The Sylow theorems

1 Definition of a p-Sylow subgroup

Lagrange's theorem tells us that if G is a finite group and $H \leq G$, then $\#(H)$ divides $\#(G)$. As we have seen, the converse to Lagrange's theorem is false in general: if G is a finite group of order n and d divides n, then there need not exist a subgroup of G whose order is d. The Sylow theorems say that such a subgroup exists in one special but very important case: when d is the largest power of a prime which divides n. (It then turns out that G has a subgroup of every order which is a prime power dividing n, not necessarily the largest such.) In fact, the Sylow theorems tell us much more about such subgroups, by giving information on how many such subgroups can exist. As we shall see, this will sometimes enable us to show that G has a nontrivial proper normal subgroup.

Definition 1.1. Let p be a prime number. Write $\#(G) = p^r m$ where p does not divide m. In other words, p^r is the largest power of p which divides n. We shall usually assume that $r \geq 1$, i.e. that $p|n$. A *p-Sylow subgroup* of G is a subgroup P such that $\#(P) = p^r$.

Theorem 1.2 (Sylow Theorems)**.** *Let G be a group of order n, let p be a prime number such that $p|n$, and write $n = p^r m$ where p does not divide m. Then:*

(i) *There exists a p-Sylow subgroup of G.*

(ii) *If P_1 and P_2 are two p-Sylow subgroups of G, then P_1 and P_2 are conjugate, i.e. there exists a $g \in G$ such that $gP_1g^{-1} = P_2$.*

(iii) *If $H \leq G$ and $\#(H) = p^s$ with $s \leq r$, then there exists a p-Sylow subgroup P of G such that $H \leq P$.*

(iv) *The number of p-Sylow subgroups of G is congruent to $1 \pmod{p}$ and divides $\#(G)$.*

Example 1.3. (1) Let $G = A_4$, so that $\#(A_4) = 12$. Then A_4 has a 2-Sylow of order 4 and a 3-Sylow of order 3. In fact, we know that there exists a subgroup H of order 4 of A_4 and S_4, and that $H \lhd A_4$ and $H \lhd S_4$: $H = \{1, (12)(34), (13)(24), (14)(23)\}$. Since H is normal in A_4, H is the unique 2-Sylow subgroup of A_4, by (ii) of the Sylow theorem. In fact, more generally we have the following corollary of (ii) of the Sylow theorem:

Corollary 1.4. *A finite group G contains exactly one p-Sylow subgroup $\iff$ there exists a normal p-Sylow subgroup.*

Proof. $\implies$: Suppose that there is exactly one p-Sylow subgroup P of G. For all $g \in G$, $gPg^{-1} = i_g(P)$ is another subgroup of G of order equal to $\#(P)$, hence gPg^{-1} is also a p-Sylow subgroup and so $gPg^{-1} = P$ for all $g \in G$. This says that P is normal in G.

$\impliedby$: Let P be a normal p-Sylow subgroup subgroup of G. If P' is another p-Sylow subgroup, then by (ii) of the Sylow theorem there exists a $g \in G$ such that $P' = gPg^{-1}$. But since P is normal, $gPg^{-1} = P$. Hence $P' = P$, i.e. P is the unique p-Sylow subgroup subgroup of G. □

To conclude the example of A_4, the 3-Sylow subgroups have order 3, hence are necessarily cyclic of order 3. In A_4, every element of order 3 is a 3-cycle. As we have seen, there are $8 = (4 \cdot 3 \cdot 2)/3$ 3-cycles. But every cyclic group of order 3 has $\varphi(3) = 2$ generators, so the number of subgroups of A_3 is $8/2 = 4$. Thus there are 4 3-Sylow subgroups, verifying the fact that the number of such is $\equiv 1 \pmod 3$ and divides 12. Explicitly, the 3-Sylow subgroups are $\langle(123)\rangle$, $\langle(124)\rangle$, $\langle(134)\rangle$, and $\langle(234)\rangle$. It is easy to see that they are all conjugate. (However, the 8 elements of order 3 are not all conjugate to each other in A_4. For example, (123) is conjugate in A_4 to (142) but not to (124).)

