Teoría de Sylow

Definiciones

> - Un grupo G donde todo elemento de G tiene orden una potencia de un primo p es llamado un p-grupo.
> - Si $H \leq G$ y H es un p-grupo, entonces decimos que H es un p-subgrupo de G.

Los teoremas de Sylow son una ayuda inmensa para describir propiedades de los subgrupos de un grupo G sólo a partir de su orden, para exponerlos tenemos que primero ver un *lema* importante:

Lema:

Si un grupo H de orden p^n con p primo actúa sobre un conjunto finito S y si $S_0 = \{x \in S : hx = x, \ \forall h \in H\}$, entonces $|S| \equiv |S_0| \bmod(p)$.

Resumen de la demostración:

1. Revisamos que $|\overline{x}| = 1 \iff x \in S_0$.
2. Planteamos a S como la unión disjunta de las órbitas de sus elementos de la siguiente forma:

$$S = S_0 \cup \overline{x}_1 \cup \overline{x}_2 \cup ... \cup \overline{x}_n$$

3. Para algún n. donde $\overline{x}_i > 1$ para todo $1 \leq i \leq n$. Por lo que tenemos que

$$|S| = |S_0| + |\overline{x}_1| + |\overline{x}_2| + ... + |\overline{x}_n|$$

4. Por lo visto en acciones, $|\overline{x}_i| = [G : H_{x_i}]$ y por el teorema de Lagrange tenemos que $|\overline{x}_i|$ divide a $|H| = p^n$ para todo i.
5. Concluimos que $|S| = |S_0| + |\overline{x}_1| + |\overline{x}_2| + ... + |\overline{x}_n| \equiv |S_0| + 0 + 0 + ... + 0 = |S_0| \bmod(p)$.

Con esto en mano, podemos pasar a otro teorema necesario antes de entrar de lleno a Sylow:

Teorema de Cauchy:

Si G es un grupo finito cuyo orden es divisible por un primo p, entonces G contiene un elemento de orden p.

Resumen de la demostración:

1. Definimos a $S = \{(a_1, a_2, ..., a_p) : a_i \in G \wedge a_1 \cdot a_2 \cdot ... \cdot a_p = e\}$ como el conjunto de las p-tuplas cuyo producto es el neutro. Claramente podemos caracterizar a a_p como $(a_1 \cdot a_2 \cdot ... \cdot a_n)^{-1}$ por lo que deducimos que $|S| = n^{p-1}$.

   > Básicamente tenemos que para un elemento de S necesitamos una n-upla donde para la primera componente tenemos n opciones (donde $|G| = n$), para la segunda componente seguimos teniendo n opciones, así hasta la $p-1$ componente, pues para garantizar que nuestra upla esté en S necesitamos que la p-ésima componente sea el inverso de todas las anteriores (que es único). Así, $|S| = n^{p-1} \times 1 = n^{p-1}$.

2. Como $p|n$, particularmente $p|n^{p-1}$ y por tanto $|S| \equiv 0 \bmod (p)$.

3. Ahora, vamos a hacer actuar a $\mathbb{Z}_p$ sobre S por medio de permutaciones cíclicas, esto es que si $k \in \mathbb{Z}_p$, $k(a_1, a_2, ..., a_p) = (a_{k+1}, ..., a_p, a_1, ..., a_k)$ (básicamente moviendo hacia la izquierda k veces la p-upla).

   Tenemos que ver que esta acción está bien definida, por lo que vemos los siguientes tres puntos:

   - $k(a_1, a_2, ..., a_p) \in S$: En efecto, si $(a_1, a_2, ..., a_p) \in S$ entonces $a_1 \cdot a_2 \cdot ... \cdot a_p = e$, esto significa que $(a_1 \cdot a_2 \cdot ... \cdot a_k) \cdot (a_{k+1} \cdot ... \cdot a_p) = e$ por lo que $(a_1 \cdot a_2 \cdot ... \cdot a_k) = (a_{k+1} \cdot ... \cdot a_p)^{-1}$ y como los inversos conmutan, $(a_{k+1} \cdot ... \cdot a_p)(a_1 \cdot a_2 \cdot ... \cdot a_k) = e$ y por tanto $(a_{k+1}, ..., a_p, a_1, ..., a_k) \in S$.

