the set of left-cosets of  $G/\text{Stab}_G(a)$ , where  $\text{Stab}_G(a)$  denotes the stabilizer subgroup of  $a \in S$ . Furthermore, the number of elements of a finite orbit of  $a \in O_a$  is the index of  $\text{Stab}_G(a)$  — this is the much celebrated *orbit-stabilizer theorem*.

Note that from the orbit-stabilizer theorem, we can partition  $S$  into a formula involving the conjugacy classes. Since every element of  $s$  is either in an orbit or is in the set

$$Z := \{a \in S \mid g \cdot a = a \text{ for all } g \in G\},$$

we calculate

$$\begin{aligned} |S| &= |Z| + \sum_{a \in A} |O_a| \\ &= |Z| + \sum_{a \in A} [G : \text{Stab}_G(a)], \end{aligned}$$

where  $A$  is a system of representatives for the orbits. This is a class formula for the action of  $G$  on  $S$ .

The power of this class formula is that when  $G$  is finite,  $[G : \text{Stab}_G(a)]$  always divides  $|G|$ , which is a very strong constraint when we know something about  $|G|$ .

**Proposition:** Let  $|G| = p^n$  be a group that acts on a finite set  $S$ , and let  $Z$  be the set of fixed points for the action. Then,  $|Z| \equiv |S| \pmod{p}$ .

*Proof.* Since each summand of the form  $[G : \text{Stab}_G(a)]$  is a number larger than 1 and a power of  $p$ , each  $[G : \text{Stab}_G(a)]$  is congruent to 0 mod  $p$ .  $\square$

**Definition** (Conjugation Action). Let  $G$  be a group. The *conjugation action* of  $G$  on itself is defined by  $\rho: G \times G \rightarrow G$ , where

$$\rho(g, a) = gag^{-1}.$$

This map is equal to a particular group homomorphism  $\sigma: G \rightarrow \text{Sym}(G)$ .

**Definition** (Center). The *center* of  $G$ , denoted  $Z(G)$ , is the subgroup  $\ker(\sigma) \subseteq G$ . Concretely, it is

$$Z(G) = \{g \in G \mid ga = ag \text{ for all } a \in G\}.$$

Note that  $Z(G)$  is always a normal subgroup, and all elements of  $Z(G)$  commute with each other. Furthermore, a group  $G$  is abelian if and only if  $Z(G) = G$ .

**Lemma:** Let  $G$  be a finite group, and suppose  $G/Z(G)$  is cyclic. Then,  $G$  is commutative.

*Proof.* Write  $Z := Z(G)$ , and suppose  $G/Z$  is cyclic. Then, there is some  $g \in G$  such that  $\langle gZ \rangle = G/Z$ . For all  $a \in G$ , there is some integer  $r$  such that

$$aZ = g^r Z,$$

meaning there exists some  $z \in Z$  such that  $a = g^r z$ . Similarly, we write  $b = g^s w$  for some  $w \in Z$  and integer  $s$ . However, this means

$$ab = (g^r z)(g^s w)$$

$$\begin{aligned}
 &= g^{r+s}zw \\
 &= (g^s w)(g^r z) \\
 &= ba,
 \end{aligned}$$

where we use the fact that  $z$  and  $w$  commute with every element of  $G$ .  $\square$

**Definition.** Let  $a \in G$ . The *centralizer* of  $a$ , denoted  $Z_G(a)$ , is the stabilizer of  $a$  under conjugation. Concretely,

$$Z_G(a) = \{g \in G \mid ga = ag\},$$

or the set of elements of  $G$  that commute with  $a$ .

Note that  $Z(G) \subseteq Z_G(a)$  for all  $a \in G$ , and that

$$Z(G) = \bigcap_{a \in G} Z_G(a).$$

**Definition.** The *conjugacy class* of  $a \in G$  is the orbit  $[a]$  of  $a$  under conjugation.

## The Class Equation

What we call *the class equation* is generally the class formula for conjugation.