(2) Taking $G = S_4$, with $\#(S_4) = 24$, we see that the 2-Sylow subgroups have order 8 and the 3-Sylow subgroups have order 3. The 3-Sylow subgroups of S_4 are the same as those for A_4, namely the cyclic subgroups generated by 3-cycles, and hence there are 4 of them. Every 2-Sylow subgroup contains H, since H is normal in S_4 and all 2-Sylow subgroups are conjugate, so to describe all possible 2-Sylow subgroups it is enough to describe all ways that H can be completed to a subgroup of order 8 of S_4. It is not hard to show that there are 3 such ways, so that S_4 has 3 different 2-Sylow subgroups; note that $3 \equiv 1 \pmod 2$ and 3 divides 24. One of these is the subgroup D_4, given explicitly by

$$D_4 = \{1, (1234), (13)(24), (1432), (12)(34), (14)(23), (13), (24)\}.$$

But there are two other ways to enlarge H to a subgroup of order 8. For example, if we add $(1,2)$ to H, we obtain the subgroup

$$P = \{1, (12)(34), (13)(24), (14)(23), (12), (34), (1324), (1423)\}.$$

Another way to find the subgroup P is as follows: we have seen that the conjugacy class containing $(12)(34)$ has 3 elements. Thus the order of the centralizer $Z_{S_4}((12)(34))$ is $24/3 = 8$. In other words, the set of elements of S_4 commuting with $(12)(34)$ is a subgroup P of S_4 of order 8. Note that P contains H, since H is abelian. The other 4 elements of P can be found by inspection: clearly (12) commutes with $(12)(34)$, and then the remaining 4 elements of P must be the coset $(12)H$. Finally, the third subgroup of order 8 is found similarly, by adding (14) to H.

(3) Consider the symmetric group S_p, where p is prime. Then p divides $p! = \#(S_p)$, and clearly p is the largest power of the prime p which divides $p!$, since every natural number $k < p$ is relatively prime to p. Thus every p-Sylow subgroup of S_p has order p, hence is cyclic, and the number of them is $\equiv 1 \pmod{p}$ and divides $p!$. In fact, we can count the number of p-Sylow subgroups of S_p directly: the only elements of order p in S_p are p-cycles, and as in (1) the number of p-cycles is $p!/p = (p-1)!$. However, to count the number of cyclic **subgroups** of order p, we should divide the number of elements of order p by the number of generators of a cyclic group of order p, namely $\varphi(p) = p - 1$. So the total number of p-Sylow subgroups of S_p is $(p-1)!/(p-1) = (p-2)!$, which clearly divides $p!$. The fact that this number is $\equiv 1 \pmod{p}$ is equivalent to the following theorem in elementary number theory:

Theorem 1.5 (Wilson's Theorem)**.** *If p is a prime number, then* $(p-1)! \equiv -1 \pmod{p}$.

Wilson's Theorem is obvious in case $p = 2$. For an odd prime p, Wilson's theorem is a simple group theory fact, using the result (which we have stated but not proved) that $(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic of order $p - 1$, hence is a cyclic group of even order. But if G is a cyclic group of even order k, written multiplicatively, and $-1 \in G$ is the unique element of order 2, then

$$\prod_{g \in G} g = -1,$$

since if $g \in G$, $g \neq \pm 1$ (i.e. g does not have order 1 or 2), then $g^{-1} \neq g$. Thus in the product above, every element is paired with its inverse except for 1 and -1, so the above product becomes $1 \cdot (-1) = -1$.

(4) Let G be a group of order 100. Then every 2-Sylow subgroup of G has order 4 and every 5-Sylow subgroup of G has order 25. The number of 2-Sylow subgroups of G is odd and divides 100, hence is equal to 1, 5, or 25. The number of 5-Sylow subgroups of G is $\equiv 1 \pmod 5$ and divides 100, hence is equal to 1, since the only factors of 100 not divisible by 5 are 1, 2, 4, and none of them is $\equiv 1 \pmod 5$. In particular, G has a normal subgroup of order 25 and hence is not simple.

(5) Let p and q be distinct primes, with, say, $p < q$. Then a group of order pq is not simple. In fact, let P be a p-Sylow subgroup, and let Q be a q-Sylow subgroup. Then the number of q-Sylow subgroups is a divisor of pq and $\equiv 1 \pmod q$. But the only divisors of pq are 1, p, q, and pq, and the only one of these $\equiv 1 \pmod q$ is 1. Hence $Q \lhd G$. Note further that, by the same reasoning, if q is not congruent to 1 mod p, then P is also normal. It then follows by homework problems that $P \cap Q = \{1\}$ and that every element of P commutes with every element of P, i.e. for all $h \in P$ and $k \in Q$, $hk = kh$. From this, it is easy to see that, still under the assumption that q is not congruent to 1 mod p,

$$G \cong P \times Q \cong (\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/q\mathbb{Z}) \cong \mathbb{Z}/pq\mathbb{Z}.$$

If $q \equiv 1 \pmod p$, it turns out that there is exactly one non-abelian group of order pq up to isomorphism. We shall describe this group explicitly in the last handout; it is a generalization, in a certain sense, of the dihedral groups.

