

---

# The Sylow Theorems

## Sylow Theorems

The Sylow theorems tell us quite a lot of information in general about the subgroups of a group of finite order. In this post, I'll be covering the basic ideas behind and finally the proofs of the Sylow theorems.

### 1.1 Group Actions

First, we describe group actions. For any group  $G$  and a set  $S$ , we can define a group action  $\rho : G \rightarrow \text{Perm}(S)$  which is a homomorphism from the group to the symmetric group to the set's permutations group. Alternatively, we could define the group action as operating on pairs in the product  $G \times S$ , i.e.:

$$\rho : G \times S \rightarrow S$$

With this definition, we also require associativity and also the action of the identity ( $\rho(e, s) = s$ ).

Example

For example, we look at conjugation. Let  $c(x) : G \rightarrow G$  be the map so that  $c(x)(y) = xyx^{-1}$ . In other words,  $c$  is a homomorphism from  $G$  to  $\text{Aut}(G)$ . We denote the kernel of this homomorphism as the **center** of  $G$ , denoted  $Z(G)$ .

---

**Definition:** For a defined group action  $\rho : G \rightarrow S$ , the **stabilizer** of  $s \in S$  consists of all the elements  $x \in G$  so that  $\rho(x, s) = s$ . In other words, the stabilizer of  $s$  is all the group elements which send  $s$  to itself. Often it is denoted  $G_s$

**Definition:** In the case where  $\rho$  is the conjugation group action, the isotropy group of  $a$  is called the **centralizer** of  $a$ . These are also all the elements  $x$  which commute with  $a$ . The isotropy group of a subgroup  $H \subseteq G$  is called the **normalizer** of  $H$ .

**Definition:** We define the **orbit** of  $s \in S$  under  $G$  to be the set  $\{xs | x \in G\}$ . In the case of the conjugation action, we refer to the orbits as **conjugacy classes** and it is clear that they form an equivalence class for the set.

---

There is a natural bijection between  $G/G_s$  and  $G_s$ , with the explicit bijection given by  $hG_s \rightarrow hs$ . Furthermore, the order of the orbit  $G_s$  is equal to the index  $(G : G_s)$ .

In particular, the number of conjugate subgroups to  $H$  is equal to the index of the normalizer of  $H$ . Also, the number of elements in the conjugacy class of  $x$  is equal to the index of the centralizer, i.e.  $G/G_s$ .

**Example** We will prove that every subgroup of index 2 is normal. Let  $S$  be the set of cosets of  $H$  defined in the usual way (there should be two). Then, the group action is defined as a homomorphism from  $G$  to  $S_2 = Z_2$ . Consider the kernel  $K$  of this homomorphism; this is all group elements  $g \in G$  so that  $gH = H$ . So, the kernel of this homomorphism is a subgroup of  $H$ . But then that means  $G/K$  is a subgroup of  $Z_2$ . So  $(G : K)$  is either 1 or 2. But we know that:

$$(G : K) = (G : H)(H : K)$$

And  $(G : H) = 2$ , so we must have  $(H : K) = 1$  so this tells us that  $(H : K) = 1$  and indeed  $H = K$ . So that means  $H$  is the kernel of the given homomorphism.

But for any homomorphism  $\phi$ , if we pick an arbitrary  $g \in G$  and  $k$  in the kernel, we have  $\phi(gkg^{-1}) = \phi(g) \phi(k) \phi(g)^{-1} = e$ . So indeed, the kernel is a normal subgroup. Therefore,  $H$  from the previous example is a normal subgroup.

---

We also can write the obvious fact that the order of a set  $S$  is the sum of all the orbits in this new notation, in the **decomposition formula**:

$$|S| = \sum_{G_s} (G : G_s)$$

We have a special case where the group action is conjugation. In this case, we take  $Y$  to be a set of representatives from each conjugation class and write the **class formula**:

$$|G| = |Z(G)| + \sum_{y \in Y} (G : G_y)$$


---

---

## 1.2 Sylow Subgroups

**Definition** Let  $p$  be a prime number. Then a Sylow  $p$ -group is a finite group of order  $p^n$  for some  $n$ .

With this definition, we prove an intermediate theorem:

### 1.2.1 Theorem

Let  $G$  be a non-trivial  $p$ -group. Then  $G$  has a non-trivial center. Furthermore,  $G$  is solvable.

