Sylow's Theorem

In this section, we will make much more progress classifying finite groups based on their order. First, some definitions:

Definition: Let G be a group and p prime.

1.) A group of order p^α for $\alpha \geq 0$ is called a p-group. Subgroups that are p-groups are p-subgroups.

2.) If G is a group of order $p^\alpha m$ where p doesn't divide m, then a subgroup of order p^α is called a Sylow p-subgroup of G.

3.) The set of Sylow p-subgroups of G is $Syl_p(G)$ and the number of Sylow p-subgroups of G is $n_p(G)$.

Before we state and prove the Sylow Theorems, we need the following lemma:

Lemma: Let $P \in Syl_p(G)$. If Q is any p-subgroup of G, then $Q \cap N_G(P) = Q \cap P$.

Pf: Let $H = Q \cap N_G(P)$. Note that $H \leq Q$ so it's a p-group.

$P \leq N_G(P)$, so $Q \cap P \leq H$. Thus, we just need to show the reverse containment.

We know $H \leq Q$, so we just need to show $H \leq P$.

$H \leq N_G(P)$, so by a theorem from a previous section (end of section 12 in the notes), PH is a subgroup of G.

The second isom Thm says $PH/P \cong H/P\cap H$, so $|PH| = \frac{|P||H|}{|P\cap H|}$. ($|P|$: p-group; $|H|$: p-group; $|P\cap H|$: p-group.)

Thus PH is a p-group. $P \leq PH$, so $p^\alpha \mid PH$. Thus, $|PH| = p^\alpha$, so $P = PH$. Thus $H \leq P$. $\square$

Now we prove the Sylow Theorems. For the rest of the section, assume G is a group of order $p^\alpha m$, where p is a prime not dividing m.

Sylow's Theorem, part 1: Sylow p-subgroups of G exist! i.e. $Syl_p(G) \neq \emptyset$.

Pf: We will prove this by induction on $|G|$. If $|G| = 1$, we're done. Assume the statement holds for all groups of order $< |G|$.

Case 1: $p \mid |Z(G)|$. Then by Cauchy's Thm for abelian groups, $\exists$ a subgroup $N \leq Z(G)$ of order p.

Thus, $|G/N| = p^{\alpha-1}m$. So, by induction, G/N has a subgroup P/N of order $p^{\alpha-1}$.

Then $|P| = |P/N| \cdot |N| = p^\alpha$, so P is a Sylow p-subgroup of G, and we're done.

Case 2: p doesn't divide $|Z(G)|$. Let $g_1, \ldots, g_r$ be representatives of the conjugacy classes not contained in the center.

The class equation is $|G| = |Z(G)| + \sum_{i=1}^{r} |G : C_G(g_i)|$.

If $p \mid |G : C_G(g_i)|$ for all i, then we'd also have $p \mid |Z(G)|$, a contradiction. Thus, there is some i s.t. p doesn't divide $|G : C_G(g_i)|$. For this i set $H = C_G(g_i)$.

Then $|H| = p^\alpha k$, where p doesn't divide k.

$g_i \notin Z(G)$, so the centralizer can't be all of G. Thus $|H| < |G|$, so by induction, H has a Sylow p-subgroup of order p^α, so it's also a Sylow p-subgroup of G! □

Ex: If $|G| = 168$, then $168 = 2^3 \cdot 3 \cdot 7$, so G has subgroups of orders 8, 3, and 7 (among others!). We also know it has a subgroup of order 2.

Before proving the next part, we make a calculation. By the first part, there is some Sylow p-subgroup P of G.

Let $S = \{P_1, P_2, \ldots, P_r\}$ be the conjugates of P.

i.e. $S = \{gPg^{-1} \mid g \in G\}$. Let Q be any p-subgroup of G. Q also acts on the set S by conjugation.

By construction, G acts transitively on S, but Q may not. We can write

$$S = \mathcal{O}_1 \cup \mathcal{O}_2 \cup \ldots \cup \mathcal{O}_s$$

where the $\mathcal{O}_i$ are the orbits of S under the action of Q. Thus $r = |\mathcal{O}_1| + \ldots + |\mathcal{O}_s|$. Renumber the P_i so that the first r elements are representatives of each $\mathcal{O}_i$.

i.e $P_i \in \mathcal{O}_i$ for $i = 1, \ldots, s$. (Note: r doesn't depend on Q, s does)

Thus, $|\mathcal{O}_i| = |Q : Q_{P_i}|$, where Q_{P_i} is the stabilizer of P_i. But

$$Q_{P_i} = \{q \in Q \mid qP_iq^{-1} = P_i\} = N_Q(P_i) = N_G(P_i) \cap Q = P_i \cap Q, \text{ by the lemma.}$$

Thus, $|\mathcal{O}_i| = |Q : P_i \cap Q|$.