2 Proof of the Sylow theorem

We now turn to the proof of the Sylow theorem. Before we give the proof, we record two lemmas which we shall use:

Lemma 2.1. *Let G_1 and G_2 be two finite groups, $f\colon G_1 \to G_2$ a finite surjective homomorphism, and H_2 a subgroup of G_2. Then, if*

$$H_1 = f^{-1}(H_2) = \{g \in G_1 : f(g) \in H_2\},$$

then $(G_1 : H_1) = (G_2 : H_2)$.

Proof. Let $K = \operatorname{Ker} f$. Then $K \lhd G_1$ and $G_1/K \cong G_2$, by the Fundamental Theorem of Homomorphisms. Hence $\#(G_2) = \#(G_1)/\#(K)$. Now, since $1 \in H_2$, $K \leq H_1$ and in fact $K \lhd H_1$. If we define $f|H_1\colon H_1 \to H_2$ to be the restriction of f, then $f|H_1$ takes values in H_2 by definition, and

$f|H_1$ is surjective since f is surjective. Clearly $\mathrm{Ker}(f|H_1) = \mathrm{Ker}\, f \cap H_1 = K \cap H_1 = K$, since $K \leq H_1$. Thus, again by the Fundamental Theorem of Homomorphisms, $H_2 \cong H_1/K$ and hence $\#(H_2) = \#(H_1)/\#(K)$. Now we compute the indexes:

$$\begin{aligned}(G_2 : H_2) &= \#(G_2)/\#(H_2) = (\#(G_1)/\#(K))\Big/(\#(H_1)/\#(K)) \\ &= \#(G_1)/\#(H_1) = (G_1 : H_1).\end{aligned}$$

□

Lemma 2.2 (Cauchy's Theorem for abelian groups)**.** *Let G be a finite* ***abelian*** *group. If p is a prime number such that p divides $\#(G)$, then there exists an element of G of order p.*

Proof. The proof is by complete induction on the order of G (where we take the statement as vacuously true if p does not divide the order of G, and hence for $G = \{1\}$). Also, if G is cyclic, we know that, for every divisor d of $\#(G)$, G contains an element of order d, so the lemma holds for all cyclic groups. In general, suppose that the lemma has been proved for all groups of order less than n, and let G be a group of order n. Let p be a prime dividing n. Since $n > 1$, there exists an element $g \in G$ with $g \neq 1$. Consider the cyclic subgroup $\langle g \rangle$. If $p|\#(\langle g \rangle)$, then, by our earlier results on cyclic groups, $\langle g \rangle$ contains an element of order p, which then gives an element of order p in G. If p does not divide $\langle g \rangle$, then consider the quotient group $G/\langle g \rangle$, of order $\#(G)/\#(\langle g \rangle) < \#(G)$. (Note that, since G is abelian, $\langle g \rangle$ is automatically normal in G and so the cosets form a group, which is the only place where we use the assumption that G is abelian.) Then p divides $\#(G) = \#(\langle g \rangle)\#(G/\langle g \rangle)$ and p does not divide $\langle g \rangle$, so that p divides $\#(G/\langle g \rangle)$. By the inductive assumption, there exists an element of $G/\langle g \rangle$, in other words a coset $x\langle g \rangle$, which has order p. Let N be the order of x in G. Since

$$(x\langle g \rangle)^N = x^N \langle g \rangle = \langle g \rangle,$$

when we raise the coset $x\langle g \rangle$ to the power N we get the identity coset $\langle g \rangle$. Hence the order of the coset $x\langle g \rangle$, namely p, divides N. It follows that the cyclic group $\langle x \rangle$ has order N and p divides N, so, again by earlier results on cyclic groups, there exists an element of $\langle x \rangle$ of order p. Again, this gives an element of order p in G. □

Proof of (i) *of the Sylow theorem.* We must prove that, for every p dividing $\#(G)$, a p-Sylow subgroup P of G exists. As in the proof of Cauchy's

theorem, the proof will be by complete induction on $\#(G)$ and the statement is vacuous if p does not divide $\#(G)$. As in the statement of the Sylow theorem, write $\#(G) = p^r m$; we are looking for a subgroup P of order p^r, or equivalently such that $(G : P) = m$. Note that, if $H \leq G$ and $\#(H) = p^r m'$, then a p-Sylow subgroup for H will also be a p-Sylow subgroup for G.

