CONCURSO ÁLGEBRA Y LÓGICA 473426

PRUEBA DE OPOSICIÓN: DR. MARCO ANDRÉS FARINATI

Teoremas de Sylow [1872, Math. Ann.]

Peter Ludwig Mejdell Sylow, matemático noruego (1832 - 1918).

Sea G un grupo finito y p un número primo. Si $|G| = p^r m$ con p y m coprimos, un subgrupo S de G se llama un p-subgrupo de Sylow si $|S| = p^r$. El primer teorema de Sylow nos dicen que todo grupo finito admite, para cada primo p, un p-subgrupo de Sylow. El segundo y tercer teorema proveen información sobre ellos (ver secciónes 2 y 3). Las demostraciones consisten en utilizar ingeniosamente, y de diversas maneras, la noción de acción de un grupo en un conjunto.

Preliminares

Utilizaremos los siguientes resultados y herramientas de las acciones de grupos en un conjunto. Si X es un conjunto, G un grupo que actua (a izqueirda) en X, y $x \in X$, el estabilizador de x es el subgrupo $St_x = \{g \in G : gx = x\} \subseteq G$, la órbita de x es el subconjunto $G.x = \{g.x : g \in X\} \subseteq X$. Por ejemplo si la acción es trivial, las orbitas son puntuales, en general, cuanto mayor sea el estabilizador de un punto, menor será su órbita; más exactamente, utilizaremos la fórmula

$$|\mathcal{O}_x| = [G : St_x] = |G|/|St_x|$$

También podemos considerar los puntos fijos por la acción: $X^G = \{x \in X : gx = x \forall g \in G\}$, este conjunto es la reunión de todas las órbitas puntuales.

Sabemos que una acción de un grupo induce una relación de equivalencia, y las clases de equivalencia son las órbitas, por lo tanto el conjunto X es unión disjunta de sus órbitas: $X = \coprod_{x \in X/G} \mathcal{O}_x$. Separando las órbitas puntuales de las demás, obtenemos la ecuación de clases:

$$|X| = |X^G| + \sum_{x \in X/G, x \notin X^G} |\mathcal{O}_x|$$

y sobre las orbitas no triviales $\mathcal{O}_x$ la información que tenemos es que tienen orden igual al índice del estabilizador de x, que siempre son divisores no triviales de $|G|$.

1. Primer teorema de Sylow: existencia de p-subgrupos

Demostración. Por inducción (global) en el orden de G. Consideremos $\mathcal{Z}(G)$ el centro de G. Conviene demostrar primero el siguiente *lema: si G es abeliano y $p|\ |G|$ entonces existe $g \in G$ con $|g| = p$.*

Demostracion del lema: tomamos g un elemento arbitrario no trivial de G. Si $p|\ |g|$, digamos $|g| = pn$, entonces $x = g^n$ tiene orden p. Si en cambio $|g|$ es coprimo con p, podemos considerar el grupo cociente (es un grupo pues siendo G abeliano todo subgrupo es normal) y la proyección $\pi : G \to G/\langle g\rangle$. Como p divide al orden de G y no divide al orden de g, entonces p divide al orden de $G/\langle g\rangle$, y como éste es un grupo de orden menor, por hipótesis inductiva, tendrá un elemento $\overline{x} \in G/\langle g\rangle$ de orden p. Si considermos $x \in G$ tal que $\pi(x) = \overline{x}$, podemor tomar $y = x^n$. Éste elemento es no trivial pues $\pi(y) = \overline{x}^n \neq 1$ ya que n es coprimo con p, e $y^p = x^{np} = 1$ pues $\overline{x}^p = 1$ lo que significa que $x^p \in \langle g\rangle$ y $g^n = 1$.

Observación 1.1. Este lema es una versión más débil del Teorema de Cauchy que veremos como consecuencia de este mismo teorema más adelante.

Continuamos ahora con el teorema de Sylow: consideramos el grupo abeliano $\mathcal{Z}(G)$. Si $p|\ |\mathcal{Z}(G)|$, tenemos un elemento $g \in \mathcal{Z}(G)$ de orden p, y evidentemente $\langle g\rangle$ es un subgrupo normal. El grupo cociente $G/\langle g\rangle$ tiene orden $p^{r-1}m$. Por hipótesis inductiva en el orden del grupo, existe $\overline{S}$ subgrupo de $G/\langle g\rangle$ de orden p^{r-1}, luego $S = \pi^{-1}(\overline{S})$ tiene orden p^r como queriamos.

