

15 Sylow Theorems

Suppose that G is a finite group of order $|G| = n = p_1^{e_1} \cdots p_k^{e_k}$. We saw in the last section that, if G is abelian, then

$$G = P_1 \times P_2 \times \cdots \times P_k$$

where P_i is a group of order $p_i^{e_i}$ given by the formula:

$$P_i = \{g \in G \mid o(g) \text{ is a power of } p_i\}.$$

Note that P_i contains every p_i -subgroup of G . (Why?)

Now we go to the nonabelian case. We will take a fixed prime p and assume that

$$|G| = n = p^k m$$

where p does not divide m .

Theorem 15.1. *Suppose that $P \trianglelefteq G$ and $|P| = p^k$. Then*

$$P = \{g \in G \mid o(g) \text{ is a power of } p\}.$$

In words: P contains every element of G of p -power order.

Proof. Call the set on the right side S . So we have to prove that $P = S$.

($P \subseteq S$) If $g \in P$ then $o(g) \mid |P| = p^k$ so $o(g) = p^j$ for some $j \leq k$. So $g \in S$.

($S \subseteq P$) Suppose that $g \in S$. Let $Q = \langle g \rangle$. Then $|Q| = o(g) = p^j$. By the second isomorphism theorem, $PQ \leq G$ and

$$m = |G : P| = |G : PQ| \cdot |PQ : P|.$$

Since $p \nmid m$, p does not divide $|PQ : P| = |Q : P \cap Q|$. But this number divides $|Q| = p^j$ so it must be a power of p . So

$$|PQ : P| = |Q : P \cap Q| = 1.$$

In other words, $Q = P \cap Q$ which gives $Q \subseteq P$. So $g \in P$ which shows that $S \subseteq P$. \square

Definition 15.2. A *Sylow p -subgroup* of a group G is defined to be a maximal p -subgroup of G .¹ (P *maximal* means there is no other p -subgroup Q of G so that $P \subsetneq Q \leq G$.)

Now we do group actions. Let X be the set of all p -subgroups of G . Then $P \in X$. G acts on X by conjugation:

$$\alpha_g(P) = gPg^{-1}.$$

Recall that $P \trianglelefteq G$ if $gPg^{-1} = P$ for every $g \in G$.

¹By Zorn's Lemma even infinite groups have maximal p -subgroups. So every group has at least one Sylow p -subgroup.

Definition 15.3. The stabilizer of P under the conjugation action is called the *normalizer* of P in G

$$N_G(P) := \{g \in G \mid gPg^{-1} = P\}.$$

Note that

$$P \trianglelefteq N_G(P)$$

by definition.

Example 15.4. Take $G = S_4$. Then $n = |S_4| = 4! = 24 = 8 \cdot 3$. The Klein subgroup is normal

$$K = \{(12)(34), (13)(24), (14)(23), e\} \trianglelefteq G$$

So

$$N_{S_4}(K) = S_4.$$

Let $H = \langle (12) \rangle = \{e, (12)\} \leq S_4$ and let $P = KH$. Then

$$|P| = \frac{|K||H|}{|K \cap H|} = \frac{2 \cdot 4}{1} = 8$$

so P is a Sylow p -subgroup of S_4 . But P cannot be normal since S_4 has 16 elements of 2-power order. (There are 6 four-cycles, 6 two-cycles (transpositions) and 3 elements of cycle type $(ab)(cd)$. Plus the identity makes $6 + 6 + 3 + 1 = 16$.) But

$$|S_4 : P| = 3 = |S_4 : N_{S_4}(P)| \cdot |N_{S_4}(P) : P|$$

So we must have $P = N_{S_4}(P)$. We say that P is *self-normalizing*.

G acts on $X =$ the set of p -subgroups of G . The orbit of $P \in X$ is the set of all conjugates of P . We have a formula for the number of elements in the orbit:

$$r = |O(P)| = |G : G_P| = |G : N_G(P)|.$$

This proves:

Lemma 15.5. *The index of the normalizer of P is equal to the number of conjugates of P .*

Lemma 15.6. (a) *Every conjugate of P is also a Sylow p -subgroup.*

(b) *p does not divide $s = |N_G(P)/P|$.*

Proof. (a) This says that gPg^{-1} is a maximal p -subgroup. To prove this, suppose not. Then

$$\begin{aligned} gPg^{-1} &\not\leq Q \\ \Rightarrow P &\not\leq g^{-1}Qg \end{aligned}$$

which contradicts the maximality of P .

