

## SYLOW THEOREMS

Cauchy's theorem asserted that if  $p \mid |G|$  then  $G$  contains an element of  $g \in G$  order  $p$ . The subgroup  $H = \langle g \rangle < G$  cyclically generated by this element has order  $p$ , and so we have in this sense a partial converse to Lagrange's theorem. In fact, from the proof of Cauchy's theorem we saw there are at least  $p - 1$  such  $H$ 's.

Sylow's (first) theorem is a strengthening of Cauchy. It states that if  $p^k \parallel |G|$  (i.e.,  $p^k \mid |G|$  but  $p^{k+1} \nmid |G|$  — for example  $4 \parallel 12$ ) then  $G$  contains a subgroup  $P < G$  with  $|P| = p^k$ . We call  $P$  a Sylow  $p$ -subgroup.

**Example 1.** If  $|G| = 12$ , then  $G$  contains Sylow 2-subgroups and Sylow 3-subgroups. The Sylow 2-subgroups are all subgroups of  $G$  of order 3. The Sylow 3-subgroups are all subgroups of  $G$  of order 4. The group  $G$  might very well contain subgroups of order 2, but these are not Sylow subgroups.

**Example 2.** The Sylow 2-subgroups of  $S_3$  are  $\langle(12)\rangle, \langle(13)\rangle, \langle(23)\rangle$ . The Sylow 3-subgroup of  $S_3$  is  $\langle(123)\rangle$ .

**Theorem 1** (Sylow Theorems). Let  $G$  be a finite group and  $p^k \parallel |G|$ . Then

- (1)  $G$  has a Sylow  $p$ -subgroup  $P < G$ ;
- (2) Any two Sylow  $p$ -subgroups are conjugate;
- (3) Let  $n_p$  be the number of distinct Sylow  $p$ -subgroups, then  $n_p \equiv 1 \pmod{p}$  and  $n_p$  divides  $|G|/p^k$ .

**Example 3.** For  $G = S_3$  we have  $n_2 = 3$  and  $n_3 = 1$ , and we can explicitly check that

$$(13)(12)(13) = (23), \quad (12)(23)(12) = (13), \quad (23)(13)(23) = (12)$$

One of the major application of the Sylow theorems is to establish the existence of normal subgroups, which then rule out the existence of finite simple groups of given order. To this purpose the main lemma is the following.

**Lemma 1.** Let  $G$  be finite, and  $P$  be a Sylow  $p$ -subgroup of  $G$ . Then  $P \triangleleft G$  if and only if  $P$  is the unique Sylow  $p$ -subgroup of  $G$ .

*Proof.* If  $P \triangleleft G$ , then for any Sylow  $p$ -subgroup  $Q$ , we have  $Q = gPg^{-1} = P$  for some  $g \in G$ . Conversely, if  $P$  is the unique Sylow  $p$ -subgroup, then for any  $g \in G$ , the conjugate  $gPg^{-1}$  is also a Sylow  $p$ -subgroup, hence  $gPg^{-1} = P$ .  $\square$

We can now work out some examples of applications of Sylow.

**Proposition 1.** If  $|G| = pq$  then  $G$  is not simple.

*Proof.* Say  $p < q$ . By (3)  $n_q \mid p$  and  $n_q \equiv 1 \pmod{q}$ . Together these conditions force  $n_q = 1$ . But if there only one Sylow  $q$ -subgroup, it is normal. Hence  $G$  is not simple.  $\square$

**Proposition 2.** If  $|G| = p^2q$  then  $G$  is not simple.

*Proof.* Suppose  $|G| = p^2q$  with  $p > q$ . Then  $n_p \mid q$  and  $n_p \equiv 1 \pmod{p}$ , so  $n_p = 1$ . But if there only one Sylow  $p$ -subgroup, it is normal. Hence  $G$  is not simple.

Suppose  $|G| = p^2q$  with  $p < q$ . Then  $n_q \mid p^2$  and  $n_q \equiv 1 \pmod{q}$ , so  $n_q$  is 1 or  $p^2$ . If it is 1, then the Sylow  $q$ -subgroup is normal and  $G$  is not simple.

So let's assume there are  $p^2$  Sylow  $q$ -subgroups. Each such Sylow subgroup contains  $q - 1$  nonidentity element. If the different subgroups don't have common elements, that is **if for  $Q, Q'$  Sylow  $q$  subgroups, we have  $Q \cap Q' = \{e\}$** , then their union contains  $p^2(q - 1)$  elements. We know there exists at least one Sylow  $p$ -subgroup, call it  $P$ . This group has  $p^2 - 1$  nonidentity elements. **If Sylow  $p$ -subgroups and Sylow  $q$ -subgroups have trivial intersection, i.e.,  $P \cap Q = \{e\}$**  then we already have a total of

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

nonidentity elements in  $G$ . Since  $|G| = p^2q$ , this accounts for all nonidentity elements in  $G$  and there is no more space for a second, distinct, Sylow  $p$ -subgroup. Hence  $n_p = 1$  and  $P \triangleleft G$ .

We need to check the claims in boldface. First, we claim that if  $P$  is a Sylow  $p$ -subgroup and  $Q$  is a Sylow  $q$ -subgroup then  $P \cap Q = \{e\}$ . This is because  $P \cap Q$  is a subgroup of both  $P$  and  $Q$ . By Lagrange,  $|P \cap Q|$  must divide both  $|P|, |Q|$ , and hence their greatest common divisor. But here this is 1, and so  $P \cap Q = \{e\}$ .

Second, we claim that if  $|Q| = |Q'| = q$  then either  $Q = Q'$  or  $Q \cap Q' = \{e\}$ . This follows since  $|Q \cap Q'| \mid |Q| = |Q'| = q$ . □