Caso $p \not| |\mathcal{Z}(G)|$ (por ejemplo si $\mathcal{Z}(G)$ es trivial). Consideramos la ecuación de clases para la situación $X = G$ y G actuando por conjugación. En este caso X^G es el centro, cuyo orden no es divisible por p, y la ecuación de clases nos dice

$$|G| = |\mathcal{Z}(G)| + \sum_{g \in X/G, g \notin \mathcal{Z}(G)} \mathcal{O}_g$$

Si p dividiera al cardinal de todas las clases de conjugación no triviales entonces p dividiría al orden de $\mathcal{Z}(G)$, lo que es absurdo, por lo tanto hay por lo menos una clase de conjugación no trivial cuyo cardinal no es múltiplo de p. Pero ese cardinal es igual al indice del estabilizador correspondiente, por lo tanto, ése estabilizador tiene orden tal que la potencia máxima que divide a G también lo divide. Ese estabilizador es un subgrupo propio porque la clase de conjugación es no trivial, por lo tanto tiene orden estrictamente menor, y por hipótesis inductiva admite un subgrupo de Sylow. El orden es el correcto. □

Otra demostración: La siguiente demostración utiliza una fórmula combinatoria, pero la ventaja es que luego el argumento es único para todos los casos, no hace falta estudiar el centro del grupo.

Sea r tal que p^r divida al orden de G pero p^{r+1} no, es decir, $|G| = p^r m$ donde m es coprimo con p. Consideramos todos los subconjuntos X de G de cardinal p^r, llamamos Ω a la colección de todos estos subconjuntos. El cardinal de Ω es el número combimatorio $\binom{|G|}{p^r} = \binom{p^r m}{p^r}$. Este número *no* es divisible por p como puede verse de diversas

maneras. Una de ellas, utilizando el pequeño teorema de Fermat: $a^p \equiv a$ modulo p para cualquier entero a, y su consecuencia en el anillo de polinomios $\mathbb{Z}_p[x]$:

$$(f(x)+1)^p = f(x)^p + 1 = f(x^p) + 1,$$

lo que implica $(x+1)^{p^r} = x^{p^r} + 1$. Ahora podemos calcular $(x+1)^{p^r m}$ de dos maneras diferentes:

$$(x+1)^{p^r m} = (x^{p^r}+1)^m = \sum_{\ell=0}^{m} x^{p^r \ell} \binom{m}{\ell}$$

o bien de la forma habitual $(x+1)^{p^r m} = \sum_{j=0}^{p^r m} x^j \binom{p^r m}{j}$. Éstas dos maneras de calcular el mismo polinomio en $\mathbb{Z}_p[x]$ nos dice que el número combinatorio $\binom{p^r m}{j}$ es cero (modulo p) a menos que j sea un múltiplo de p^r, digamos $j = p^r \ell$, y en ese caso $\binom{p^r m}{p^r \ell} \equiv \binom{m}{\ell} MOD\ p$. En particular, $\binom{p^r m}{p^r}$ es congruente a $\binom{m}{1}$ módulo p, pero $\binom{m}{1} = m$ que es coprimo con p, por lo tanto $\binom{p^r m}{p^r}$ no es divisible por p.

Volvemos ahora al teorema de Sylow. Si Ω es el conjunto formado por los subconjuntos de cardinal p^r de G, el cardinal de Ω no es divisible por p. Si consideramos la acción de G en Ω por multiplicacion a izquierda, Ω es una reunión de órbitas, y no puede ser que todas las órbitas tengan cardinal múltiplo de p porque el cardinal de Ω no es múltiplo de p. Tomamos X un elemento de Ω tal que su órbita $\mathcal{O}_X = G \cdot X$ no sea múltiplo de p. Pero $|\mathcal{O}_X| = |G|/|St_X|$, de donde se sigue que $p^r | \ |St_X|$. Si fijamos $x_0 \in X$ y consideramos $h \in St_X$, tenemos que $hx_0 \in X$ pues St_X estabiliza a X (i.e. $hX = X, \forall h \in St_X$), lo que provee de una aplicación

$$St_X \to X$$

$$h \mapsto hx_0$$

que es claramente inyectiva, por lo tanto $|St_X| \leq \#X = p^r$. Como a su vez $p^r | \ |St_X|$ se sigue que vale la igualdad, y en consecuencia $|St_X| = p^r$ es un p-subgrup de Sylow.

