Definition .0.1

A Sylow p-subgroup is a subgroup of G of order p^n where $|G| = p^n m$ with $p \nmid m$.

Theorem .0.1

If G is a finite group, and $p^k \mid |G|$ where p is prime and $k > 0$ then G has a subgroup of order p^k. Furthermore

- Any two Sylow p-subgroups of G are conjugate.
- Any p-subgroup of G is contained in a Sylow p-subgroup of G.
- The # of Sylow p-subgroups divides $|G|$ and is $\equiv 1 \mod p$.

Proof. Say $p^k \mid |G|$ and write $|G| = p^n m$ for $p \nmid m$. The proof proceeds via acting on a clever set.

Let S be the set of subsets of G of size p^k. G acts on S by left multiplication.

$$g \cdot T = \{gt \mid t \in T\}.$$

Goal: Show there exists a $T \in T$ such that G_T has order p^k.

The first thing to notice is that this is the largest possible order of any stabilizer. Why? Well for any $t \in T \in S$, we know $G_T \cdot t \subseteq T$. Thus because $|G_T \cdot t| = |G_T|$ we have $|G_T| \leq |T| = p^k$.

Therefore by orbit-stabilizer we know

$$|\mathcal{O}_T| = \frac{|G|}{|G_T|}$$

this is divisible by p^{n-k}, and this is the smallest power of p dividing $|\mathcal{O}_T|$ (prime factorization). We want to show there exists T such that $|\mathcal{O}_T|$ is not divisible by p^{n-k+1}.

Consider the orbits $\mathcal{O}_T$ for varying T's. These form a partition of S. So we'll show $|S|$ is not divisible by p^{n-k+1}, and so we have to have some T so that $|\mathcal{O}_T|$ is not divisible by p^{n-k+1}. Thus $p^k \mid |G|_T$ and $|G_T| = p^k$.

Claim

The largest power of p dividing $|S|$ is p^{n-k}.

Well, we see that

$$\begin{aligned} |S| = \binom{|G|}{p^k} = \binom{p^n m}{p^k} &= \frac{(p^n m)(p^n m - 1)\cdots(p^n m - p^k + 1)}{p^k(p^k - 1)\cdots(p^k - p^k + 1)} \\ &= (p^{n-k} m) \prod_{i=1}^{p^k - 1} \frac{p^n m - i}{p^k - i} \end{aligned}$$

If $i = p^\ell j$ for $p \nmid j$ then

$$\begin{aligned} p^k - i = p^k - p^\ell j = p^\ell(p^{k-\ell} - j) \\ p^n m - i = p^n m - p^\ell j = p^\ell(p^{n-\ell} m - j) \end{aligned}$$

Both $p^{k-\ell} - j$ and $p^{n-\ell} m - j$ are coprime to p, so $p^k - i$ and $p^n m - i$ are divisible by exactly rhe same powers of p. Thus $|S| = p^{n-k} \cdot$ (some # coprime to p).

This is an awful way to prove this fact. Lets do it in a better way. A better proof is that $\binom{pa}{pb}$ is the coefficient of x^{pb} in $(x+1)^{pa}$. Thus in $\mathbb{Z}/p\mathbb{Z}$ we have

$$(x+y)^p = x^p + y^p$$
$$(x+1)^{pa} = (x^p+1)^a.$$

Thus the coefficient of x^{pb} is $\binom{a}{b}$. Therefore

$$\binom{pa}{pb} \equiv \binom{a}{b} \mod p$$

This proves the existence of p-subgroups.

Now we prove that any two Sylow p-subgroups are conjugate and any p-subgroup of G is contained in a Sylow p-subgroup of G. We first need a lemma.

Lemma .0.2

If H is a p-group acting on a set X then $|X| = (\#$ of fixed points of $H) \mod p$.

X is a union of disjoint H-orbits, each H-orbit has size dividing $|H|$, so this size is a power of p. The number of length-1 orbits is then equivalent to $|X| \mod p$, and we're done.

We now show that for any p-subgroup H of G and any Sylow p-subgroup J of G that there exists $g \in G$ such that $g^{-1}Hg \leq J$.

H acts on G/J by multiplication $h \cdot (gJ) = hgJ$. Since J is a Sylow p-subgroup, $|G/J|$ is coprime to p. Thus the $\#$ of fixed points of H on G/J is nonzero (because it is coprime to p).

This says there exists a $g \in G$ such that $HgJ = gJ$. Thus $g^{-1}HgJ = J$. Therefore $g^{-1}Hg \subseteq J$.

Finally we need to show that the number of Sylow p-subgroups divides $|G|$ and is $\equiv 1 \mod p$. Let A be the set of all Sylow p-subgroups. G acts on A by conjugation. This action is transitive (i.e., has one orbit). Pick a Sylow p-subgroup J. Then by orbit-stabilizer

$$|A| = |\mathcal{O}_J| = [G : G_J] = \frac{|G|}{|G_J|}$$

Thus $|A| \mid |G|$. Furthermore, note that $J \subseteq G_J$, so $p^n \mid |G|_J$. Therefore $|A|$ is coprime to p. Now we need to see that it is $\equiv 1 \mod p$.

Well, restrict the action so that J is acting on A. It then suffices to determine the fixed points, which we claim is just $J \in A$. Well

$$\begin{aligned} J \text{ fixes some } H \in S &\iff jHj^{-1} = H \quad \forall\, j \in J \\ &\iff J \subseteq N_G(H) \qquad \text{(i.e., normalizer of } H \text{ in } G) \end{aligned}$$

H and J are now Sylow p-subgroups of $N_G(H)$. Thus they are conjugate in$N_G(H)$. But wait! Then $J = xHx^{-1} = H$ for some $x \in N_G(H)$. Perfect!

Thus there is one fixed point, and by the lemma $|A| \equiv 1 \mod p$.