

I will try to present a quick summary of the Sylow theorems. Probably Dylan told you nearly all of this.

Sylow subgroups exist.

We proved this by a method that is not so well known but seems natural to me: prove the theorem by inspection for a class of “standard” groups and then embed arbitrary groups into one of the standard ones.

The key statement is this one: If H is a subgroup of G and P is a p -Sylow subgroup of G , then there is a conjugate P' of P in G so that $P' \cap H$ is a p -Sylow subgroup of H .

Corollary: All p -subgroups of G are contained in a conjugate of P .

For the proof, we take H to be a p -group inside G . Then $H \cap P'$ must be H , so that $H \subseteq P'$.

Corollary: All p -Sylows of G are conjugate.

We take H to be a p -Sylow. Since $H \subseteq P'$, $H = P'$.

Corollary: Each p -subgroup of G is contained in a p -Sylow of G . This is true because $H \subseteq P'$ and P' is a p -Sylow.

Because all p -Sylow subgroups of G are conjugate, we have: if P is a p -Sylow of G , then the set of p -Sylows is $G/N(P)$, where N stands for “normalizer.”

This is clear because the p -Sylows are the conjugates of P . In particular, the number of p -Sylows is $(G : N(P))$, a divisor of the prime-to- p part of $\#(G)$.

Next: When P acts on the set of p -Sylows by conjugation, P fixes itself but fixes no other p -Sylow. Said differently: a p -Sylow cannot normalize another p -Sylow.

The proof is that if P normalizes P' , then PP' is a p -group containing P and must therefore be P .

The upshot is the famous theorem to the effect that the number of p -Sylows is congruent to 1 mod p .

Recall that if a p -group H acts on a finite set S , then

$$\#(S) \equiv \#(S^H) \pmod{p}.$$

Here, S^H is the set of points of S that are fixed by H . The reason is that the orbits of H acting on S have p -power order and are therefore either singleton sets or sets of size divisible by p .

To derive the famous theorem, we take $H = P$ and S to be the set of p -Sylows of G . Because P normalizes only itself, there is a unique singleton set, so that $\#(S^H) = 1$.

A finite group is *simple* if it's non-trivial and has no proper normal subgroups other than $\{e\}$.

I think that I assigned the exercise in Lang to check that there are no non-abelian simple groups of order < 60 . (Recall that a finite abelian group is *simple* if and only if it has prime order.)

For $n \geq 5$, the group \mathbf{A}_n is simple. The proofs of this fact that I know are totally unenlightening, so we pretend that it has been carried out in Math 113 (or the equivalent course elsewhere).

A well-known theorem is that a finite simple group of order 60 is isomorphic to A_5 . There are lots of proofs of this fact in the literature (and on the web). I will present the proof that's in Dummit–Foote. This is a good proof because it's simple and efficient.

I will present the proof on the white board, but the proof is summarized in this .pdf, which you can download.

Let G be simple of order 60. Suppose that H is a proper subgroup of G and let $n = (G : H)$. The action of G on G/H defines a non-trivial permutation

$$\pi : G \rightarrow \text{Perm}(G/H) \approx \mathbf{S}_n.$$

The kernel of π is a proper normal subgroup of G and thus must be $\{e\}$. Hence

$$G \hookrightarrow \mathbf{S}_n.$$

In fact, we have

$$G \hookrightarrow \mathbf{A}_n;$$

otherwise, we could intersect the image of G with \mathbf{A}_n and get a subgroup of G of index 2.

Thus $n \geq 5$. Also, if $n = 5$, we have $G \approx \mathbf{A}_5$ as desired.

Accordingly, the goal will be to exhibit a subgroup of G of order 12 (i.e., of index 5). This is connected up with the 2-Sylow subgroups of G .

The number of 2-Sylow subgroups of G divides 15 (and is 1 mod 2, but that's obvious anyway). The number can't be 1 because then the unique 2-Sylow would be normal. The number of 2-Sylows is $(G : N)$, where N is the normalizer of one of the 2-Sylows. This index can't be 3 because then we'd get an embedding of G into \mathbf{S}_3 by the discussion above; that can't work because of orders.

If the index is 5, then we get $G \approx \mathbf{A}_5$ and are completely happy.

Hence we are left with the possibility that the index is 15. We assume that this is the case and press on.

We have to rule out the following crazy possibility: if P and Q are two distinct 2-Sylows, then $P \cap Q = \{e\}$. We prove that this is impossible by contradiction. If it's really true, then the number of elements of G with 2-power order is $1 + 15(4 - 1) = 46$.

On the other hand, it's obvious from the Sylow theorems that the number of 5-Sylows is 6. Hence the number of elements of order 5 is $6 \cdot 4 = 24$. We're in trouble because $46 + 24 = 70 > 60$.

Conclusion: there exist two different 2-Sylows P and Q with $P \cap Q$ of order 2.

Let M be the normalizer of $P \cap Q$. This group contains both P and Q because P and Q are abelian. Hence the order of M is divisible by 4 but is bigger than 4 (since P and Q are both in M and are distinct group of order 4). The order of M could thus a priori be 60, 20 or 12.

Equivalently, the index of M in G is one of 1, 3, 5. Index 1 means that $M = G$, so that $P \cap Q$ is a non-trivial normal subgroup of G (which is impossible because G is simple). Index 3 is impossible (too small by our discussion). Index 5 is what we wanted to achieve, so it's QED and we celebrate.

Exercise: calculate the number of 2-Sylow subgroups of \mathbf{A}_5 . Is it 15, or is it 5?