**Proof** From the class formula, we have:

$$|G| = |Z(G)| + \sum_{y \in Y} (G : G_y)$$

If the center is trivial, then the sum on the RHS of the equation adds up to  $|G| - 1$ . Since  $G$  is a  $p$ -group, the prime  $p$  divides both sides of the equation. However, this is clearly impossible since  $p$  does not divide  $|G| - 1$ . So the center is non-trivial.

We also know that  $G/Z(G)$  is a  $p$ -group as well, and it is strictly smaller than  $G$ . The rest of the proof proceeds by induction on  $n$ .

We know for a fact that cyclic groups are solvable (with the shortest normal series which is abelian). Suppose the theorem holds for all  $p$ -groups with  $n \leq k - 1$ . Then, we have that  $Z(G)$  and  $G/Z(G)$  are both solvable since they are  $p$ -groups as well. So, we have proved the  $n = k$  case.

---

### 1.2.2 Theorem: First Sylow Theorem

Suppose that we have  $p^n \mid G$  and  $p^{n-1} \nmid G$  for some prime  $p$ . Then, define a Sylow  $p$ -subgroup of  $G$  to be a subgroup of order  $p^n$ . We will prove that for every  $p \mid G$ , there exists a  $p$ -Sylow subgroup.

---

**Lemma: Cauchy's Theorem** We start with the brief lemma that for any finite abelian group  $G$ , for any prime  $p \mid |G|$ , there is a subgroup in  $G$  of order  $p$ . This is known as Cauchy's lemma and is a special case of Sylow's First Theorem.

By the fundamental theorem of finite abelian groups,  $G$  can be written as the direct product:

$$G = G(p) \times G'$$

Where  $|G'|$  is prime to  $p$ . Take an element  $a \in G(p)$  with order  $p^k$ . Then take:

$$b = a^{p^{k-1}}$$

We know that  $b$  is not the identity. However,  $b^p = a^p = e$ . So,  $b$  generates a cyclic group of order  $p$ , and we are done.

In fact, we can generalize Cauchy's theorem to arbitrary finite groups using the class equation:

$$|G| = |Z(G)| + \sum_{y \in Y} (G : G_y)$$

Suppose that  $p \mid |Z(G)|$ . Then we can apply the earlier proof to  $Z(G)$  to find an element of order  $p$  in  $Z(G) \subseteq G$ ; so we are done.

Suppose instead that  $p \nmid |Z(G)|$ . Then, the sum on the right hand side cannot divide  $p$  either, and in particular there is at least one conjugacy class  $G_y$  with order prime to  $p$ . Therefore,  $p \nmid |G_y|$ . But this means that  $G_y$  divides  $p!$ . Applying Cauchy's lemma to this group, we find an element of order  $p$  in  $G_y$  and therefore in  $G$ , and we are done.

---

**Proof of Sylow's First Theorem** Cauchy's lemma proves that  $G$  certainly has a subgroup of size  $p$ . With Sylow's first theorem, we prove that  $G$  has a subgroup of size  $p^n$ , where  $p^n$  is the largest power of  $p$  dividing the order of  $G$ . We proceed by induction on the size of  $G$ .

Suppose that there is a proper subgroup  $H \subset G$  so that  $(G : H)$  does not divide  $p$ . Then  $p^n \mid |H|$ , and so by induction  $H$  has a  $p$ -Sylow subgroup which is also a  $p$ -Sylow subgroup of  $G$ . We assume then that every proper subgroup  $H \subset G$  has the property

---

that  $p \mid (G : H)$ . Now, we let  $G$  act on itself by conjugation and consider the class formula:

$$|G| = |Z(G)| + \sum_{y \in Y} (G : G_y)$$

The order of each of the orbits divides the order of the group (since a stabilizer or in this case a conjugacy class, is a subgroup), so  $p$  divides the order of  $Z(G)$ , and  $G$  has a non-trivial center; furthermore, by a similar proof to Cauchy's lemma, we have that  $G$  contains a subgroup  $H$  of size  $p$ . Furthermore, since  $H$  is a subgroup of the center in particular, it is a normal subgroup.

