

# The Sylow Theorems

Our aim is to prove the following theorem:

**Theorem 1 (Sylow's Theorem)** *Let  $G$  be a finite group and  $p$  a prime number. If  $p^n$  divides the order of  $G$ , then  $G$  has a subgroup of order  $p^n$ .*

We need some preliminary concepts and results, all of which are interesting in their own right. Our first topic is

## Conjugacy Classes and the Class Equation

If  $G$  is a group, define a relation on  $G$  by saying that  $a \sim b$  for  $a, b \in G$  if and only if there exists an element  $x \in G$  such that  $x^{-1}ax = b$ , in which case we say that  $a$  is *conjugate* to  $b$ .

**Lemma 2**  *$\sim$  is an equivalence relation on  $G$ .*

**Proof:** For every  $a \in G$  we have  $e^{-1}ae = a$ , so  $\sim$  is reflexive. If  $a \sim b$  then there exists  $x \in G$  such that  $x^{-1}ax = b$ . But then  $a = xbx^{-1} = (x^{-1})^{-1}bx^{-1}$ , so  $b \sim a$ , and  $\sim$  is symmetric. Finally, if  $a \sim b$  and  $b \sim c$ , then there exist  $x, y \in G$  such that  $x^{-1}ax = b$  and  $y^{-1}by = c$ . Hence we have

$$(xy)^{-1}a(xy) = y^{-1}(x^{-1}ax)y = y^{-1}by = c,$$

so  $a \sim c$  and  $\sim$  is transitive.  $\square$

The equivalence class of an element  $a \in G$  under  $\sim$  is denoted  $[a]$  and is called the *conjugacy class* of  $a$ . Our immediate aim is to prove that if  $G$  is finite, then  $\#[a] \mid |G|$  for every  $a \in G$ . Our strategy will be to show that  $\#[a] = (G : C_G(a))$ , where  $C_G(a)$  is the centralizer of  $a$  in  $G$ . (Recall that  $C_G(a) := \{g \in G \mid ga = ag\}$  is the subgroup of elements that commute with  $a$ .)

**Proposition 3** *If  $G$  is a finite group and  $a \in G$ , then  $\#[a] = (G : C_G(a))$ , and hence divides the order of  $G$ .*

**Proof:** First note that if  $a, x, y \in G$ , then  $x^{-1}ax = y^{-1}ay$  iff  $C_G(a)x = C_G(a)y$ . Indeed, if  $x^{-1}ax = y^{-1}ay$ , then

$$a = xy^{-1}ayx^{-1} = (xy^{-1})a(xy^{-1})^{-1} \implies (xy^{-1})a = a(xy^{-1}),$$

so that  $xy^{-1} \in C_G(a)$ . But then  $x$  and  $y$  yield the same right coset of  $C_G(a)$  as claimed.

This means that the function  $f : [a] \rightarrow \{C_G(a)x \mid x \in G\}$  defined by  $f(x^{-1}ax) = C_G(a)x$  is well-defined and injective. It is also surjective, since for every coset  $C_G(a)x$ , the conjugate  $x^{-1}ax \in [a]$ . Hence,  $f$  is bijective, so  $\#([a]) = (G : C_G(a))$ . But  $|C_G(a)|(G : C_G(a)) = |G|$  by Lagrange's Theorem, so  $\#([a]) \mid |G|$ .  $\square$

Proposition 3 has the following consequence:  $\#([a]) = 1$  (i.e.  $[a] = \{a\}$ ) if and only if  $(G : C_G(a)) = 1$  if and only if  $G = C_G(a)$ . But this last condition means that every element of  $G$  commutes with  $a$ , which is the same as saying that  $a \in Z(G)$ , the center of  $G$ . Thus, the number of conjugacy classes in  $G$  with a single element is the order of  $Z(G)$ . Let  $[a_1], \dots, [a_t]$  be the distinct conjugacy classes of  $G$  having more than one element, say  $k_i = \#([a_i]) > 1$  for  $i = 1, \dots, t$ . Since the conjugacy classes form a partition of  $G$ , the foregoing remarks yield the *class equation* for  $G$ :

$$(\dagger) \quad |G| = |Z(G)| + k_1 + \dots + k_t.$$

## ***p*-Groups**

Since Sylow's Theorem concerns subgroups of prime-power order, we are led to investigate finite groups of order  $p^n$ , where  $p$  is a prime number.