2. Segundo teorema de Sylow

El segundo teorema de Sylow nos dice que si S y S' son dos p-subgrupos de Sylow de G, entonces existe $x \in G$ tal que $S' = xSx^{-1}$.

Conviene comenzar con el siguiente *lema: Sea S un grupo de orden p^r y X un conjunto finito en el que S actúa. Si $|X|$ no es divisible por p, entonces X^S es no vacío, es decir, existe un elemento $x \in X$ tal que $s.x = x \forall s \in S$. Más aún $|X| \equiv |X^S|\ MOD\ p$.*

Demostración. (del Lema). A partir de la acción, la ecuación de clases nos dice que $|X| = |X|^S + \sum_{x \in X/S, x \notin X^S} |\mathcal{O}_x|$. El cardinal de $\mathcal{O}_x$ es igual al índice del estabilizador St_x, que es un divisor de $|S| = p^r$. Si la órbita es no puntual, entonces su cardinal es un múltiplo de p, de donde se obtiene $|X| \equiv |X^S|\ MODp$. □

Observación 2.1. De esta manera se muestra que un grupo de orden p^r tiene centro no trivial, y como corolario del primer teorema de Sylow se obtiene el Teorema de Cauchy: *si $p|\ |G|$ entonces existe un elemento en G de orden p*. En efecto, si $p|\ |G|$ entonces existe S un subgrupo G de orden una potencia de p. El grupo S actúa en sí mismo por conjugación, y el orden del grupo es congruente al orden de $|S^S| = |\mathcal{Z}(S)|$ módulo p, por lo tanto $\mathcal{Z}(S)$ es no trivial, su orden también es una potencia de p. Utilizamos el lema sobre grupos abelianos para encontrar un elemento en $\mathcal{Z}(S)$ de orden p, y obtenemos el elemento en G deseado.

Demostración. (Del segundo teorema de Sylow). Sean S y T son dos subgrupos de Sylow de G, es decir, sus órdenes son iguales a p^r, consideramos X el conjunto de todos los subgrupos de G que sean conjugados a T. Hacemos actuar S en X por conjugación, y chequeamos que las hipótesis del lema son satisfechas, es decir, que $p \not| |X|$. En efecto, si consideramos a G actuando en sus subgrupos por conjugación, X no es otra cosa que la órbita de S bajo esta acción, por lo tanto su cardinal es igual al índice de su estabilizador $St_S = \{g \in G : gSg^{-1} = S\} =: N_G(S)$ es el llamado *Normalizador* de S en G, que claramente contiene a S y por lo tanto $|S|$ divide a $|N_G(S)|$. El índice $[G : N_G(S)]$ es $\frac{|G|}{|N_G(S)|}$, que es un divisor de $\frac{|G|}{|S|} = \frac{p^r m}{p^r} = m$, que es coprimo con p.

Considerando la acción de T por conjugación en X (X= todos los subgrupos conjugados a S) vemos que hay por lo menos un subgrupo (conjugado a S) que es estable por la conjugación por T. Llamemos a este grupo T'. Éste subgrupo debe ser necesariamente T. En efecto, como $T \subset N_G(T')$, el conjunto $T.T' = \{x.y : x \in T, y \in T'\}$ es un subgrupo. Por el teorema de isomorfismo $\frac{TT'}{T'} \cong \frac{T}{T \cap T'}$ concluimos que el orden de TT' es una potencia de p. Pero TT' contiene a T y a T', y ambos tienen orden la potencia máxima de p, por lo tanto $T = TT' = T'$. □

3. Tercer Teorema de Sylow

El tercer teorema de Sylow nos da informacion sobre que la cantidad de p-subgrupos de Sylow de un grupo G. Retomando la notacion $|G| = p^r m$ con m coprimo con p, si n_p es la cantidad de p-subgrupos de Sylow de G, entonces el tercer teorema afirma

$$n_p | m, \quad n_p \equiv 1\ MOD p.$$

Por ejemplo, si $|G| = 20$ entonces n_5 es un divisor de 4; podria ser 1, 2, ó 4. Pero además es congruente a 1 módulo 5, luego $n_5 = 1$, hay un único 5-subgrupo de Sylow y es, por lo tanto, normal.

