Content:

Theorem Let G be a group such that $|G| = p^k n$, p is prime and $(p, n) = 1$. Then **(1)** Sylow p-subgroups exist; **(2)** Any 2 Sylow p-subgroups are conjugate; **(3)** Let n be the number of Sylow p-subgroups, then $n_p \equiv 1 \pmod p$ and $n_p | n$.

Lemma Let P be a Sylow p-subgroup of G. Then **(1)** All conjugates of P are Sylow p-subgroups; **(2)** $|N_G(P)/P|$ is relatively prime to p; **(3)** If $a \in G$ such that $\circ(a) = p^\ell$ and $aPa^{-1} = P$, then $a \in P$.

Definition Let G be a finite group such that $|G| = p^k m$, p is prime and $(p, m) = 1$. Let $H \leq G$ such that $|H| = p^k$, then H is called a *Sylow p-subgroup* of G.

Note If G is Abelian, the Sylow p-subgroup exists and is unique (by Lemma 4).

If G is not Abelian, we don't know that Sylow p-subgroups exists yet.
Nor do we know if a Sylow p-subgroup is unique.

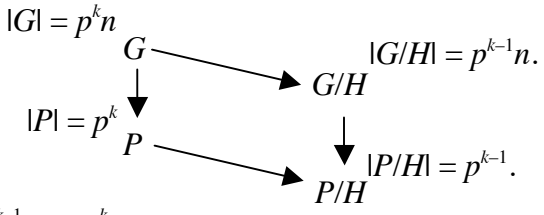
The Sylow Theorems

Theorem Let G be a group such that $|G| = p^k n$, p is prime and $(p, n) = 1$. Then
(1) Sylow p-subgroups exist.
(2) Any 2 Sylow p-subgroups are conjugate.
(3) Let n be the number of Sylow p-subgroups, then $n_p \equiv 1 \pmod p$ and $n_p | n$.

Proof (1):
We will prove (1) by induction on $|G|$.
If $|G| = 1$, we have for any prime p, a subgroup of $p^0 = 1$ and G itself is a subgroup of order p^0.
Assume inductively that any group of order $< p^k n$ has a Sylow p-subgroup.
By the Class Equation, we have
$|G| = |Z(G)| + \sum_i [G : C_G(a_i)]$ where for each i, $[G : C_G(a_i)] > 1$.

Case 1: Assume $p^k \mid |C_G(a_i)|$ for some a_i. Since $a_i \notin Z(G)$, then
$\exists\ g \in G$ such that $g a_i g^{-1} = a_i$. So $|a_i^G| \geq 2$.
And $|a_i^G| = [G : C_G(a_i)]$, so $C_G(a_i) \neq G$.
But $p^k \mid |C_G(a_i)|$, so $|C_G(a_i)| = p^k m$ where $m < n$ and $(p, m) = 1$.
By our induction hypothesis, $\exists\ P \leq C_G(a_i)$ such that $|P| = p^k$, a Sylow p-subgroup of G.
Case 2: Assume p^k does not divide $|C_G(a_i)|$ for all $a_i \in G$.
But $p^k \mid |G|$. So $p \mid \dfrac{|G|}{|C_G(a_i)|} = [G : C_G(a_i)]$.
So $p \mid [G : C_G(a_i)]$ for all $a_i \in G$.

By the class equation we have $p \mid Z(G)$.
By Cauchy's theorem, $\exists\ b \in Z(G)$ such that $\circ(b) = p$.
Let $H = \langle b \rangle$. Then $|H| = p$. We know $H \lhd G$ since $b \in Z(G)$.
$\therefore$ G/H is a group.
And $|G/H| = p^k n / p = p^{k-1} n$.
By our induction hypothesis,
G/H contains a Sylow p-subgroup.
By the Correspondence theorem,
$\exists\ P \leq G$ such that P/H is a
Sylow p-subgroup of G/H.
So $|P/H| = p^{k-1}$. Thus $|P| = p^{k-1}|H| = p^{k-1} \bullet p = p^k$.
So P is a Sylow p-subgroup of G.



Note — If P is a Sylow p-subgroup of G, then it is a maximal p-group in G.
Suppose $H \leq G$ such that H is a p-group. If $P \leq H$, then $P = H$.

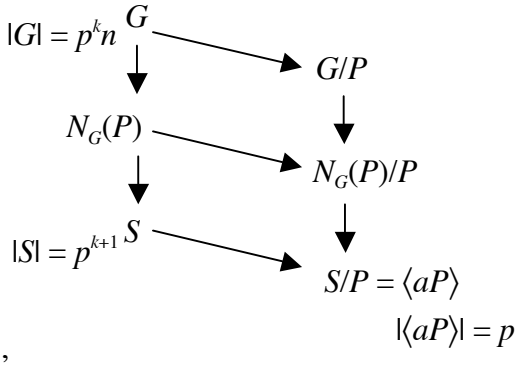
Lemma Let P be a Sylow p-subgroup of G. Then
(1) All conjugates of P are Sylow p-subgroups.
(2) $|N_G(P)/P|$ is relatively prime to p.
(3) If $a \in G$ such that $\circ(a) = p^\ell$ and $aPa^{-1} = P$, then $a \in P$.

