5 Los teoremas de Sylow

A continuación expondremos uno de los resultados más clásicos de la teoría de grupos finitos, históricamente debidos al matemático ruso Sylow.

El planteamiento es francamente simple. La teoría de Galois genera como tarea importante la búsqueda de subgrupos de un grupo finito. El teorema de Lagrange garantiza que el orden de todo subgrupo es divisor del orden del grupo, lo que acota nuestras posibilidades.

Ahora bien, dos preguntas se nos plantean: ¿debemos buscar subgrupos de orden cualquier divisor?, ¿cuántos y cuáles son los subgrupos de un orden dado?

Para el caso de grupos cíclicos, estas preguntas han sido contestadas de manera taxativa: para cada divisor del orden del grupo, existe un único subgrupo, que además es cíclico. Por otro lado, sabemos que el recíproco del teorema de Lagrange es falso; de hecho, hemos visto que el grupo A_4, que es de orden 12, carece de subgrupos de orden 6.

Para el caso de que la primera pregunta sea afirmativa, notemos que S_3 tiene 3 subgrupos de orden 2; lógicamente son isomorfos; más aún los tres son conjugados, como veremos[1], lo que facilita su localización. Otra situación no tan deseada la presenta el grupo diédrico de grado 4; es un grupo de orden 8 que tiene un subgrupo de orden 4 que es cíclico y dos subgrupos de orden 4 que son producto directo de grupos cíclicos de orden 2. Por tanto, no pueden ser isomorfos y deben ser localizados uno a uno.

Los teoremas de Sylow localizan en un grupo finito los subgrupos de orden potencia de primo mediante el siguiente

Teorema [Sylow] Sea G un grupo de orden $p^m q$, donde p es un primo no divisor de q. Entonces,

1. G posee al menos un subgrupo de orden p^m, que recibe el nombre de p-subgrupo de Sylow[2] de G
2. El número de p-subgrupos de Sylow es congruente con 1 módulo p.
3. Cada dos p-Sylow de G son conjugados. En consecuencia, el número de p-subgrupos de Sylow es divisor de q.
4. Cada p-subgrupo de G está contenido en un p-Sylow.

Vayamos por partes.

Definición 5.1 *Dado un número primo p, se dice p-subgrupo de G a un subgrupo de orden potencia de p.*

[1] o por comprobación directa si el lector lo prefiere
[2] Abreviadamente, p-Sylow

Ejemplo C_4 es un 2-subgrupo de D_4. Por convenio 1_G es p-subgrupo de G para cada primo p.

Aunque sea redundante, repitamos la siguiente

Definición 5.2 *Dado un número primo p, se dice p-subgrupo de Sylow de G a un p-subgrupo P de G tal que $[G : P]$ es primo con p.*

Ejemplo C_2 es un 2-Sylow de S_3 y C_3 es un 3-Sylow de S_3.

Antes de demostrar los teoremas de Sylow veamos un caso particular debido a Cauchy:

Proposición 5.3 (Cauchy) *Si G es un grupo finito abeliano y p es un primo divisor de $|G|$, existe, al menos, un elemento de orden p.*

Demostración: Sea G un contraejemplo minimal[3]; puesto que p es divisor del orden de G, debe existir $1 \neq g \in G$.

- Si $o(g) = pq$, entonces, $o(g^q) = p$, que contradice la existencia de G.
- En caso contrario, $p \mid |G/ < g > |$; puesto que $G/ < g >$ no puede fallar el teorema, existe $x < g > \in G/ < g >$ de orden p. Así,

$$p = o(x < g >) \mid o(x) \Longrightarrow o(x) = pq \Longrightarrow o(x^q) = p$$

que vuelve a contradecir la existencia de G.

Teorema 5.4 (Primer teorema de Sylow) *Sea G un grupo de orden $p^m q$, donde p es un primo no divisor de q. Entonces, para cada $r = 0, \ldots, m$, G posee, al menos un subgrupo de orden p^r. Como consecuencia, todo grupo finito posee p-subgrupos de Sylow.*

Demostración: El resultado es claro si m ó r son 0. Para $m, r > 0$, razonaremos por inducción sobre el orden de G. Consideremos la ecuación de las clases

$$|G| = |\mathbf{Z}(G)| + \sum [G : C_G(x_i)]$$

- Si p no divide a $|\mathbf{Z}(G)|$ tampoco puede dividir a algún sumando $[G : C_G(x)]$. Por tanto, p^r es divisor de $|C_g(x)|$; puesto que $x \notin \mathbf{Z}(G)$, $C_G(x)$ es un subgrupo estricto de G y por inducción existe un subgrupo de $C_G(x)$, luego de G, de orden p^r.
- Si p es divisor de $|\mathbf{Z}(G)|$, por el teorema de Cauchy, existe $g \in \mathbf{Z}(G)$ de orden p. Ahora $< g >$ es un subgrupo normal de G (por estar dentro del centro), y podemos aplicar inducción al grupo $G/ < g >$ obteniendo $S/ < g >$ de orden p^{r-1}. Ahora, S es un subgrupo de G de orden p^r.