La demostarción del tercer teorema es consecuencia del lema mostrado en la prueba del segundo teorema y en el argumento final. Más precisamente, si X es el conjunto de todos los p-subgrupos de Sylow, $|X| = n_g$, fijado un p-subgrupo de Sylow S, éste actúa en X. Tenemos $n_p = |X| \equiv |X^S|\ MOD p$. Pero si tenemos un T que queda fijo por la conjugación por S entonces es necesariamente igual a S, luego $|X|^S = 1$, y $n_p \equiv 1\ MOD p$.

También sabemos (por el segundo teorema) que X = "todos los p-subgrupos de Sylow" coincide con la órbita por conjugación de G de un dado subgrupo de Sylow S,

ya que todos son conjugados entre sí. Luego $|X| = [G : St_S] = [G : N_G(S) = \frac{|G|}{|N_G(S)|}$, y como S está contenido en $N_G(S)$, resulta $n_p = |X| = \frac{|G|}{|N_G(S)|}$ es un divisor de $\frac{|G|}{|S|} = \frac{p^r m}{p^r} = m$.

4. Aplicaciones usuales

4.1. Grupos no simples

Ya hemos mencionado que un grupo de orden 20 no puede ser simple, pues tiene un único 5-subgrupo de Sylow, luego normal. Un ejercicio similar nos muestra que si $|G| = 84 = 2^2 \times 3 \times 7$, $n_7|12$ y $n_7 \equiv 1\ MOD\ 7 \Rightarrow n_7 = 1$.

Con un poco más de trabajo podemos ver que no hay grupos simples de orden $30 = 2 \times 3 \times 5$. Por ejemplo, n_5 es un divisor de 6, por lo tanto es 1,2,3, ó 6. A su vez $n_5 \equiv 1\ MOD 5$, por lo que las posibilidades se reducen a 1 ó 6. Por otra parte, n_3 divide a 10, luego $n_3 = 1, 2, 5, 10$. A su vez $n_3 \equiv 1\ MOD 3$ luego $n_3 = 1$ o $n_3 = 10$. Si $n_3 = 1$ o $n_5 = 1$, el grupo no sería simple, pues tendría el respectivo p-subgrupo invariante. Pero si $n_3 = 10$ y $n_5 = 6$ entonces habría $10 \times (3 - 1) = 20$ elementos de orden 3 y $6 \times (5 - 1) = 24$ elementos de orden 5. Pero el grupo tiene orden 30, asi que no puede contener a 44 elementos distintos...

Si realizamos un estudio similar para grupos de orden 60, vemos que las restricciones que nos provee el tercer teorema de Sylow no alcanza para determinar que alguno de los n_p sea 1, y de hecho, A_5 tiene orden 60 y es simple.

4.2. Grupos de orden pq

Sean $p < q$ dos números primos y G de orden pq. $n_q \equiv 1\ MODq$, es decir $n_q = 1, 1 + q, 1 + 2q, \ldots$, pero a su vez $n_q|p$, en particular es menor o igual que p, y como $p < q$, la única posibilidad es $n_q = 1$. Luego el único subgrupo de orden q es invariante, digamos $C_q = \langle x \rangle$ (es necesariamente cíclico).

Sabemos que admite un elemento de orden p, llamémoslo y, $C_p = \langle y \rangle$. Como p y q son coprimos resulta $C_p \cap C_q = \{1\}$ y el conjunto $\{x^i y^j\}$ es un subgrupo por ser $\langle x \rangle$ normal, que contiene estrictamente a C_p y a C_q, luego es igual a G. Resulta entonces que G es un producto semidirecto de $C_q\langle x \rangle$ y $C_p\langle y \rangle$.

Un análisis más detallado de las posibles acciones de C_p en $\mathrm{Aut}(C_q) \cong \mathcal{U}(\mathbb{Z}_q) \cong C_{q-1}$ (éste análisis no involucra los teoremas de Sylow) nos muestra que hay sólo dos clases de isomorfismo de grupos de orden pq: el abeliano

$$G_{ab}^{pq} = \langle x, y : x^p = 1 = y^q; xyx^{-1} = y \rangle \cong \mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq},$$

y cuando p divide a $q - 1$ (condición necesaria y suficiente para que exista un elemento de orden p en $\mathrm{Aut}C_q \cong \mathbb{Z}_{q-1}$), tenemos el grupo no abeliano

$$G_{noab}^{pq} = \langle x, y : x^p = 1 = y^q, xyx^{-1} = y^{i_0} \rangle$$

donde i_0 es tal que $i_0^p \equiv 1\ MODq$.