**Definition.** Let  $G$  be a finite group. Then,

$$|G| = |Z(G)| + \sum_{a \in A} [G : Z_G(a)],$$

where  $A$  is a family of representatives of conjugacy classes in  $G$ . This is known as the *class equation* for the group  $G$ .

We are very easily able to apply the class equation to prove certain properties about  $p$ -groups.

**Proposition:** Let  $G$  be a nontrivial  $p$ -group. Then,  $G$  has a nontrivial center.

*Proof.* Since  $|Z(G)| \equiv |G|$  modulo  $p$ , and  $|G| > 1$  is a power of  $p$ , we have  $|Z(G)|$  is a multiple of  $p$ . Since  $e_G \in Z(G)$ , we know that  $|Z(G)| \geq p$ .  $\square$

**Exercise:** Let  $p, q$  be prime numbers, and let  $G$  be a group of order  $pq$ . Prove that either  $G$  is commutative or the center of  $G$  is trivial.

Conclude that every group of order  $p^2$  is commutative.

**Solution:** From the class equation, we know that

$$pq = |Z(G)| + \sum_{a \in A} [G : Z_G(a)].$$

If  $|Z(G)| = pq$ , then  $G$  is abelian.

Suppose toward contradiction that, without loss of generality,  $|Z(G)| = p$ . Then,  $|G/Z(G)| = q$ , meaning  $G/Z(G)$  is cyclic, so  $G$  is abelian, so  $Z(G) = G$ .  $\perp$

Since, in any  $p$ -group,  $|Z(G)| \geq p$ , we must have that  $Z(G) = G$ , so  $G$  is abelian.

**Example.** Let  $G$  be a group of order 6. What are the possibilities for its class formula?

In general, if  $G$  is commutative, the class formula doesn't say much — in this case, it says  $6 = 6$ .

If  $G$  is not commutative then its center is trivial ( $6 = 2 \times 3$ ), so we have  $6 = 1 + \dots$ . Specifically, the  $\dots$  refers to the sizes of the conjugacy classes, which must be smaller than 6, greater than 1, and divide 6. Thus, we have

$$6 = 1 + 2 + 3$$

as the only possible class equation for a noncommutative group with six elements.

Note that normal subgroups are unions of conjugacy classes.<sup>1</sup> If  $H$  is a normal subgroup, and  $a \in H$  with  $b = gag^{-1}$  conjugate to  $a$ , we must have  $b \in gHg^{-1} = H$ .

Furthermore, every subgroup must have the identity and its size must divide the order of the group; therefore, a noncommutative group of order 6 cannot have any subgroup of order 2, since 2 cannot be written as a sum of orders of conjugacy classes including the center.

**Definition.** Let  $A \subseteq G$  be a subset,  $g \in G$  an element. The *conjugate* of  $A$  is the subset  $gAg^{-1}$ ; the map  $a \mapsto gag^{-1}$  is a bijection between  $A$  and  $gAg^{-1}$ .

**Definition.** Let  $A \subseteq G$  be a subset. The *normalizer*  $N_G(A)$  is its stabilizer under conjugation. The *centralizer* of  $A$  is the subgroup  $Z_G(A) \subseteq N_G(A)$  that fixes each element of  $A$ .

Therefore,  $g \in N_G(A)$  if and only if  $gAg^{-1} = A$ , and  $g \in Z_G(A)$  if and only if  $gag^{-1} = a$  for all  $a \in A$ . If  $A = \{a\}$ , then  $N_G(A) = Z_G(A) = Z_G(a)$ . However, in general,  $Z_G(A) \subsetneq N_G(A)$ .

If  $H$  is a subgroup of  $G$ , then every conjugate  $gHg^{-1}$  of  $H$  is also a subgroup of  $G$ ; all conjugate subgroups have the same order.

**Lemma:** Let  $H \subseteq G$  be a group. Then, the number of subgroups conjugate to  $H$  equals the index  $[G : N_G(H)]$  of the normalizer of  $H$  in  $G$ .