Case I: p divides $\#(Z(G))$. In this case, by Cauchy's theorem, there exists an element $x \in Z(G)$ of order p, since $Z(G)$ is abelian. Since $\langle x \rangle \leq Z(G)$, $\langle x \rangle$ is a normal subgroup of G of order p, and hence $G/\langle x \rangle$ is a group of order $p^{r-1}m$. If $r = 1$, then $\langle x \rangle$ is a subgroup of G of order p, hence is a p-Sylow subgroup of G. If $r > 1$, then p divides the order of $G/\langle x \rangle$. By induction, there exists a p-Sylow subgroup P' of $G/\langle x \rangle$. The quotient homomorphism $\pi \colon G \to G/\langle x \rangle$ is surjective, and we take $P = \pi^{-1}(P') \leq G$. By Lemma 2.1, $(G : P) = (G/\langle x \rangle : P') = m$. Hence $\#(P) = p^r$ and P is a p-Sylow subgroup of G.

Case II: p does not divide $\#(Z(G))$. In this case, we consider the class equation:

$$\#(G) = \#(Z(G)) + \sum_i \#(C_G(x_i)) = \#(Z(G)) + \sum_i (G : Z_G(x_i)).$$

Then, since p divides $\#(G)$ but p does not divide $\#(Z(G))$, there must exist some i such that p does not divide $(G : Z_G(x_i))$. Thus, $Z_G(x_i)$ is a proper subgroup of G, since $(G : Z_G(x_i)) > 1$, and p does not divide $(G : Z_G(x_i))$. Since

$$(G : Z_G(x_i)) = \frac{\#(G)}{\#(Z_G(x_i))} = \frac{p^r m}{\#(Z_G(x_i))},$$

the order of $Z_G(x_i)$ is of the form $p^r m'$ with $m' < m$. By the inductive hypothesis, there exists a p-Sylow subgroup P of $Z_G(x_i)$, in other words a subgroup P of $Z_G(x_i)$ of order p^r. But then P is a p-Sylow subgroup of G.

Before we prove the remaining statements of the Sylow theorem, we make some general remarks. Let G be a group and let H and K be two subgroups of G. Then G acts transitively on $X = G/K$, the set of left cosets of K. In particular, there are no one element orbits unless G/K is a single element, i.e. unless $G = K$. Put another way, if K is a proper subgroup of G, then $X^G = \emptyset$. However, we can also look at the action of the subgroup H on X. Here $h \in H$ acts in the usual way by left multiplication. In this case, it is certainly possible for there to be elements of the fixed set, and in fact we can describe these explicitly:

Lemma 2.3. *Let G be a group, let H and K be two subgroups of G, and let $X = G/K$, which we view as an H-set.*

(i) *The fixed set X^H is given by*

$$X^H = \{gK : H \subseteq gKg^{-1}\}.$$

(ii) *If $K = H$ and H is finite, the fixed set of H acting on G/H is*

$$X^H = \{gH : gHg^{-1} = H\}.$$

Here, we define $N_G(H)$, the *normalizer of H in G*, by

$$N_G(H) = \{g \in G : gHg^{-1} = H\}.$$

Then, $N_G(H) \leq G$, $H \leq N_G(H)$, and (ii) of the lemma states that $X^H = N_G(H)/H$.

Proof of Lemma 2.3. (i) The coset gK is fixed by $H \iff$ for all $h \in H$, $hgK = gK \iff$ for all $h \in H$, $g^{-1}hgK = K \iff$ for all $h \in H$, $g^{-1}hg \in K \iff$ for all $h \in H$, $h \in gKg^{-1} \iff H \subseteq gKg^{-1}$.
(ii) Applying (i) to the case $H = K$, we see that gH is fixed by $H \iff H \subseteq gHg^{-1} \iff H = gHg^{-1}$, since H and gHg^{-1} have the same number of elements. It is a straightforward exercise to show that $N_G(H)$ is a subgroup of G, and it clearly contains H. The description of X^H as $N_G(H)/H$ then follows from the fact that $X^H = \{gH : g \in N_G(H)\}$. □

Proof of (ii), (iii) *of the Sylow theorem.* Fix one p-Sylow subgroup P of G; we know one exists by the proof of (i). Let H be **any** subgroup of G of order p^s, $1 \leq s \leq r$. We will show that there exists a $g \in G$ such that $H \leq gPg^{-1}$. Since gPg^{-1} has order p^r, it is also a p-Sylow subgroup of G. This proves (iii). To see (ii), if H is itself a p-Sylow subgroup, then $H \leq gPg^{-1}$, but both of these subgroups have order p^r. Hence $H = gPg^{-1}$, so that H and P are conjugate. This proves (ii).