If we set $Q = P_1$, we get $|\mathcal{O}_1| = |P_1 : P_1 \cap P_1| = 1$.

For $i > 1$, $P_1 \neq P_i$, so $P_1 \cap P_i < P_1$. So

$$|\mathcal{O}_i| = |P_1 : P_1 \cap P_i| > 1 \quad \text{for} \quad 2 \leq i \leq s$$

($|P_1 : P_1 \cap P_i|$ is a power of p.)

Thus $r = |\mathcal{O}_1| + \underbrace{|\mathcal{O}_2| + \dots + |\mathcal{O}_s|}_{\text{div. by } p} \Rightarrow r \equiv 1 \pmod{p}$.

($|\mathcal{O}_1| = 1$)

i.e. we just showed that the # of conjugates of a Sylow p-subgroup is equiv. to 1 (mod p). We'll use this in the proof.

Sylow's Theorem, part 2:

1.) If P is a Sylow p-subgroup of G and Q any p-subgp of G, then $\exists\, g \in G$ s.t. $Q \leq gP^{-1}g$. i.e. Q is contained in some conjugate of P. In particular, any two Sylow p-subgroups are conjugate in G.

2.) The number of Sylow p-subgroups of G is of the form $1 + kp$. i.e.

$$n_p \equiv 1 \pmod{p}.$$

Moreover, $n_p = |G : N_G(P)|$ for any Sylow p-subgroup P.
Thus, $n_p \mid m$.

Pf: Let Q be any Sylow p-subgroup. Suppose Q is not contained

in any conjugate of P, i.e. any P_i.

Then $Q \cap P_i < Q$ $\forall$ i, so

$$|\mathcal{O}_i| = \underbrace{|Q : Q \cap P_i|}_{\text{div. by } p} > 1 \quad \text{for } 1 \leq i \leq s.$$

Thus p divides $|\mathcal{O}_1| + \dots + |\mathcal{O}_s| = r$, a contradiction.

Thus, $Q \leq P_i$, for some i, which proves the first part of 1.)

If Q is a Sylow p-subgroup, then $Q \leq P_i \cong P$. But $|Q| = |P|$, so $Q = P_i$, some i, which finishes the proof of 1.).

Thus, every Sylow p-subgroup is one of the P_i, so $n_p = r \equiv 1 \pmod{p}$.

Recall that we showed that the number of conjugates of a subset of a group is the index of its normalizer. Thus,

$$n_p = |G : N_G(P)| \quad \text{for any Sylow } p\text{-subgroup } P. \quad \square$$

Note that this theorem implies that

any two Sylow p-subgroups are isomorphic.

We also know that if $n_p > 1$, none of the Sylow p-subgroups can be normal. In fact:

Cor: Let P be a Sylow p-subgroup of G. The following are equivalent.

1.) P is the unique Sylow p-subgroup of G. i.e. $n_p = 1$.

2.) $P \trianglelefteq G$

3.) If $\varphi : G \to G$ is an automorphism $\varphi(P) = P$. (i.e. P is characteristic)

4.) If $X \subseteq G$ s.t. $|x|$ is a power of p $\forall\ x \in X$, then $\langle X \rangle$ is a p-group.

Pf: 1.) holds $\iff gPg^{-1} = P\ \forall\ g \in G \iff P$ is normal.

So 1.) $\iff$ 2.).

If 1.) holds then for any automorphism $\varphi : G \to G$, $|\varphi(P)| = |P|$, so $\varphi(P) = P$, so 1.) $\Rightarrow$ 3.)

If 3.) holds, then for any $g \in G$, consider the automorphism $\varphi : G \to G$ defined $h \mapsto ghg^{-1}$. Then $P = \varphi(P) = gPg^{-1}$, so P is normal. i.e. 3.) $\Rightarrow$ 2.).

If 4.) holds, then let X be the union of all the Sylow p-subgps. Each elt of X must have order a power of p, so $\langle X \rangle$ is a p-subgp. But then it's contained in a Sylow p-subgp. $\Rightarrow \langle X \rangle = X =$ a Sylow p-subgroup

Thus, there is only one Sylow p-subgroup, so 4.) $\Rightarrow$ 1.)