*Proof.* Considering the group's self-action of conjugation, this follows from the orbit-stabilizer theorem.  $\square$

**Corollary:** If  $[G : H]$  is finite, then the number of subgroups conjugate to  $H$  is finite and divides  $[G : H]$ .

*Proof.*

$$[G : H] = [G : N_G(H)][N_G(H) : H].$$

$\square$

A useful fact is that if  $H$  and  $K$  are subgroups of  $G$  such that  $H \subseteq N_G(K)$  — i.e., that  $gKg^{-1} = K$  for all  $g \in H$  — then conjugation by  $g \in H$  gives an automorphism of  $K$ . Thus, there is a set function

$$\gamma: H \rightarrow \text{Aut}(K).$$

**Exercise:** Let  $H$  and  $K$  be subgroups of  $G$  with  $H \subseteq N_G(K)$ . Verify that the function  $\gamma: H \rightarrow \text{Aut}(K)$  defined by conjugation is a homomorphism of groups, and  $\ker(\gamma) = H \cap Z_G(K)$ , where  $Z_G(K)$  is the centralizer of  $K$ .

**Solution:** Let  $a, b \in H$ . Then,

$$\begin{aligned} \gamma(ab^{-1}) &= (ab^{-1})K(ab^{-1})^{-1} \\ &= ab^{-1}Kba^{-1} \\ &= (aKa^{-1})(b^{-1}Kb) \\ &= (aKa^{-1})(bKb^{-1})^{-1} \\ &= \gamma(a)\gamma(b)^{-1}. \end{aligned}$$

The kernel of  $\gamma$  consists of all those elements of  $H$  that map to  $\text{id}: K \rightarrow K$  — i.e., those that map to the central-

<sup>1</sup>This is used to show that  $A_5$  is simple, for those of us studying for qualifiers.

izer of  $K$ . Therefore,  $\ker(\gamma)$  consists of  $H \cap Z_G(K)$ .

## The Sylow Theorems

The Sylow Theorems are a collection of theorems that concern  $p$ -subgroups of a certain finite group  $G$ . The first of the theorems says that  $G$  contains  $p$ -groups of all sizes allowed by Lagrange's theorem.

**Theorem (Cauchy's Theorem):** Let  $G$  be a finite group, and let  $p$  be a prime divisor of  $|G|$ . Then,  $G$  contains an element of order  $p$ .

We can show the abelian case as an exercise.

**Exercise:** Suppose  $G$  is a finite abelian group, and let  $p$  be a prime divisor of  $|G|$ . Prove there exists an element of order  $p$ .

**Solution:** Let  $g \in G$ . Then,  $\langle g \rangle \subseteq G$  is a cyclic subgroup, meaning that it is of order  $k$ , where  $k$  divides  $|G|$ . Assuming  $k \geq 2$ , we may write  $k = p_1^{e_1} \cdots p_n^{e_n}$ , where  $p_i$  are prime. Then, for some prime  $q$  such that  $q$  divides  $k$ , we may take the prime subgroup  $\langle h \rangle := \langle g^{k/q} \rangle$ .

Now, if  $q = p$ , we are done; else, we may take  $G/\langle h \rangle$ , which has order  $|G|/q$ , and since  $p \neq q$ , we may commence with the same process on  $G/\langle h \rangle$ .

However, we can also show the general case.

*Proof.* Let  $S$  be the set of ordered  $p$ -tuples of elements of  $G$ ,  $(a_1, \dots, a_p)$ , such that  $a_1 \cdots a_p = e$ . Then,  $|S| = |G|^{p-1}$ , as we may choose  $a_1, \dots, a_{p-1}$  arbitrarily, and select  $a_p$  to be the inverse of  $a_1 \cdots a_{p-1}$ .

