The Second Sylow Theorem

Definition: Let G be a finite group and let p^r be the largest power of p that divides the order of G. Then a subgroup of G of order p^r is called a *Sylow p-subgroup* of G.

[$G = S_4$, $|G| = 24$, $8 \mid 24$]
Sylow 2-subgroup has order 8

Sylow's first theorem says that Sylow p-subgroups always exist. Sylow's second theorem says they are all related to each other by conjugation.

Theorem: (Sylow II) Let P_1 and P_2 be Sylow p-subgroups of a finite group G. Then there is a $g \in G$ so that $gP_1g^{-1} = P_2$. In other words, all Sylow p-subgroups are conjugate to each other.

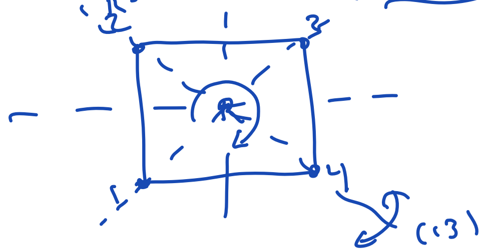
if P_1 is a Sylow p-subgroup
gP_1g^{-1} is a subgroup of same order

$$P_1 \longrightarrow gP_1g^{-1}$$
$$x \longmapsto gxg^{-1}$$
$$g^{-1}xg \longleftarrow y$$

An example

Example: Let $G = S_4$, a group of order 24. A Sylow 2-subgroup of G has order 8. One such subgroup consists of the 4-element cyclic subgroup generated by the four cycle $R = (1234)$ and a transposition $s = (13)$. These permutations generated a copy of the Dihedral group D_4, with elements:

$$e, \underbrace{(1234)}_{R}, \underbrace{(13)(24)}_{R^2}, \underbrace{(1432)}_{R^3}, (13), (24), (14)(23), (12)(34).$$



However, there are others:

$$e, (1324), (12)(34), (1423), (12), (34), (13)(24), (14)(23).$$

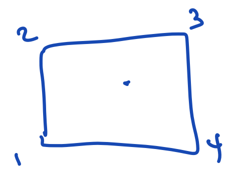
and

$$e, (1243), (14)(23), (1342), (13)(24), (14)(23), (14), (23)$$

Each of these 3 subgroups H_1, H_2, H_3 is a copy of D_4, corresponding to different ways of labelling the vertices of the square.

- The first example labels the vertices (going around the square) $1, 2, 3, 4$ (so that the diagonals connect $1, 3$ and $2, 4$).

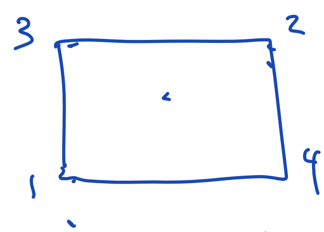
H_1



$R = (1\,2\,3\,4)$

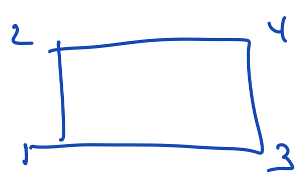
- The second labels them $1, 3, 2, 4$ (so that the diagonals connect $1, 2$ and $3, 4$)

H_2



$R = (1\,3\,2\,4)$

- The third labels them $1, 2, 4, 3$ (so that the diagonals connect $1, 4$ and $2, 3$)



$R = (1\,2\,4\,3)$

H_3

Notice that $(12)H_1(12) = H_3$ and $(14)H_1(14) = H_2$. So all of these Sylow 2-subgroups are conjugate to one another.

Key definitions and lemmas

The orbit of a subgroup H under the conjugation action of G is the set of subgroups $\{g\cancel{P}g^{-1} : g \in G\}$.

H

$H \subseteq G$

Orbit of H under conjugation. $\{gHg^{-1} \mid g \in G\}$

From our study of group actions, we know that this orbit is in bijection with the cosets of the stabilizer G_H of H under this action.

Orbit is in bijection with cosets G/G_H

G_H = Stabilizer of H under conjugation.

But

$$G_H = \{g \in G : \underline{gHg^{-1} = H}\}.$$

Definition: The subgroup $G_H = \{g \in G : gHg^{-1} = H\}$ is called *the normalizer $N(H)$ of H in G*.