To find the element g above, consider the action of the group H on the set X of left cosets G/P. Then $\#(X) = \#(G/P) = (G : P) = m$. Since the order of H is a power of p,

$$\#(X^H) \equiv \#(X) = m \pmod{p}.$$

In particular, $X^H \neq \emptyset$ since m is not $\equiv 0 \bmod p$. By Lemma 2.3, if gP is a coset in the fixed set X^H, then $H \leq gPg^{-1}$ as claimed.

Proof of (iv) *of the Sylow theorem.* Referring to the proof of (ii), (iii) above, with $X = G/P$ as before, take $H = P$. By Lemma 2.3, $X^P = N_G(P)/P$, the set of left cosets gP of P such that $g \in N_G(P)$, where $N_G(P) \leq G$ is the normalizer of P. Moreover, since $\#(P)$ is a power of p, we have:

$$\#(X^P) = (N_G(P) : P) \equiv \#(X) = m \pmod{p}.$$

Now let Y be the set of all p-Sylow subgroups, viewed as a subset of $\mathcal{P}(G)$, the set of all subsets of G. The statement of (iv) is the statement that $\#(Y)$ divides $\#(G)$ and that $\#(Y) \equiv 1 \pmod{p}$. The group G acts on Y by conjugation, since if P is a p-Sylow subgroup, then so is $i_g(P) = gPg^{-1}$, for every $g \in G$. By (ii), the action of G on Y is transitive, since every two p-Sylow subgroups are conjugate. Moreover, the isotropy subgroup of a fixed p-Sylow subgroup P is by definition the normalizer $N_G(P)$. Thus,

$$\#(Y) = (G : N_G(P)) = \#(G)/\#(N_G(P)).$$

In particular, $\#(Y)$ divides $\#(G)$. Also, using the multiplicative property of the index, we have

$$\begin{aligned} m = (G : P) &= (G : N_G(P))(N_G(P) : P) \\ &= \#(Y)(N_G(P) : P) \equiv \#(Y) \cdot m \pmod{p}, \end{aligned}$$

by what we proved above. Since m and p are relatively prime, we can cancel m in the equation $m \equiv \#(Y) \cdot m \pmod{p}$, to obtain $\#(Y) \equiv 1 \pmod{p}$. This concludes the proof of (iv), and hence the proof of the Sylow theorem. □

Proposition 2.4. *Let G be a finite group of order p^r, where p is a prime number. Then for each $i \leq r$, there exists a subgroup of G of order p^i.*

Proof. The proof is by induction on r, the case $r = 1$ being vacuously true. Assuming the result for all groups of order p^t with $t < r$, we know that the center $Z(G)$ is nontrivial, hence there exists an element $g \in Z(G)$ of order p. Thus $\langle x \rangle$ is a subgroup of G of order p. Now let s be a natural number with $1 < s \leq r$. The subgroup $\langle x \rangle$ is a normal subgroup of G and the quotient group $G/\langle x \rangle$ has order p^{r-1}. For each s with $1 < s \leq r$, by the inductive hypothesis, there exists a subgroup J of $G/\langle x \rangle$ order p^{s-1}, or equivalently $(G/\langle x \rangle : J) = p^{r-s}$. Then if $\pi \colon G \to G/\langle x \rangle$ is the quotient homomorphism and $H = \pi^{-1}(J)$, we have: $(G : H) = (G/\langle x \rangle : J) = p^{r-s}$, and hence the order of H is p^s. This completes the inductive step and hence the proof. □

Corollary 2.5. *If G is a group of order $n = p^r m$, where $r > 0$ and p does not divide m, then G has a subgroup of order p^i for all $i \leq r$.*

Proof. This follows by applying the above proposition to a p-Sylow subgroup $P \leq G$. □

The case $i = r$ of the corollary is (i) of the Sylow Theorem and the case $i = 1$ is the general form of Cauchy's Theorem: if G is a finite group, not necessarily abelian, and $p|\#(G)$, then there exists an element of G of order p. However, it is possible to prove Cauchy's Theorem directly.

Warning. The statements (ii) and (iv) in the Sylow theorems only apply to p-Sylow subgroups, not necessarily to subgroups of G of order p^s with $s < r$. Thus it need not be true that every two such subgroups are conjugate, and there is no result in general concerning the number of such subgroups. For example, in a group of order $8 = 2^3$, every subgroup of order $4 = 2^2$ is normal, and hence, if every two such subgroups are conjugate, then there is a unique such subgroup. But $(\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ has a subgroup of order 4 isomorphic to $\mathbb{Z}/4\mathbb{Z}$ and another subgroup of order 4 isomorphic to $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$, so the two subgroups are not even isomorphic as groups.