Proof (1):

Suppose $|G| = p^k n$ and P is a Sylow p-subgroup of G, then $|P| = p^k$.
Let $x \in G$. By Proposition 2.58 (i) (If G is a group and $g \in G$, then conjugation γ_g: $G \to G$ is an isomorphism.), we have xPx^{-1} is a subgroup of G that is isomorphic to P. Hence $|xPx^{-1}| = |P|$. Since xPx^{-1} is an arbitrary conjugate of P and $|xPx^{-1}| = p^k$, then we can conclude that all conjugates of P are Sylow p-subgroups.

Proof (2):

We will prove the result by contradiction. Suppose $p \mid | N_G(P)/P |$.
By Cauchy's theorem, there is an element
$aP \in N_G(P)/P$ such that $\circ(aP) = p$.
Let $S' = \langle aP \rangle$. Then $|S'| = p$.
Since $\langle aP \rangle \leq N_G(P)/P$, then
by the Correspondence theorem,
$S' = S/P$ for some $S \leq N_G(P)$.
So $|S/P| = p$.
Then $|S| = p|P| = p \bullet p^k = p^{k+1}$.
Since $|G| = p^k n$, $S \leq G$, and $|S| = p^{k+1}$,
then we have a contradiction.



Proof (3):

Let $a \in G$ such that $\circ(a) = p^{\ell}$ and $aPa^{-1} = P$. Then $a \in N_G(P)$.

So $aP \in N_G(P)/P$.

Thus $\circ(aP) \mid |N_G(P)/P|$ and $\circ(aP) \mid \circ(a) = p^{\ell}$.

But, by part (2), p does not divide $|N_G(P)/P|$.

So, ($\underbrace{|N_G(P)/P|}_{\text{no } p\text{'s}}$, $\underbrace{\circ(a)}_{\text{all } p\text{'s}}$) = 1.

So $\circ(aP) = 1$. Hence $aP = P$, which gives us that $a \in P$.

We will use the preceding lemma in the proof of the 2nd and 3rd parts of the Sylow Theorems.

Theorem Sylow, part (2):
Let G be a group such that $|G| = p^k n$, p is prime and $(p, n) = 1$.
Then any 2 Sylow p-subgroups are conjugate.

Proof:

Assume $|G| = p^k n$, p is prime and $(p, n) = 1$.

Let P be a Sylow p-subgroup of G.

Let X be the set of all conjugates of P.

We will denote $X = \{P_1, P_2, \ldots, P_t\}$ where $P = P_1$.

Let P_1 act on X by conjugation.

Then by Corollary 2.99 (If a finite group G acts on a set X, then the number of elements in any orbit is a divisor of |G|.)

we have for any i, $|\mathcal{O}(P_i)| \mid |P_1| = p^k$.

So $|\mathcal{O}(P_i)| = 1$ or $p \mid |\mathcal{O}(P_i)|$.

If $|\mathcal{O}(P_i)| = 1$, then $\mathcal{O}(P_i) = P_i$, hence $aP_ia^{-1} = P_i \ \forall\ a \in P_1$.

Since $a \in P_1$, then $\circ(a) = p^{\ell}$.

So, by our previous lemma, part (3), $a \in P_i \ \forall\ a \in P_1$. $\therefore\ P_1 \subseteq P_i$.

And since $|P_1| = |P_i|$, then $P_1 = P_i$.

$\therefore\ |\mathcal{O}(P_i)| = 1$ only when $i = 1$.

And since X is a disjoint union of these orbits,

(i.e. $X = \mathcal{O}(P_1) \dot{\cup} \mathcal{O}(P_{i_1}) \dot{\cup} \cdots \dot{\cup} \mathcal{O}(P_{i_l})$),

then $|X| = 1 + ps$, for some $s \in \mathbb{Z}$. So $|X| \equiv 1 \pmod{p}$.

We will now show X contains all Sylow p-subgroups.

Suppose Q is a Sylow p-subgroup such that $Q \notin X$.
Then let Q act on X. By repeating the argument above,
we can conclude that
$|\mathcal{O}(P_i)| \neq 1$, since $P_i \neq Q$.
And X is a disjoint union of these orbits as well.
The size of each of these orbits is divisible by p, so $p \mid |X|$.
This contradicts the fact that $|X| \equiv 1 \pmod{p}$.
Thus, X must contain all Sylow p-subgroups.

Theorem Sylow, part (3):
Let G be a group such that $|G| = p^k n$, p is prime and $(p, n) = 1$.
Let n be the number of Sylow p-subgroups, then $n_p \equiv 1 \pmod{p}$
and $n_p \mid n$.
Proof:
X, as defined in part (2) above, contains all Sylow p-subgroups as
shown above. So $|X| = n_p$. Thus $n_p = |X| \equiv 1 \pmod{p}$.
And since $n_p = |\mathcal{O}(P)| = [G:N_G(P)] \mid |G| = p^k n$, then $n_p \mid p^k n$.
But $n_p \equiv 1 \pmod{p} \Rightarrow (n_p, p) = 1$, so $n_p \mid n$.