Since  $p$  divides the order of  $S$ , it divides the order of  $G$ . Note that if  $a_1, \dots, a_p = e$ , then

$$a_2 \cdots a_p a_1 = e,$$

as  $a_1$  is a left-inverse to  $a_2 \cdots a_p$ , so it is a right inverse. Therefore, we may act  $\mathbb{Z}/p\mathbb{Z}$  on  $S$  by taking  $[m]$  to act on  $(a_1, \dots, a_p)$  yielding  $(a_{m+1}, \dots, a_p, a_1, \dots, a_m)$ ; this yields an element of  $S$ .

Thus, by the general class equation, we have  $|Z| \equiv |S| \equiv 0$  modulo  $p$ , where  $Z$  is the set of fixed points of the action.

In particular, fixed points are  $p$ -tuples of the form  $(a, \dots, a)$ ; note that  $Z \neq \emptyset$ , since  $(e, \dots, e) \in Z$ . Thus, there is some element in  $Z$  of the form  $(a, \dots, a)$  with  $a \neq e$ .

In particular, this means there is  $a \in G$  with  $a \neq e$  and  $a^p = e$ . □

**Corollary:** If  $p$  is a prime divisor of  $|G|$ , and  $N$  is the number of cyclic subgroups of order  $p$ , then  $N \equiv 1 \pmod{p}$ .

*Proof.* Since  $|Z|$  in the proof of Cauchy's theorem is congruent to 0 modulo  $p$ , we must have  $|Z| = mp$  for some  $m \geq 1$ . Now, since  $e_G \in Z$  but  $e_G$  is not of order  $p$ , we must have  $mp - 1$  elements of order  $p$  in  $G$ .

Since it takes  $p - 1$  elements of order  $p$  to yield a cyclic subgroup of order  $p$ , we thus have  $N = \frac{mp-1}{p-1} \equiv \frac{-1}{-1} = 1 \pmod{p}$ . □

**Exercise:** Let  $G$  be a group. A subgroup  $H$  of  $G$  is called *characteristic* if  $\varphi(H) \subseteq H$  for all automorphisms  $\varphi$  of  $G$ .

- Prove that characteristic subgroups are normal.
- Let  $H \subseteq K \subseteq G$ , with  $H$  characteristic in  $K$  and  $K$  normal in  $G$ . Prove that  $H$  is normal in  $G$ .
- Let  $G, K$  be groups, and suppose  $G$  contains a single subgroup  $H$  isomorphic to  $K$ . Prove that  $H$  is normal in  $G$ .
- Let  $K$  be a normal subgroup of a finite group  $G$ , and assume  $|K|$  and  $|G/K|$  are relatively prime. Prove that  $K$  is characteristic in  $G$ .

**Solution:**

- (a) Since conjugation is an automorphism, we have  $gHg^{-1} \subseteq H$  for each  $g \in G$ , meaning  $H$  is normal.
- (b) Since  $K$  is normal in  $G$ ,  $K$  is preserved under conjugation by elements of  $G$ , so conjugation by elements of  $G$  is an automorphism of  $K$ . Thus  $H$  is preserved by conjugation of elements in  $G$ , so  $H$  is normal in  $G$ .
- (c) Let  $\varphi: G \rightarrow K$  be a surjective homomorphism such that  $\varphi(H) \cong K$ . Then,

$$\begin{aligned}\varphi(gHg^{-1}) &= \varphi(g)\varphi(H)\varphi(g)^{-1} \\ &= K,\end{aligned}$$

so  $gHg^{-1} = H$ , meaning  $H$  is normal.

- (d) Let  $|K|$  and  $|G/K|$  be relatively prime. Let  $\varphi \in \text{Aut}(G)$ . Then, by the second isomorphism theorem, we have that

$$\begin{aligned}\frac{K\varphi(K)}{K} &\cong \frac{\varphi(K)}{\varphi(K) \cap K} \\ &:= H.\end{aligned}$$

Therefore, we have that  $|H|$  divides  $|\varphi(K)| = |K|$ . However, at the same time, we also have

$$\begin{aligned}\left| \frac{K\varphi(K)}{K} \right| &= [K\varphi(K) : K] \\ &= \frac{[G : K]}{[G : K\varphi(K)]},\end{aligned}$$

meaning that  $|H|$  divides  $[G : K]$ , so  $|H| = 1$ , and  $f(K) \cap K \subseteq K$ , so  $f(K) \subseteq K$ .