   - Naturalmente un movimiento de 0 a la izquierda no altera a la upla luego $0(a_1, a_2, ..., a_p) = (a_1, a_2, ..., a_p)$.

   - Sean $m, n \in \mathbb{Z}_p$,

     $$\begin{aligned}(m+n)(a_1, a_2, ..., a_p) &= (a_{m+n+1}, ..., a_p, a_1, ..., a_{m+n}) \\ &= m(a_{n+1,...,}) \\ &= m(n(a_1, a_2, ..., a_p))\end{aligned}$$

     > Esto no lo he terminado, lo tengo que preguntar.

4. Usando el lema anterior, tenemos que para $S_0 = \{x \in S : hx = x\}$, $0 \equiv |S| \equiv |S_0| \bmod (p)$.

5. Ahora, si $(a_1, a_2, ..., a_p) \in S_0$ entonces $(a_{k+1}, ..., a_p, a_1, ..., a_k) = (a_1, ..., a_p)$ para todo $k \in \mathbb{Z}_p$ por lo que $a_1 = a_2 = ... = a_p$, llamemos $x = a_1$, como $(x, x, ..., x) \in S$, se tiene que $x^p = e$.

6. Ahora bien, sabemos que $(e, e, ..., e) \in S_0$ por lo que $|S_0| \neq 0$ y por tanto $|S_0| = hp$ para algún $h \in \mathbb{N}$, como $p \geq 2$, sabemos que existe $x \neq e$, $x \in G$ tal que $x^p = e$.

Por últimos, tenemos que definir 1 concepto:

- **Definición:** Sea G un grupo ($H \leq G$ un subgrupo de G), en el cual para todo elemento $x \in G$ ($x \in H$) se tiene que $|x| = p^k$ con p primo y $k \in \mathbb{N}$, entonces diremos que G es un **p-grupo** (**H es un p-subgrupo**).

Ahora si, los susodichos teoremas:

1^{er} Teorema de Sylow:

Sea G un grupo de orden $p^n m$, con $n \geq 1$, p primo y $(p, m) = 1$. Entonces, G contiene un subgrupo de orden p_i para cada $1 \leq i \leq n$ y cada subtrupo de orden p^i es normal en algún otro subgrupo de orden p^{i+1}.

Resumen de la demostración:

La idea para demostrar que existen los i gruos de orden p^i gira alrededor de hacerla por inducción matemática sobre i.

1. La existencia del subgrupo del caso $i = 1$ es garantizado por el Teorema de Cauchy pues existe un elemento x con orden p por lo que $\langle x \rangle \leq G$ es un subgrupo de orden p^1.

2. Ahora supongamos que tenemos un grupo H de orden p^i, por el **lema del normalizador** $H \lneq N_G(H)$ y además el orden del grupo cociente $N_G(H)/H$ es múltiplo de p, aplicando el teorema de Cauchy existe un elemento $xH \in N_G(H)/H$ tal que $|xH| = p$, como $x \in N_g(H)$, podemos definir al siguiente subgrupo:

$$H' = H \cup xH \cup x^2 H \cup ...x^{p-1} H$$

   Donde dado que $x^i H \in N_G(H)/H$ para $0 \leq i < p$ entonces son todos disyuntos dos a dos y por tanto

$$\begin{aligned} |H'| &= |H| + |xH| + ... + |x^{p-1} H| \\ &= p^i + p^i + ... + p^i \\ &= p \cdot p^i \\ &= p^{i+1} \end{aligned}$$

3. Tenemos que verificar que H' es subgrupo:

    - Como $H \subseteq H'$, $H \neq \varnothing$ y $e \in H'$.
    - Sean $a, b \in H'$, $a \in x^j H$ y $b \in x^k H$ para $0 \leq j, k < p$. Esto es, $a = x^j h_1$ y $b = x^k h_2$ para $h_1, h_2 \in H$, para b^{-1} sabemos que $b^{-1} = (x^k h^2)^{-1} = (h^2)^{-1} x^{-k} = h_3 x^l$ para algún $h_3 \in H$ y $0 \leq l < p$. Así, $ab^{-1} = (x^j h_1)(h_3 x^l) = x^j h_4 x^l$, usando que $x \in N_G(H)$ se tiene que $x^j(h_4 x^l) = x^j(x^l h_5) = x^{j+l} h_5 = x^m h^5$ para $h_5 \in H$ y $0 \leq m < p$ por lo que $ab^{-1} \in x^m H \subseteq H'$.