If 1.) holds, then let x have order a power of p. Then $\langle x \rangle \leq P$, so any set of such elements generate a subgroup of P, which is thus a p-group. so 1.) $\Rightarrow$ 4.). $\square$

Examples: Let G be a finite group and p prime.

1.) If p doesn't divide $|G|$, then 1, which has order p^0, is the unique Sylow p-subgroup.

2.) If G is a finite abelian group, then all its subgroups are normal, so it has a unique Sylow p-subgroup for each p.

3.) $|S_3| = 2 \cdot 3$. It has $3 \equiv 1 \pmod 2$ sylow 2-subgroups $\langle (12) \rangle, \langle (23) \rangle, \langle (13) \rangle$. It has a unique (thus normal) Sylow 3-subgroup $\langle (123) \rangle$.

4.) $|A_4| = 12 = 2^2 \cdot 3$. It has just one Sylow 2-subgp (of order 4) by a hw problem. It has 4 Sylow 3-subgroups.

5.) Note that D_8 acts faithfully on $\{1,2,3,4\}$ so $D_8 \hookrightarrow S_4$.
$|S_4| = 24 = 2^3 \cdot 3$. Thus every Sylow 2-subgroup is isomorphic to D_8.

However, S_4 has 9 elements of order 2,

$(12), (13), (14), (23), (24), (34), (12)(34), (13)(24), (14)(23)$

which must be in Sylow 2-subgroups. So $n_2 > 1$. n_2 divides 3 and is $1 \pmod 2$, so $n_2 = 3$.

There are more than 2 elements of order 3, so $n_3 > 1$. But $n_3 \mid 8$ so $n_3 = 4$.

We are now able to prove Cauchy's Theorem more generally:

Cauchy's Theorem: Let G be a finite group and suppose $p \mid |G|$. Then G has an element of order p.

Pf: Let P be a Sylow p-subgroup. Since $p \mid |G|$, P has order p^α, some $\alpha \geq 1$.

We showed P has nontrivial center, so $p \mid |Z(P)|$. $Z(P)$ is abelian, so by Cauchy's Theorem for abelian groups there is some $g \in Z(P)$ s.t. $|g| = p$. $\square$

Ex: Let G be a group of order $12 = 3 \cdot 2^2$. We show either G has a normal Sylow 3-subgroup or $G \cong A_4$.

Suppose $n_3 \neq 1$. Let $P \in Syl_3(G)$.

$n_3 \equiv 1 \bmod 3$ and $n_3 | 4$, so $n_3 = 4$. Distinct subgroups of order 3 intersect just at the identity and each have 2 elements of order 3, so G has $2 \cdot 4 = 8$ elements of order 3.

$|G : N_G(P)| = n_3 = 4$, so $N_G(P) = P$.

G acts by conjugation on the four Sylow 3-subgroups so we get a permutation representation $\varphi : G \longrightarrow S_4$.

The kernel is the subgroup $K \leq G$ which normalizes all the Sylow 3-subgroups. In particular, $K \leq N_G(P) = P$, but P isn't normal so $K = 1$. Thus φ is injective, so

$$G \cong \varphi(G) \leq S_4$$

There are exactly 8 elements of order 3 in S_4, all in A_4, so $\varphi(G) \cap A_4$ has at least 9 elements (including the identity).

But both groups have order 12, so $\varphi(G) = A_4$, so $G \cong A_4$.

Ex: Let p and q be primes, $p \neq q$, and suppose $|G| = p^2 q$. We'll show G has a normal Sylow subgroup (for either p or q). Let $P \in \mathrm{Syl}_p(G)$, $Q \in \mathrm{Syl}_q(G)$.

Case 1: $p > q$. Then $n_p \equiv 1 \pmod{p}$ but $n_p \mid q$, so $n_p = 1$, so $P \trianglelefteq G$.

Case 2: $p < q$. If $n_q = 1$, $Q \trianglelefteq G$. Thus assume $n_q > 1$.

Then $n_q = 1 + tq$, some $t > 0$, and $n_q \mid p^2$. Thus $n_q = p$ or p^2. But $q > p$, so $n_q \neq p$. Thus $n_q = 1 + tq = p^2$.

$$\Rightarrow tq = p^2 - 1 = (p+1)(p-1)$$

q is prime so $q \mid p+1$ or $q \mid p-1$. since $q > p$, the latter can't happen. Thus, $q \mid p+1$, so $q = p+1$.

But the only two primes that have a difference of 1 are 2 and 3, so $p = 2$, $q = 3$, and $|G| = 12$.

Thus, by the previous example, G has a normal Sylow 3-subgp or $G \cong A^4$, which has a normal Sylow 2-subgroup.