Sylow's Theorems

Here are two different ways of proving Sylow's theorems. The first set of proofs is rather 'magical', picking a different clever action that works for each part. The second set of proofs is rather more 'natural', using the same familiar action for all three parts.

Let G be a group of order $p^a m$, where p is prime and $(p, m) = 1$.

Sylow 1. G has a Sylow p-subgroup – that is, a subgroup of order p^a.

Let X be the set of all subsets of G of size p^a, and let G act on X by left multiplication: for g in G and $\{x_1, \ldots x_{p^a}\}$ in X, we let $g * \{x_1, \ldots x_{p^a}\} = \{gx_1, \ldots gx_{p^a}\}$.

We'll show that (a) any orbit has size at least m, and (b) there is an orbit of size dividing m. Such an orbit then has size equal to m, and by Orbit-Stabiliser the corresponding stabiliser has size p^a, which is our required Sylow subgroup.

(a) Pick an orbit $\mathcal{O}$, let S be a member of $\mathcal{O}$, let $s \in S$, and let $g \in G$. Then $gs^{-1} * A$ contains g. So the sets in $\mathrm{orb}(S)$ cover all of G, and hence there are at least $|G|/|S| = m$ sets in $\mathrm{orb}(S)$.

(b) We have

$$|X| = \binom{p^a m}{p^a} = \left(\frac{p^a m}{p^a}\right)\left(\frac{p^a m - 1}{p^a - 1}\right) \cdots \left(\frac{p^a m - p^a + 1}{1}\right).$$

For each factor in this product, the same power of p divides the numerator and denominator, and so all factors of p cancel. Hence $|X|$ is coprime to p.

Then, when we partition X up into orbits, at least one orbit has size coprime to p (for if they are all multiples of p, then so is $|X|$, but it's not). By Orbit-Stabiliser the size of this orbit divides $|G|$. And if a number divides $p^a m$ and is coprime to p, then it divides m.

Combining (a) and (b), we have proved Sylow 1.

Sylow 2. Any two Sylow p-subgroups are conjugate.

Let P be the Sylow p-subgroup we found above, and let X be the set of left cosets of P. Let Q be some other Sylow p-subgroup, and let Q act on X by left multiplication: $q * gP = qgP$.

The orbits have sizes dividing $|Q| = p^a$, so they are powers of p, and since $|X| = |G|/|P| = m$ is coprime to p, there must be some orbit $\{gP\}$ of size 1.

Then, for all $q \in Q$ we have $qgP = gP$, so $g^{-1}qgP = P$, so $g^{-1}qg \in P$, and so $q \in gPg^{-1}$. Hence $Q \leqslant gPg^{-1}$ and so by sizes we have $Q = gPg^{-1}$, as required.

Sylow 3. The number n_p of Sylow p-subgroups satisfies $n_p \equiv 1 \bmod p$ and n_p divides m.

Let P be the Sylow p-subgroup we found above, and let X be the set of Sylow p-subgroups of G. Let P act on X by conjugation: $g * Q = gQg^{-1}$.

By Orbit-Stabiliser, the orbits have size dividing $|P|$ and hence are powers of p, and we know that $\{P\}$ is an orbit of size 1. If $\{Q\}$ is another orbit of size 1, then $gQg^{-1} = Q$ for all $g \in P$, and so $P \leqslant N(Q)$. But $N(Q)$ has Q as its unique Sylow p-subgroup (any two are conjugate by Sylow 2, and Q is normal in $N(Q)$), so $P = Q$ and hence $\{P\}$ is in fact the only orbit of size 1.

Hence $n_p \equiv 1 \bmod p$.

Now, let G act on X by conjugation. Sylow 2 tells us that there is only one orbit, which has size n_p. By the Orbit-Stabiliser theorem, we have that n_p divides $|G|$. Since n_p is coprime to p, we have that n_p divides m.

Now a second set of proofs, where everything is a bit more natural and motivated.

Sylow 1. G has a Sylow p-subgroup – that is, a subgroup of order p^a.

Let P be a maximal p-subgroup of G. Our aim is to show that $|P| = p^a$, or equivalently that $|G|/|P|$ is not a multiple of p. Writing N for the normaliser of P in G, we have

$$\frac{|G|}{|P|} = \frac{|G|}{|N|} \times \frac{|N|}{|P|}.$$

This is useful because both factors have a meaning:

- via orbit-stabiliser on the conjugation action of G on its subgroups, we have that $|G|/|N|$ is the number of conjugates of P
- since P is normal in N, we have $|N|/|P| = |N/P|$, the size of the quotient group.

We'll show that neither factor is a multiple of p.

- Let $\pi : N \to N/P$ be the quotient map.

  If p divides $|N/P|$, then Cauchy's theorem gives us an element $x \in N/P$ of order p. Then $\pi^{-1}(\langle x \rangle)$ is a subgroup of G of order $p|P|$, contradicting P being maximal.

- Let X be the set of conjugates of P, i.e. $X = \{gPg^{-1} : g \in G\}$. Then $|G|/|N| = |X|$.

  Let P act on X by conjugation. Since $|P|$ is a power of p, each orbit has size a power of p. We have at least one orbit of size 1, namely $\{P\}$. We'll show that this is the only orbit of size 1, and then we are done, with $|X| \equiv 1 \bmod p$ and hence $|G|/|N|$ coprime to p.

  Suppose that $\{gPg^{-1}\}$ is an orbit of size 1. Then P fixes gPg^{-1} in the action – i.e., P normalises gPg^{-1}. So, for all $h \in P$ we have

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

  Rearranging this, we have

  $$P = (g^{-1}hg)P(g^{-1}hg)^{-1}$$

  which says that $g^{-1}hg$ normalises P. This is true for all $h \in P$, and so $g^{-1}Pg \subset N$.

  We can therefore restrict $\pi : N \to N/P$ to $g^{-1}Pg$. The image $\pi(g^{-1}Pg)$ is a subgroup of N/P and so has size dividing $|N/P|$ which has no factors of p. But the size of the image also divides $|g^{-1}Pg|$ which is a power of p. Hence the image has size 1 and thus is $\{e\}$.

  Therefore, we have $g^{-1}Pg \subset P$, and so $g^{-1}Pg = P$, and hence $P = gPg^{-1}$, as required.

Sylow 2. Any two Sylow p-subgroups are conjugate.

Let Q be another Sylow p-subgroup of G. We want $Q = gPg^{-1}$ for some g.

Let Q act on X by conjugation. The orbits have size a power of p, and there is an orbit of size 1 since $|X| \equiv 1 \bmod p$. Let this orbit be $\{gPg^{-1}\}$.

So Q normalises gPg^{-1}, and then $g^{-1}Qg$ normalises P (as above). Then $g^{-1}Qg \subset N$, and $\pi(g^{-1}Qg) = \{e\}$ (as above). So $g^{-1}Qg \subset P$, so $g^{-1}Qg = P$, and hence $Q = gPg^{-1}$, as required.

Sylow 3. The number of Sylow p-subgroups is $1 \pmod p$ and divides m.

This is now immediate. We showed that the number of conjugates of P is congruent to $1 \pmod p$, and then we showed that all Sylow subgroups were conjugate to P. Hence $n_p \equiv 1 \pmod p$. And finally, n_p divides m by orbit-stabiliser, since it divides $|G|$ and is coprime to p.