      Así, ya probamos que existe al menos un subgrupo con orden p^i para cada $1 \leq i \leq n$.

4. Vemos que con el paso inductivo ya tenemos que $H \trianglelefteq H'$ pues $H' \subseteq N_G(H)$. Así queda demostrado el teorema.

Definición:

> - Si $|G| = p^n m$ donde p es primo y m un entero tal que $(p, m) = 1$, entonces un subgrupo $H \leq G$ que cumpla que $|H| = p^n$ es llamado un p-subgrupo de Sylow.

2^{do} Teorema de Sylow:

Si H es un p-subgrupo de un grupo finito G, y P es un p-subgrupo de Sylow de G, entonces existe $x \in G$ tal que $H < xPx^{-1}$. En particular, dos p-subgrupos de Sylow de G son conjungados.

Resumen de la demostración:

1. Definimos a S como el conjunto de todas las clases módulo P.

2. Hacemos a H actuar sobre S por medio de traslación a izquierda. Dada esta acción podemos definir

$$S_0 = \{xP \in S : hxP = xP, \forall h \in H\}$$

3. Por Lema, $|S| \equiv |S_0| \bmod(p)$ donde $|S| = [G : P]$.

4. Sabemos que $|G| = p^n m$ para algún primo p y un natural m tales que $(p, m) = 1$, como P es un p-subgrupo de Sylow, es el máximo subgrupo con orden potencia de p, esto es $|P| = p^n$ y por tanto $[G : P] = m$.

5. Como $(p,m)=1$, $p \nmid |S|$ luego $|S_0| \not\equiv 0 \bmod(p)$ y por tanto existe $xP \in S_0$.

   Tenemos que

$$\begin{aligned} xP \in S_0 &\Leftrightarrow hxP = xP, &\quad \forall h \in H \\ &\Leftrightarrow x^{-1}hxP = P, &\quad \forall h \in H \\ &\Leftrightarrow x^{-1}HxP = P \end{aligned}$$

6. Ahora bien, sea $H' = x^{-1}Hx$. Si $H'P = P$ necesariamente todo elemento de H debe pertenecer a P, pues es cerrado algebráicamente. Por tanto:

$$\begin{aligned} xP \in S_0 &\Leftrightarrow x^{-1}Hx \leq P \\ &\Leftrightarrow H \leq xPx^{-1} \end{aligned}$$

7. Para algún $x \in G$, y por tanto H es subgrupo de una conjugación de P.

3^{er} Teorema de Sylow

Si G es un grupo finito y p un primo, entonces el número n de p-subgrupos de Sylow de G divide a $|G|$ y es de la forma $kp+1$ para algún $k \in \mathbb{N}$.

Resumen de la demostración:

1. Por el segundo Teorema de Sylow sabemos que el número n de p-subgrupos de Sylow para un p primo particular es el número de conjugaciones de H, donde H es algún p-subgrupo de Sylow.

2. Así, sabemos que $n = [G : N_G(H)]$, un divisor de G.

3. Definamos S como el conjunto de todos los p-subgrupos de Sylow y hagamos actuar a H sobre S por conjugación.

4. Nuevamente usamos a $S_o = \{K \in S : hKh^{-1} = K, \forall h \in H\}$, naturalmente $S_0 \neq \varnothing$ pues $H \in S_0$.

5. Ahora bien, sabemos que $H \trianglelefteq N_G(H)$ y que $H \lneq N_G(H)$. También sabemos que para cualquier $K \in S$, $H = gKg^{-1}$ para algún $g \in G$. (Por el segundo teorema de Sylow)

6. Por lo tanto, para cualquier $P \in S_0$, se tiene que $hPh^{-1} = P$ para todo $h \in H$ por lo que $P \trianglelefteq N_G(H)$ pero como $|H| = |P|$, necesariamente $H = P$ y por tanto, $|S_0| = 1$.

7. Luego $n = |S| \equiv |S_0| \equiv 1 \bmod(p)$ por lo que $n = kp+1$ para algún natural k.