(b) Suppose that p divides $|N_G(P)/P|$. Then Cauchy tells us that the quotient group $N_G(P)/P$ has an element x of order p . This generates a subgroup $\langle x \rangle$ of order p . The Correspondence Theorem tells us that $\langle x \rangle$ corresponds to a subgroup Q with $P \leq Q \leq N_G(P)$ and $|Q : P| = |\langle x \rangle| = p$. But then Q has order p^{k+1} contradicting the maximality of P . \square

Example 15.7. Take $G = S_5$ and $P = \langle (12345) \rangle$. There are 24 five-cycles in S_5 which form 6 Sylow 5-subgroups (each has 4 five-cycles). Therefore,

$$r = 6 = |S_5 : N_{S_5}(P)| \Rightarrow |N_{S_5}(P)| = \frac{120}{6} = 20$$

So

$$s = |N_{S_5}(P)/P| = \frac{20}{5} = 4.$$

The lemma says that $p = 5$ does not divide $s = 4$.

Lemma 15.8. $P = \{g \in N_G(P) \mid o(g) \text{ is a power of } p\}$.

Proof. This follows from Theorem 15.1. (Lemma 15.6 tells us that P satisfies the conditions of Theorem 15.1.) \square

Theorem 15.9 (Sylow). (1) *Every Sylow p -subgroup of G is conjugate to P .*

(2) *The number of Sylow p -subgroups of G is congruent to 1 modulo p :*

$$r \equiv 1 \pmod{p}$$

$$r := |G : N_G(P)| =_{15.5} \# \text{conjugates of } P =_{(1)} \# \text{Sylow } p\text{-subgroups of } G.$$

Remark 15.10. (a) In the first example $r = 3$ is congruent to 1 modulo $p = 2$. In the second example $r = 6$ which is congruent to 1 modulo $p = 5$.

(b) Note that the index of P is a product of two numbers

$$|G : P| = |G : N_G(P)| \cdot |N_G(P) : P| = rs$$

Lemma 15.6 says that p does not divide s and (2) in the Sylow theorem says that p does not divide r . So p doesn't divide the index of P so $|P| = p^k$ and $|G : P| = m$.

Corollary 15.11 (Sylow). *If $|G| = n = p^k m$ where $p \nmid m$ then G contains a subgroup of order p^k and every p -subgroup of G is contained in a p -subgroup of order p^k . Consequently, the Sylow p -subgroups of G are the ones of order p^k .*

Proof. Every p -subgroup of G is contained in a maximal one (just take the biggest one containing it). This is Sylow by Rotman's definition. Remark (b) tells us that Sylow subgroups have order p^k . \square

Proof of the Sylow Theorems. By Lemma 15.5, $r = |G : N_G(P)|$ counts the number of conjugates of P which also counts the size of the orbit of $P = P_1$:

$$Y = O(P) = \{P_1, P_2, \dots, P_r\}$$

Let Q be any Sylow p -subgroup of G . Then we have to show that Q is equal to one of the elements P_i in the set Y . We will consider what happens if $Q = P_i$ and also what happens if Q is not one of the P_i 's.

In either case, the group Q acts on the set Y by conjugation. So Y breaks up into a disjoint union of smaller orbits.

$$Y = \coprod Q\text{-orbits.}$$

(Y is one G -orbit but many Q -orbits.) The size of each Q -orbit must be a power of p (since it is equal to the index of its stabilizer=normalizer in Q). Suppose that one of these Q -orbits has only one element: $\{P_i\}$. Then every element of Q normalizes P_i so

$$Q \leq N_G(P_i).$$

But P_i contains all elements of $N_G(P_i)$ of p -power order (Lemma 15.8), so $Q \leq P_i$. Since Q is maximal, $Q = P_i$.

Case 1. $Q \notin Y$. Then this doesn't happen, i.e., none of the Q -orbits can have size equal to one. This implies that the size of each orbit is a nontrivial power of p so p divides r . (!??)

Case 2 $Q \in Y$, say $Q = P_r$. In that case, Q cannot be equal to any of the other elements ($Q \neq P_i$ for $i < r$). So $\{P_r\}$ is the only one-element orbit. The other orbits have nontrivial p -power size so

$$r \equiv 1 \pmod{p}$$

In particular $p \nmid r$.

To summarize: We chose a Sylow p -subgroup Q of G . There are two cases. Either Q is in Y (Case 2) or it isn't (Case 1). In one case p divides r . In the other case p doesn't divide r . But r is the number of conjugates of P . It has nothing to do with Q !!! So these two cases cannot both happen. Either all Sylow p -subgroups lie in Y (Case 2) or none of them lie in Y (Case 1).

But the members of Y are all Sylow p -subgroups. The conclusion is: Case 1 is not possible. All Sylow p -subgroups lie in Y and are thus conjugate to P and $r \equiv 1 \pmod{p}$. These are the Sylow Theorems. \square