**Definition 4** *A finite group  $G$  is called a  $p$ -group if the order of every  $g \in G$  is a power of  $p$ .*

**Lemma 5**  *$G$  is a  $p$ -group iff  $|G|$  is a power of  $p$ .*

**Proof:** If  $|G| = p^n$ , then every  $g \in G$  has order a power of  $p$  by Lagrange's Theorem, so  $G$  is a  $p$ -group. On the other hand, if  $G$  is a  $p$ -group, and  $q$  is a prime number dividing  $|G|$ , then Cauchy's Theorem implies that  $G$  has an element of order  $q$ . Hence  $q$  must be a power of  $p$ , which means that  $q = p$  since  $q$  is prime. This means that the only prime dividing  $|G|$  is  $p$ , so  $|G|$  is a power of  $p$ .  $\square$

Now suppose that  $G$  is a non-trivial  $p$ -group with  $|G| = p^n$  and consider the class equation  $(\dagger)$  for  $G$ . Each  $k_i > 1$  divides  $|G| = p^n$ , so we have  $k_i = p^{m_i}$  for integers  $m_i > 0$ . But then

$$|Z(G)| = |G| - k_1 - \dots - k_t = p^n - p^{m_1} - \dots - p^{m_t},$$

which implies that  $p$  divides  $|Z(G)|$ . But  $|Z(G)| > 0$  since  $e \in Z(G)$ , so it follows that  $|Z(G)| \geq p$ . We have proved the following remarkable fact:

**Proposition 6** *If  $G$  is a nontrivial  $p$ -group, then  $Z(G)$  is nontrivial.*

As an application, we exploit the nontriviality of centers in  $p$ -groups to obtain a classification theorem about groups of order  $p^2$ .

**Proposition 7** *If  $|G| = p^2$  then  $G$  is abelian. Moreover, we have either  $G \simeq \mathbb{Z}/p^2\mathbb{Z}$  or  $G \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ .*

**Proof:** If  $|G| = p^2$ , then either  $Z(G) = G$  (in which case  $G$  is abelian) or  $|Z(G)| = p$ . In the latter case,  $G/Z(G)$  has order  $p$ , and hence is cyclic, say generated by the coset  $Z(G)a$ . This means that if  $g \in G$  is arbitrary, then  $Z(G)g = (Z(G)a)^m = Z(G)a^m$  for some  $m > 0$ . But then  $g = ca^m$  for some  $c \in Z(G)$ . If  $h$  is another element of  $G$ , then  $h = da^n$  for some  $d \in Z(G)$  and  $n > 0$ . But then  $gh = ca^m da^n = da^n ca^m = hg$ , since  $c$  and  $d$  commute with everything in  $G$ . This shows that  $G$  is abelian.

If  $G$  is cyclic, then we know from our classification theorem that it is isomorphic to  $\mathbb{Z}/p^2\mathbb{Z}$ . So suppose  $G$  is not cyclic. Then by Lagrange's Theorem, every nonidentity element of  $G$  has order  $p$ . Choose any  $g \neq e$  in  $G$ , and then choose another  $h \notin \langle g \rangle$ . Then the elements  $g^i h^j$  are all distinct for  $0 \leq i, j \leq p-1$ , and thus these are all the elements of  $G$ . The function  $f : G \rightarrow \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$  defined by  $f(g^i h^j) = (i, j)$  is then well-defined and an isomorphism.  $\square$