Using part (c) of the exercise, we can see that if there is only one cyclic subgroup  $H$  of order  $p$ , then that subgroup must be normal.

**Definition.** A group  $G$  is called *simple* if the only normal subgroups of  $G$  are  $\{e\}$  and  $G$ .

**Example.** Let  $p$  be a positive prime integer. If  $|G| = mp$  with  $1 < m < p$ , then  $G$  is not simple.

Consider the subgroups of  $G$  with  $p$  elements. Then, the number of these subgroups is congruent to 1 modulo  $p$ , so if there is more than one such subgroup, there must be at least  $p + 1$ . Any two distinct subgroups of prime order can only have trivial intersection (else, since both subgroups of prime order are cyclic, they would coincide on a generator), so this accounts for at least

$$p^2 = 1 + (p + 1)(p - 1)$$

elements in  $G$ . However, since  $|G| = mp < p^2$ , this is not possible. Therefore, there is only one cyclic subgroup of order  $p$  in  $G$ , which must be normal, so  $G$  is not simple.

Now, we can start on the Sylow theorems, the first of which generalizes the result from Cauchy's theorem.

**Definition.** Let  $p$  be a prime number. A  $p$ -Sylow subgroup of a finite group  $G$  is a subgroup of order  $p^r$ , where  $|G| = p^r m$  and  $\gcd(p, m) = 1$ .

In other words,  $P \subseteq G$  is a “maximal”  $p$ -group, in the sense that  $p$  does not divide  $[G : P]$ .

**Theorem (First Sylow Theorem):** Every finite group contains a  $p$ -Sylow subgroup for all primes  $p$ .

We may prove this from a more general result — that if  $p^k$  divides the order of  $G$ , then  $G$  has a subgroup of order  $p^k$ . But first, an exercise.

**Exercise:** Let  $p$  be a prime number, and let  $G$  be a  $p$ -group, with  $|G| = p^r$ . Prove that  $G$  contains a normal subgroup of order  $p^k$  for all  $0 \leq k \leq r$ .

**Proposition:** If  $p^k$  divides the order of  $G$ , then  $G$  has a subgroup of order  $p^k$ .

*Proof.* If  $k = 0$ , there is nothing to prove, so we may assume that  $k \geq 1$ , and that  $|G|$  is a multiple of  $p$ . We argue by induction on  $|G|$ . If  $|G| = p$ , there is nothing to prove, and if  $|G| > p$  with subgroup  $H \subseteq G$  where  $[G : H]$  is relatively prime to  $p$ , then  $p^k$  divides the order of  $H$ , and  $H$  has a subgroup of order  $p^k$  by the inductive hypothesis.

Thus, we assume that all proper subgroups of  $G$  have index divisible by  $p$ . By the class equation,  $p$  divides the order of  $Z(G)$ , so by Cauchy's theorem, there exists  $a \in Z(G)$  such that  $a$  has order  $p$ . The cyclic subgroup  $N := \langle a \rangle$  is contained in  $Z(G)$ , so it is normal on  $G$ .

Since  $|G/N| = |G|/p$ , and  $p^k$  divides  $|G|$ , we have that  $p^{k-1}$  divides  $|G/N|$ , so by the induction hypothesis,  $G/N$  has a subgroup of order  $p^{k-1}$ . This subgroup must be of the form  $P/N$  for some subgroup  $P$  of  $G$ .

Therefore, we have  $|P| = |P/N||N| = p^k$ . □

The second and third Sylow theorems are arguably more powerful than the first Sylow theorem. Specifically, the second Sylow theorem shows that all the  $p$ -Sylow subgroups are conjugates, and that every  $p$ -group is contained in a conjugate of some fixed  $p$ -Sylow subgroup. But first, an exercise.