Lemma: $N(H)$ has these properties:

- H is a normal subgroup of $N(H)$
- if K is any subgroup of G containing H as a normal subgroup, then $K \subset N(H)$. ☆

Proof: $H \subseteq N(H)$ $\qquad hHh^{-1} = H$ for all $h \in H$.

H is normal in $N(H)$ $\qquad \subseteq G$

$g \in N(H) \Rightarrow gHg^{-1} = H$. $\qquad \underline{H}$ $\underline{N(H)}$

In $D_4 \subseteq S_4$ which is a Sylow 2-subgroup

$N(D_4) = D_4$.

Conjugates of $D_4 \simeq [G : N(D_4)]$

3 conjugates $\qquad N(D_4) \subseteq G$ has index 3

$\underbrace{D_4 \subseteq N(D_4) \subseteq G}_{3}$

Lemma: If P is a Sylow p-subgroup, then $N(P)$ has some additional properties:

- The index $[N(P) : P]$ is not divisible by p.
- Any element of $N(P)$ of prime power order belongs to P.

Proof:

$|G| = p^n m \qquad p \nmid m.$

$|P| = p^n$

$[G : P] = m \qquad p \nmid m.$

$P \leq N(P) \subseteq G$

$[G : N(P)] \underbrace{[N(P) : P]}_{p \nmid m.} = \underset{p \nmid m}{\underline{m}}.$

If $g \in N(P)$ and is of order p^s then $g \in P$.

~~(P is a sylow p-subgroup~~ $\quad |N(P)/P| = K \qquad p \nmid K.$

$g \in N(P)$

$g \in N(P) \quad (gP)$ has order a power of p in $N(P)/P$.

$(gP)^{p^s} = g^{p^s} P = P$

order (gP) divides p^s and $K \Rightarrow$ order $(gP) = 1$

$\Leftrightarrow gP = P$

$\Leftrightarrow g \in P.$

The proof

Proof of Sylow II: Let $P = P_1$ be a Sylow p-subgroup of G and let $X = \boxed{\{P_1, P_2, \ldots, P_k\}}$ be its conjugates under the action of G. Our goal is to show that, if Q is any Sylow p-subgroup of G, then $Q = P_s$ for some $s = 1, \ldots, k$.

1. The number k of conjugates of P is $[G : N(P)]$ which is not a multiple of p.

   $N(P) = G_P$

   $\underbrace{[G:N(P)][N(P):P]}_{[G:P]} = m \quad p \nmid m \qquad |G| = p^n m \quad |P| = p^n$

2. Let Q be any Sylow p-subgroup and consider the action of Q on the set X.

   Because $Q \leq G$, $\quad gP_ig^{-1} = P_i \quad i = 1, \ldots, k$ for all $g \in Q$.

   X has Q-action.

3. X is divided up into orbits for the action of Q. Each orbit has $[Q : Q \cap N(P_i)]$ elements for some $i = 1, \ldots, k$. So

$$k = \sum_{s=1}^{r} [Q : Q \cap N(P_s)]$$

   where P_s, for $s = 1, \ldots, r$, are representatives for the different orbits of Q.

   $P_i \in X \qquad Q_{P_i} = \{g \in Q \mid gP_ig^{-1} = P_i\} = Q \cap N(P_i)$

4. Each number $\overbrace{[Q : Q \cap N(P_i)]}$ is a power of p, but k is not divisible by p. So in the sum for k, at least one of the terms $[Q : Q \cap N(P_s)]$ is equal to one (which is p^0). In other words $Q \subset N(P_s)$ for some s.

$$K = \sum_{i=1}^{s} [\underline{Q : Q \cap N(P_i)}]$$

There is an i with

$$[Q : Q \cap N(P_i)] = 1.$$

$$Q \cap N(P_i) = Q$$

$$Q \le N(P_i)$$

5. Since every element of Q has order a power of p, this means every element of Q is in P_s. In other words $Q \subset P_s$. Since they have the same order, they are equal.

$Q \le N(P_s)$

every elt of Q has p-power order.

$Q \subseteq P_s$.

both have order p^n.

so $Q = P_s$.

Corollary: Let H be any subgroup of G of prime power order. Then H is contained in a Sylow p-subgroup of G.

Proof: Repeat the above argument for H; at the end you conclude that $H \subset P_s$ for some s.