## Proof of Sylow's Theorem

Suppose that  $G$  is a finite group,  $p$  is a prime number, and  $p^n$  divides the order of  $G$ . We must prove that  $G$  has a subgroup of order  $p^n$ . The proof goes by induction on  $|G|$ , the order of the group. There is nothing to prove for  $|G| = 1$ , since  $G$  is the trivial group in this case. So suppose the claim is true for all groups of order less than  $|G|$ . To begin, note that if the group  $G$  has a *proper* subgroup  $H < G$  such that  $p^n$  divides  $|H| < |G|$ , then  $H$  has a subgroup of order  $p^n$  by the induction hypothesis, and this subgroup is also a subgroup of  $G$ . So we may assume that  $p^n$  does not divide the order of any proper subgroup of  $G$ . Consider the class equation ( $\dagger$ ) for  $G$ :

$$|G| = |Z(G)| + k_1 + \cdots + k_t$$

where  $k_i = \#([a_i])$ , and  $[a_1], \dots, [a_t]$  are all of the distinct conjugacy classes in  $G$  containing more than one element. Now  $k_i = (G : C_G(a_i))$  by Proposition 3, so Lagrange's Theorem says  $|G| = |C_G(a_i)|k_i$ . Since  $k_i > 1$ , we see that  $|C_G(a_i)| < |G|$ , so  $C_G(a_i)$  is a proper subgroup of  $G$ , and by assumption,  $p^n \nmid |C_G(a_i)|$ . Since  $p^n$  *does* divide the order of  $G$ , it follows that  $p$  must divide  $k_i$  for  $i = 1, \dots, t$ , and we see that  $|Z(G)| = |G| - k_1 - \dots - k_t$  must also be divisible by  $p$ . Cauchy's Theorem then implies that there is an element  $a \in Z(G)$  of order  $p$ .

Consider the cyclic subgroup  $\langle a \rangle < Z(G)$ , which is normal in  $G$  (every subgroup of the center of a group is normal in the whole group). Consider the quotient group  $H := G/\langle a \rangle$ , which has order  $\frac{|G|}{p}$ , which means that  $p^{n-1}$  divides  $|H| < |G|$ . By the induction hypothesis,  $H$  has a subgroup  $S$  of order  $p^{n-1}$ , and I claim that  $S^* := f^{-1}(S) < G$  is a subgroup of order  $p^n$ , where  $f : G \rightarrow G/\langle a \rangle = H$  is the canonical homomorphism. Indeed, by a Homework Problem,  $S^*/\langle a \rangle \simeq S$ , so  $|S^*| = |\langle a \rangle||S| = pp^{n-1} = p^n$ . Thus we have found a subgroup of  $G$  of order  $p^n$ . By induction, it follows that Sylow's Theorem is true for all finite groups  $G$ .  $\square$

## More Sylow Theorems

Sylow's Theorem is actually the First Sylow Theorem, and it is usually accompanied by the Second and Third Sylow Theorems, which we now state without proof. We begin with a definition:

**Definition 8** *Suppose that  $G$  is a finite group of order  $p^k m$  with  $(p, m) = 1$ . Then  $K < G$  is called a  $p$ -Sylow subgroup of  $G$  if and only if  $|K| = p^k$ .*

Sylow's Theorem implies that if  $G$  is a finite group, then  $G$  has at least one  $p$ -Sylow subgroup for every prime number  $p$ . (If  $p \nmid |G|$ , then the trivial subgroup is a  $p$ -Sylow subgroup).

**Theorem 9 (Second Sylow Theorem)** *If  $G$  is a finite group and  $H$  is a  $p$ -subgroup of  $G$ , then  $H$  is contained in a  $p$ -Sylow subgroup of  $G$ .*

**Theorem 10 (Third Sylow Theorem)** *Any two  $p$ -Sylow subgroups of a finite group  $G$  are conjugate. Moreover, if  $P$  is the number of distinct  $p$ -Sylow subgroups of  $G$ , then  $P$  divides  $|G|$  and  $P = pt + 1$  for some integer  $t \geq 0$ .*