**Exercise:** Let  $p$  be prime, let  $G$  be a  $p$ -group, and let  $S$  be such that  $p \nmid |S|$ . If  $G$  acts on  $S$ , show that the action must have a fixed point.

**Solution:** From the generalized class formula, we have

$$|S| = |Z| + \sum_{a \in A} [G : G_a].$$

Taking the modulus on both sides, the left side is some nonzero value, while  $\sum_{a \in A} [G : G_a]$  is zero mod  $p$  (as  $G$  is a  $p$ -group and stabilizers are subgroups). Thus,  $|Z| \neq 0$ .

**Theorem** (Second Sylow Theorem): Let  $G$  be a finite group, and let  $P$  be a  $p$ -Sylow subgroup. Let  $H \subseteq G$  be a  $p$ -group. Then,  $H$  is contained in a conjugate of  $P$  — i.e., there exists  $g \in G$  such that  $H \subseteq gPg^{-1}$ .

*Proof.* Use  $H$  to act on the left-cosets of  $P$  by left-multiplication. Since there are  $[G : P]$  cosets, and  $p$  does not divide  $[G : P]$ , the action must have a fixed point.

Let  $gP$  be a fixed point. Then, for all  $h \in H$ ,

$$hgP = gP,$$

or that  $g^{-1}hgP = P$  for all  $h \in H$ . Thus,  $g^{-1}Hg \subseteq P$ , and  $H \subseteq gPg^{-1}$ . □

Consider a chain

$$\{e\} = H_0 \subseteq H_1 \subseteq \cdots \subseteq H_k$$

of  $p$ -subgroups of  $G$ , with  $|H_i| = p^i$ . Then,  $H_k$  is contained in some  $p$ -Sylow subgroup of order  $p^r$ , where  $p^r$  is the maximum power of  $p$  dividing the order of  $G$ . However, we claim that the chain can be continued all the way to the form

$$\{e\} = H_0 \subseteq H_1 \subseteq \cdots \subseteq H_k \subseteq H_{k+1} \subseteq \cdots \subseteq H_r,$$

and that  $H_k$  is normal in  $H_{k+1}$ .

**Lemma:** Let  $H$  be a  $p$ -group contained in a finite group  $G$ . Then,

$$[N_G(H) : H] \equiv [G : H]$$

modulo  $p$ .

*Proof.* If  $H$  is trivial, then  $N_G(H) = G$ .

Let  $H$  be nontrivial, and act  $H$  on the set of left cosets of  $H$  by left-multiplication. The fixed points of this action are the cosets  $gH$  such that

$$hgH = gH,$$

for all  $h \in H$ , or that  $g^{-1}hg \in H$  for all  $h \in H$ ; specifically, this means the set of all  $g \in G$  such that  $gHg^{-1} = H$ , or that  $g \in N_G(H)$ . The statement then follows from the fact that  $|Z| \equiv |S| \pmod{p}$  if  $S$  is a set and  $Z$  is the set of fixed points.  $\square$

Thus, if  $H_k$  is not a  $p$ -Sylow subgroup — i.e.,  $p$  divides  $[G : H_k]$  — then  $p$  must also divide  $[N_G(H_k) : H_k]$ .

**Proposition:** Let  $H$  be a  $p$ -subgroup of a finite group  $G$ , and assume  $H$  is not a  $p$ -Sylow subgroup. Then, there exists a  $p$ -subgroup  $H'$  of  $G$  containing  $H$  such that  $[H' : H] = p$  and  $H$  is normal in  $H'$ .

*Proof.* Since  $H$  is not a  $p$ -Sylow subgroup,  $p$  divides  $[N_G(H) : H]$ . Since  $H$  is normal in  $N_G(H)$ , we consider the quotient group  $N_G(H)/H$ ; then,  $p$  divides the order of this group. Thus, by Cauchy's theorem,  $N_G(H)/H$  has an element of order  $p$ , which generates a subgroup of order  $p$  of  $N_G(H)/H$ . This subgroup has the form  $H'/H$  for some subgroup  $H'$  of  $N_G(H)$ .

