Notes on the Proof of the Sylow Theorems

1 The Theorems

We recall a result we saw two weeks ago.

Theorem 1.1 ***Cauchy's Theorem for Abelian Groups*** *Let A be a finite abelian group. If p is a prime number that divides its order, then A must have an element of order p.*

Theorem 1.2 ***Sylow's First Theorem*** *Let G be a finite group. Let p be a prime number such that its power by α is the largest power that will divide $|G|$. Then there exists at least one subgroup of order p^α. Such subgroups are called Sylow p-subgroups.*

Proof We divide the proof into two cases.
Case One: p divides the order of the center $Z(G)$ of G. By Cauchy's Theorem for abelian groups, $Z(G)$ must have an element of order p, say a. By induction, the quotient group $G/ < a >$ must have a subgroup P_0 of order $p^{\alpha-1}$. Then the pre-image of P_0 in $Z(G)$ is the desired subgroup of order p^α. (Note: in general, if S is any subset of a quotient group G/H, then the order of the pre-image of S is the product of its order with the order of the subgroup.)
Case Two: assume that p does not divide the order of the center of G. Write $|G|$ in terms of the "class equation:"

$$|G| = |Z(G)| + \sum |\text{Conj}(a)|,$$

where the sum is over all the distinct non-central conjugacy classes of G; that is, conjugacy class with more than one element. Since p fails to divide the order of the center, there must be at least one non-central conjugacy class, say $\text{Conj}(b)$, whose order is not divisible by p. Recall that $|\text{Conj}(b)| = [G : C_G(b)] = |G|/|C_G(b)|$. We observe immediately that p^α must divide the order of the subgroup $C_G(b)$. Again, by induction, G will have a Sylow p-subgroup. This ends the proof.

Corollary 1.1 *There is a subgroup Q of a Sylow p-subgroup P for every power of p that divides the order of the group G.*

Corollary 1.2 *If every element of a group is a power of a prime p, then the group is a p-group; that is, the order of the group is a power of p.*

Theorem 1.3 ***Sylow's Second Theorem*** *Let n_p be the number of Sylow p-subgroups of a finite group G. Then $n_p \equiv 1 \bmod p$.*

Proof We begin with a claim.
Claim: Let P be any Sylow p-subgroup. If $g \in G$ be a p-element and $gPg^{-1} = P$, then $g \in P$. To see this, consider the subgroup R generated by g and P. By assumption, $g \in N_G(P)$, so $R \leq N_G(P)$. Hence, P is a normal subgroup of R. We find $|R| = |R/P| \cdot |P|$. But $|R/P|$ is a cyclic group generated by the coset gP. Then gP is a p-element since g is. Hence $|R|$ is a power of p since all its elements are p-elements.
Let $\mathcal{S}_p$ be the set of all Sylow p-subgroups of G. Then G acts on this set by conjugation. Let $P, Q \in \mathcal{S}_p$ be two distinct subgroups. Then Q cannot be fixed under conjugation by all the elements of P because of the Claim.

Let $\mathcal{O}$ be the P-orbit of Q under conjugation. Then the size of the orbit must be divisible by p because of the order-stabilizer equation:

$$|\mathcal{O}| = \frac{|P|}{|\mathrm{Stab}_P(Q)|}.$$

Since $|P|$ is a power of p, the size of any orbit must be a power of p. The case $|\mathcal{O}| = p^0 = 1$ is ruled out since Q cannot be fixed by all the elements of P.
We find that the set of all Sylow p-subgroups is the union of P-orbits. There is only one orbit of order one, $\{P\}$, while the other orbits must have orders a positive power of p.
We conclude $n_p = |\mathcal{S}_p| \equiv 1 \bmod p$.

Remark: We want to emphasize a result from this proof. Let P be any Sylow p-subgroup. As above, we let P act on $\mathcal{S}_p$ by conjugation. Let S_0 be any P-invariant subset of $\mathcal{S}_p$, which means that is a disjoint union of P-orbits. Then $|S_0| \equiv 0 \bmod p$ if $P \notin S_0$; while $|S_0| \equiv 1 \bmod p$ if $P \in S_0$.

Theorem 1.4 *Any two Sylow p-subgroups are conjugate.*

PROOF Let P be any Sylow p-subgroup. Let S_0 be the set of all G-conjugates of P. Then S_0 is P-invariant and $P \in S_0$. By the above observation, $|S_0| \equiv 1 \bmod p$. If S_0 does not exhaust the set of all Sylow p-subgroups, choose one, say Q, not in S_0. Let S_1 be the set of all G-conjugates of Q. By the same reasoning as for S_0 with Q playing the role of P, we must have $|S_1| \equiv 1 \bmod p$. On the other hand, S_1 is P-invariant and $P \notin S_1$. By the above observation, $|S_1| \equiv 0 \bmod p$. Contradiction.

Corollary 1.3 *The number n_p of Sylow p-subgroups must divide $|G|/p^\alpha$.*

PROOF Recall that the number of conjugates of any subgroup H in a group G is given by

$$\#\text{conjugates} = \frac{|G|}{|N_G(H)|}$$

If H is a Sylow p-subgroup, then the order of its normalizer must be divisible by p^α since $H \leq N_G(H)$. But the number of all Sylow p-subgroups is just the number of conjugates of any one of them.

Theorem 1.5 *Any p-subgroup B is contained in a Sylow p-subgroup.*

PROOF Let B act on the space $\mathcal{S}_p$ by conjugation. Then the size of any B-orbit $\mathcal{O}$ must be a power of p, since the $|\mathcal{O}| = [G : N_G(B)]$. Since the size of $\mathcal{S}_p$ is not a power of p, there must be at least one B-orbit with one element, say P. But B must be a subgroup of P since the subgroup generated by B and P is a power of p, by the corollary to Sylow's First Theorem.

Theorem 1.6 *Any finite abelian group is a product of its Sylow p-subgroups.*

As a consequence of this last theorem, to classify the finite abelian groups, it is enough to understand their structure in the case that their order of a power of a prime. One can show that if $|A| = p^n$, then A is isomorphic to a group of the form $\mathbf{Z}_{n_1} \times \mathbf{Z}_{n_2} \times \cdot \mathbf{Z}_{n_k}$, where $n_1 \geq n_2 \geq \cdots \geq n_k$ and $n_1 + \cdots n_k = n$.