We consider the group  $G/H$ . By the inductive hypothesis, this group has a subgroup  $K'$  of order  $p^{n-1}$ . By the third isomorphism theorem,  $K'$  is really (isomorphic to) a subgroup of the form  $K/H$ , where  $H \subset K \subset G$ . Take this  $K$ ; it has order  $p^n$  as desired.

---

### 1.2.3 Theorem: Second Sylow Theorem

The second Sylow Theorem states that all  $p$ -Sylow subgroups are conjugate to each other. Before we get to that, let's prove a related lemma:

**Lemma: Every  $p$ -subgroup of  $G$  is contained in some  $p$ -Sylow subgroup.** This isn't hard to prove using the class formula. Let  $S$  be the set of  $p$ -Sylow subgroups of  $G$ , and  $G$  operates on  $S$  by conjugation. Let's take  $P$  to be one of those Sylow subgroups. Then we have:

$$|Orb(P)| = \frac{|G|}{|G_P|}$$

Where  $G_P$  is the normalizer of  $P$  which sends  $P$  to itself under conjugation. Evidently,  $G_P$  contains  $P$ , so that means  $|Orb(P)|$  is prime to  $p$ . Let's take a look at the action of a  $p$ -subgroup  $H$  on  $Orb(P)$  using the class formula:

$$|Orb(P)| = |Z| + \frac{|Orb(P)|}{|H_{Orb(P)}|}$$

By Lagrange, each term in the right hand sum divides  $|H|$  so that means there is a non-trivial center  $P'$  within  $|Orb(P)|$ . This means that  $H$  is contained within the

---

normalizer of  $P'$ . Since  $H$  is contained in the normalizer, by the second isomorphism theorem we know that  $HP'$  is a subgroup with  $P' \trianglelefteq HP'$ . The order of the quotient group  $HP'/P \cong H/(H \cap P')$  is a power of  $p$ , so the order of  $HP'$  is also a power of  $p$ . But then  $HP' = P'$  since  $P'$  is a maximal  $p$ -subgroup of  $G$ ; and therefore  $H \subseteq P'$ . We have now found a Sylow subgroup which contains  $H$ .

**Proof of Sylow's Second Theorem** Let  $H$  be some  $p$ -Sylow subgroup of  $G$ .  $H$  is contained in some conjugate  $P'$  of  $P$  by the above argument. And again by the above construction, because  $H$  and  $P'$  have equal orders,  $H = P'$ .

This second theorem implies as a direct corollary that if there is only one  $p$ -Sylow subgroup, it is normal.

---

### 1.2.4 Sylow's Third Theorem

Sylow's Third Theorem is arguably the most useful. It says that the number of  $p$ -Sylow subgroups of  $G$  is equal to  $1 \pmod{p}$ . That means by counting arguments, if  $\|G\|/p^n < p$ , then the Sylow subgroup is normal.

**Proof of Sylow's Third Theorem** Take the action of  $H = P$  on the set  $S$  consisting of the Sylow  $p$ -subgroups. Any other orbit cannot have just one element  $P'$ , or else  $H$  is contained in the normalizer of  $P'$ , and by earlier arguments  $H = P = P'$ . Take an element  $s'$  of any other orbit. It has a stabilizer, which is a proper subgroup of  $H$ ; the stabilizer is a subgroup, so it is divisible by  $p$ .

As a result, the number of elements in  $S'$  is divisible by  $p$ . So the size of  $S$  (the set of all  $p$ -Sylow subgroups) is equal to 1 (the size of the center of conjugation under  $P$ ) plus the size of all the remaining orbits (all of which have orders which divide  $p$ ). So we are done.

---