By construction,  $[H' : H] = p$ , and  $H$  is normal in  $H'$  since  $H$  is normal in  $N_G(H)$ .  $\square$

The third Sylow theorem is probably the most commonly used of the bunch — it allows us to control the number of  $p$ -Sylow subgroups of  $G$ , and also allows us to establish the existence of normal subgroups in  $G$ .

**Theorem:** Let  $p$  be a prime number, and let  $G$  be a finite group such that  $|G| = p^r m$  with  $p$  not dividing  $m$ . Then, the number of  $p$ -Sylow subgroups divides  $m$  and is congruent to 1 modulo  $p$ .

*Proof.* The  $p$ -Sylow subgroups are conjugates of any given  $p$ -Sylow subgroup  $P$ . If we let  $N_p$  be the number of  $p$ -Sylow subgroups in  $G$ , then we know that  $N_p = [G : N_G(P)]$ . This number must divide the index of  $P$ ,

$$\begin{aligned} m &= [G : P] \\ &= [G : N_G(P)][N_G(P) : P] \\ &= N_p[N_G(P) : P]. \end{aligned}$$

Now, we have  $[G : P] \equiv [N_G(P) : P] \pmod{p}$ , so multiplying by  $N_p$ , we have  $mN_p \equiv m \pmod{p}$ . Thus,  $N_p \equiv 1 \pmod{p}$ .  $\square$

**Exercise:** Let  $P$  be a  $p$ -Sylow subgroup of a finite group  $G$ , and let  $H \subseteq G$  be a  $p$ -subgroup. Assume  $H \subseteq N_G(P)$ . Show that,  $H \subseteq P$ .

**Solution:** Let  $H \subseteq N_G(P)$ . Since  $P$  is normal on  $N_G(P)$ , we have that  $PH$  is a subgroup of  $N_G(P)$ . Then,  $|PH/P| = |H/(P \cap H)|$  by the second isomorphism theorem. Since  $H$  is a  $p$ -group,  $H/(P \cap H)$  is also a  $p$ -group, so  $|PH/P|$  is a power of  $p$ . However, since  $P$  is a  $p$ -Sylow subgroup of  $G$ , we must have  $PH = P$ , as otherwise,  $PH$  would be a  $p$ -group of order greater than  $P$ . Thus, we have  $H \subseteq P$ .

**Exercise:** Let  $P$  be a  $p$ -Sylow subgroup of a finite group  $G$ , and act with  $P$  by conjugation on the set of  $p$ -Sylow subgroups of  $G$ . Show that  $P$  is the unique fixed point of this action.

**Solution:** Let  $\mathcal{S}$  be the set of  $p$ -Sylow subgroups of  $G$ , and let  $P$  act on  $\mathcal{S}$  by conjugation. Suppose there exists  $Q$  such that for all  $p \in P$ ,  $pQp^{-1} = Q$ . Then,  $P \subseteq N_G(Q)$ , so  $P \subseteq Q$ ; however, since all the  $p$ -Sylow subgroups are the same order,  $P = Q$ .

**Exercise:** Use the second Sylow Theorem, the previous exercise, and the fact that the number of subgroups conjugate to a subgroup divides  $[G : H]$  to prove the third Sylow theorem.

**Solution:** Note that  $[G : P] = m$  for any  $p$ -Sylow subgroup, so

$$m = [G : N_G(P)][N_G(P) : P].$$

Since  $[N_G(P) : P]$  is the number of  $p$ -Sylow subgroups conjugate to  $P$ , and all  $p$ -Sylow subgroups are conjugate to each other, we have that the number of  $p$ -Sylow subgroups divides  $m$ .

If  $\mathcal{S}$  denotes the set of  $p$ -Sylow subgroups, then  $|\mathcal{S}| \equiv 1 \pmod{p}$  when  $P$  acts on  $\mathcal{S}$  with conjugation; since there is only one fixed point in this action, we must have the number of  $p$ -Sylow subgroups is congruent to 1 mod  $p$ .

## Applications of the Sylow Theorems