Proof that p-Sylows exist

In this document, I outline a proof of the existence of p-Sylow subgroups in a finite group (whose order is divisible by p, which is taken to be a prime number). I learned this proof from notes of a course that J-P. Serre gave in Paris around 1980.

There are two independent steps to the proof. One step (let's say the first) is to show that H has p-Sylows if H is a subgroup of G and if G has p-Sylows. The other is to show that every finite subgroup can be embedded in a group that has p-Sylows.

For the first step, let G be a finite group and let H and P be subgroups of G such that P is a p-group and such that the index $(G : P)$ is prime to p. (Thus P is a p-Sylow subgroup of G if G has order divisible by p. We don't assume that G has order divisible by p, but the assertion to be proved is trivial if not.)

Lemma. *In the situation just described, there is a conjugate gPg^{-1} of P so that the intersection $H \cap (gPg^{-1})$ is a p-Sylow subgroup of H.*

Here we use the expression "p-Sylow subgroup" in a slightly generalized sense: it's a subgroup of p-power order and prime-to-p index. We don't assume that the ambient group (H in this case) actually has order divisible by p.

The lemma is proved by introducing the (left) action of G on the space G/P of cosets of the form gP. The stabilizer in G of gP is gPg^{-1}. If we restrict the action of G to an action of its subgroup H, then the stabilizer of gP in H is the intersection $H \cap (gPg^{-1})$. This intersection is a p-group because it's a subgroup of gPg^{-1}; it's thus a p-Sylow subgroup of H if and only if its index is prime to p. Now, as we know, this index is alternatively the size of the orbit of gP under the action of H. The punchline is this: Since G/P has size prime to p (its size being the index $(G : P)$), there must be at least one orbit whose size is prime to p. This is exactly the assertion of the lemma.

Corollary. *All p-Sylow subgroups of G are conjugate.*

This Corollary is derived from the lemma by considering the case where H is a p-Sylow subgroup of G. The lemma says that there is a g for which $H \cap (gPg^{-1})$ is a p-Sylow subgroup of H. Since H is a p-group, we have $H \cap (gPg^{-1}) = H$, i.e., $H \subseteq gPg^{-1}$. Since H and P have the same order, we deduce that $H = gPg^{-1}$.

The point, somehow, is that the standard proof of the Corollary proves the Lemma as well. The lemma is quite powerful because it has the "first step" of our proof as an immediate consequence. Said otherwise: in the statement of the lemma we did not know a priori that H has a p-Sylow subgroup. The conclusion of the lemma tells us that H does indeed have a p-Sylow subgroup.

For the second step, we start with a finite group H and seek a "bigger" group G containing H for which p-Sylow subgroups are known to exist. The nuts and bolts way to do this is first to embed H into S_n, where n is the order of H; that we can do this is "Cauchy's theorem." We then embed S_n into $\mathbf{GL}(n, \mathbf{F}_p)$, using "permutation matrices." A more intrinsic way to do the two embeddings at once is to consider the $\mathbf{F}_p$-vector space $V \approx \mathbf{F}_p^n$ of functions $\varphi : G \to \mathbf{F}_p$ and to replace $\mathbf{GL}(n, \mathbf{F}_p)$ by $\mathbf{GL}(V)$. We embed G into this latter group as follows: $g \in G$ maps to the automorphism taking $\varphi(x)$ to $\varphi(xg)$. Note that I've put g on the right side of x. You should check that this is the correct thing to do in order to get a homomorphism $G \to \mathbf{GL}(V)$; perhaps I've screwed up?

To finish, we need to check that $\mathbf{GL}(n, \mathbf{F}_p)$ has a p-Sylow subgroup. An easy linear algebra exercise is to calculate that the order of this group is the product

$$(p^n - 1)(p^n - p)(p^n - p^2) \cdots (p^n - p^{n-1}).$$

The p-part of this product is p^N, where $N = (n^2 - n)/2$. For P we take the group of upper-triangular matrices with 1's on the diagonal. This is a subgroup of G of order p^N, so it's a p-Sylow subgroup of $\mathbf{GL}(n, \mathbf{F}_p)$.