[3]Es decir, un grupo de orden mínimo entre los que fallen el resultado

Lema 5.5 *Sea P un p-Sylow de G. Si S es un p-subgrupo de G, contenido en $N_G(P)$, entonces, $S \leq P$.*

Demostración: Puesto que $S \leq N_G(P)$ podemos considerar el subgrupo SP y $|SP| = p^s$. Ahora $P \leq SP$ debe dar por órdenes $P = SP$ y S está contenido en P.

Teorema 5.6 (Segundo teorema de Sylow) *Sea g un grupo finito y p un número primo*

i) *El número ν_p de p-subgrupos de Sylow es congruente con 1 módulo p.*

ii) *Los p-subgrupos de Sylow de G son conjugados. En consecuencia, si P es un p-Sylow, ν_p es divisor de $[G : P]$.*

Demostración: El resultado es claro si p no divide al orden de G.

Consideremos la acción por conjugación sobre los p-Sylows de G

$$x \longrightarrow \begin{pmatrix} \cdots P \cdots \\ \cdots P^x \cdots \end{pmatrix}$$

La restricción a un p-Sylow P tiene una órbita de longitud 1, que es $\{P\}$. Por otro lado, si hubiera otra órbita de longitud 1, digamos $\{P_1\}$, se tendría $P_1^x = P_1 \, \forall x \in P$, por lo que $P \leq N_G(P_1)$ y, de acuerdo con el lema, $P \leq P_1$; por órdenes, $P = P_1$. Por tanto, hay una única órbita de longitud 1. Cualquier otra órbita su longitud es $[P : N_P(P_i)]$ divisor de $|P|$, y, para la suma de longitudes, se tiene

$$\nu_p = 1 + \sum p_i^r$$

Esto da el item i). Para el ii), se trata de probar que la acción es transitiva. Al efecto, si hubiera dos órbitas $\Omega_1 = \{P_1, \ldots\}$, $\Omega_2 = \{P_2, \ldots\}$ eligiendo el p-Sylow P_1 podríamos considerar las acciones restringidas

$$\begin{array}{ccc} P_1 & \longrightarrow & \Omega_1 \\ x & \longrightarrow & \binom{P_1^y}{P_1^{yx}} \end{array} \qquad \begin{array}{ccc} P_1 & \longrightarrow & \Omega_2 \\ x & \longrightarrow & \binom{P_2^y}{P_2^{yx}} \end{array}$$

Siguiendo el razonamiento anterior $|\Omega_1| \equiv 1 \bmod p$ y $|\Omega_2| \equiv 0 \bmod p$.

Eligiendo ahora el p-Sylow P_2

$$\begin{array}{ccc} P_2 & \longrightarrow & \Omega_1 \\ x & \longrightarrow & \binom{P_1^y}{P_1^{yx}} \end{array} \qquad \begin{array}{ccc} P_2 & \longrightarrow & \Omega_2 \\ x & \longrightarrow & \binom{P_2^y}{P_2^{yx}} \end{array}$$

y $|\Omega_1| \equiv 0 \bmod p$ y $|\Omega_2| \equiv 1 \bmod p$, pero esto es imposible. De esta manera, hay una sola órbita Ω, la acción es transitiva y todos los p-Sylows son conjugados. La última afirmación es consecuencia de

$$\nu_p = |\Omega| = [G : N_G(P)] \mid [G : P]$$

Ejemplos Para cada primo p impar, el grupo diédrico de grado p, D_p, posee un único p-Sylow que será normal, y exactamente $p+1$ 2-Sylows, pues si sólo hubiera uno sería normal y $D_p = C_p \times C_2 \cong C_2 p$, lo que es imposible, pues D_p no es abeliano.

Teorema 5.7 (Tercer teorema de Sylow) *Cada p-subgrupo de G está incluído en un p-subgrupo de Sylow.*

Demostración: Sea S un p-subgrupo de G y consideremos la acción por conjugación de S en el conjunto de p-Sylows de G. Puesto que dicho conjunto tiene tamaño congruente con 1 módulo p y el tamaño de las órbitas es siempre divisor de $|S|$, al menos existe una órbita de longitud 1. Así, existe un p-Sylow P de G tal que $P^x = P$, $\forall x \in S$. Entonces,

$$S \leq N_G(P) \overset{\text{lema}}{\Longrightarrow} S \leq P$$

EJERCICIOS

1. Probar que todo grupo abeliano tiene un único p-Sylow, para cada primo p.
2. Probar que no puede haber grupos simples de órdenes 148 ni 56.
3. Probar que si p y q son dos primos no hay grupos simples de orden pq.
4. Probar que un grupo de orden 6 es cíclico o (isomorfo a) S_3.
5. Probar que todo grupo G de orden 15 es cíclico.
6. Probar que C_{mn} es producto directo de sus subgrupos C_m y C_n si y sólo si $(m, n) = 1$ ¿Es cierto que todo grupo de orden $mn, (m, n) = 1$ es cíclico?
7. Probar que si P es un p-Sylow de G y $N_G(P) \leq S \leq G$, $N_G(S) = S$.
8. [Argumento de Frattini] Sea M un subgrupo normal de G y P un p-Sylow de M. Probar que $G = MN_G(P)$.
9. Probar que dos p-Sylows distintos de un subgrupo S de G no pueden estar contenidos en el mismo p-Sylow de G.