

MATH 120: THE SYLOW THEOREMS

Sylow's first theorem (Sylow I) states that if a prime p divides the order of a group, then the group has at least one Sylow p -subgroup. We proved Sylow I in class by induction on the size of the group, just as in the text.

Sylow II gives more detailed information about the Sylow p -subgroups. It is proved by examining how p -subgroups act by conjugation.

We first prove a general proposition about actions by p -groups. Let p be a prime number. Recall that a p -group is a group of order p^n for some $n \geq 1$.

Proposition 1. *Consider a group action of a p -group H on a finite set X . Then the number of elements of X is congruent mod p to the number of points in X that are fixed by H :*

$$|X| \sim |\{x \in X : h(x) = x \text{ for all } h \in H\}| \pmod{p}.$$

Proof. It suffices to prove it for a single orbit, since the size of X is the sum of the sizes of the orbits, and the number of fixed points is the sum of the number of fixed points in the various orbits.

Case 1: The orbit contains a point x fixed by H . Then the whole orbit consists just of that one point. In this case, the size of the orbit equals the number of fixed points in the orbit (they are both 1.)

Case 2: The orbit contains no fixed points.

In this case, the number of fixed points in the orbit is 0, so we must show that the size of the orbit is congruent to 0 mod p . Let x be a point in the orbit. Then the stabilizer of x , i.e., $\{h \in H : h \cdot x = x\}$, is not all of H . Thus if $|H| = p^n$, then (by Lagrange) the stabilizer of x has order p^j for some $j < n$.

Recall (see prop 2 on page 116) that

$$|\text{orbit}(x)| = |H|/|\text{stab}_H(x)| = p^{n-j}.$$

Since $j < n$, this is congruent to 0 mod p . \square

Corollary. *Suppose H_1 and H_2 are p -groups that both act on a finite set X . Then the number of points fixed by H_1 is congruent mod p to the number of points fixed by H_2 .*

Proof. By the theorem, they are both congruent mod p to $|X|$.

Before we prove Sylow II, we need one more proposition about p -groups:

Proposition 2. *Let P be a Sylow p -subgroup of G and let $H \leq G$ be any other p -subgroup. Either $H \leq P$ or H has an element h such that $hPh^{-1} \neq P$.*

Proof. Let $|G| = p^\alpha m$, where p does not divide m . Suppose $hPh^{-1} = P$ for all $h \in H$. Then $hP = Ph$ for all $h \in H$, so $HP = PH$, which implies that PH is a subgroup of G . Also

$$|PH| = \frac{|P||H|}{|P \cap H|} = |P|.$$

Since $|P|$ and $|H|$ are both powers of p , so must $|PH|$ be a power of p . Thus PH is a p -subgroup of G and it contains P . Since P has the maximum number of elements of any p -subgroup, $PH = P$. Since PH contains H , this implies that $H \leq P$. \square

This proposition may be restated in the following form (which is more convenient for the proof of Sylow II):

Proposition 2'. *Let P be a Sylow p -subgroup of G , and let H be any p -subgroup of G . Let H act on subsets of G by conjugation:*

$$h \cdot S = hSh^{-1}$$

Then P is a fixed point of this action if and only if $H \leq P$.

Theorem (Sylow II). *Let G be a finite group and let p be a prime number that divides $|G|$. Then:*

- (1) *Every p -subgroup is contained in a Sylow p -subgroup.*
- (2) *The p -Sylow subgroups are all conjugate to each other.*
- (3) *The number of p -Sylow subgroups is congruent to 1 mod p .*
- (4) *The number of p -Sylow subgroups divides $m = |G|/p^a$, where p^a is the largest power of p that divides $|G|$.*

Proof of theorem. We know (by Sylow I) that G has a Sylow p -subgroup P . Let $X = \{gPg^{-1} : g \in G\}$ be the set of its conjugates.

Let P act on X by conjugation:

$$g \cdot P' = gP'g^{-1} \quad (g \in P, \quad P' \in X).$$

By proposition 2', $P' \in X$ is a fixed point of this action if and only if $P \leq P'$. Since P and P' have the same size, $P \leq P'$ if and only if $P = P'$.

Thus this action has exactly one fixed point in X , namely P . Hence by proposition 1,

$$(*) \quad |X| \sim 1 \pmod{p}.$$

Now let H be any other p -subgroup of G and let H act on X by conjugation. Then by (*) and proposition 1,

$$1 \sim |X| \sim \text{the number of elements of } X \text{ fixed by } Q$$

modulo p . Thus at least one element P' of X must be fixed by the H -action. By proposition 2', this means $H \leq P'$.

We have proved: if H is a p -subgroup, then H is contained in one of the conjugates of P . This proves statement (1) of the theorem.

Now let H be a Sylow p -subgroup. Then (as was just shown) H is contained in one of the conjugates P' of P . But H and P' have the same size, so $H = P'$. This proves (2).

We have shown that X is the set of all Sylow p -subgroups. Thus by (*), the number of Sylow p -subgroups is congruent to 1 mod p . This proves (3).

Finally, consider the action of all of G on X by conjugation. Now X is, by definition, the orbit of P under this action. Thus (by proposition 2 on page 116)

$$(**) \quad |X| = \frac{|G|}{|\text{stab}_G(P)|} = \frac{p^a m}{|\text{stab}_G(P)|}.$$

There are two ways to see that p divides m :

- (1) By (**), $|X|$ divides $p^a m$. Since $|X| \equiv 1 \pmod{p}$, $|X|$ is relatively prime to p . Thus $|X|$ must divide m .
- (2) Alternatively, note that $\text{stab}_G(P)$ contains P , so by Lagrange's theorem, $|\text{stab}_G(P)|$ must be a multiple of $|P|$, i.e., of p^a . That is, $|\text{stab}_G(P)| = p^a k$ for some k . But then by (**), $|X| = m/k$, so $|X|$ divides m . \square