Algebra II (Doble grado Informática-Matemáticas)

29 de bril de 2020

1. Tema 6: G-conjuntos y p-grupos.

1.1. G-conjuntos

1.2. p-Grupos

Nos ocuparemos en la clase de hoy de la demostración del segundo teorema de Sylow.

Recordemos que para p un número primo, los p-subgrupos de un grupo G son aquellos que son p-grupos.

El primer teorema de Sylow asegura que si p es un primo divisor del orden de un grupo finito G, existe siempre al menos un p-subgrupo de orden p^i, para cada pontencia p^i que divida a $|G|$. Los p-subgrupos de orden la máxima potencia de p que divida a $|G|$ son los llamado p-subgrupos de Sylow.

Recordemos finalmente el Lema 1.8 que vimos en la clase de ayer (5-mayo-2020) que establece: Si $\mathcal{P}$ un p-subgrupo de Sylow de un grupo finito G y H un p-subgrupo de $N_G(\mathcal{P})$, entonces $H \leq \mathcal{P}$.

Teorema 1.1. *(Segundo teormea de Sylow) Sea G un grupo finito, p un número primo divisor del orden de G. Supogamos que $|G| = p^k m$, con $m.c.d.(p, m) = 1$. Sea $n_p :=$ número de p-subgrupos de Sylow de G. Entonces:*

(a) *Todo p-subgrupo de G está contenido en un p-subgrupo de Sylow de G.*

(b) *Todos los p-subgrupos de Sylow de G son conjugados (i.e., si $\mathcal{P}_1$ y $\mathcal{P}_2$ son dos p-subgrupos de Sylow de G, entonces existe $g \in G$ tal que $\mathcal{P}_2 = g\mathcal{P}_1 g^{-1}$).*

(c) $n_p | m$ *y* $n_p \equiv 1 (mod\ p)$.

Demostración. Sea

$$S = Syl_p(G) = \{\mathcal{P} \leq G / \mathcal{P} \text{ es un } p\text{-subgrupo de Sylow de } G\},$$

el conjunto de los p-subgrupos de Sylow de G. Por el primer teorema de Sylow, este conjunto es no vacío y su cardinal es $|S| = n_p$.

Para cada $\mathcal{P} \in S$ y cada $g \in G$, el conjugado $g\mathcal{P}g^{-1}$ es también un p-subgrupo de Sylow de G puesto que $|g\mathcal{P}g^{-1}| = |\mathcal{P}| = p^k$. Podemos entonces

considerar la acción de G sobre S dada por conjugación por los elementos de G, esto es

$$G \times S \to S,\ (g, \mathcal{P}) \mapsto {}^{g}\mathcal{P} := g\mathcal{P}g^{-1}.$$

Elegimos un elemento $\mathcal{P}_1 \in S$ y sea

$$T := O(\mathcal{P}_1) = \{\, {}^{g}\mathcal{P}_1 / g \in G\} = \{g\mathcal{P}_1 g^{-1} / g | in G\},$$

la órbita de $\mathcal{P}_1$.

Sabemos que T es un conjunto finito y su cardinal es $|T| = [G : Stab_G(\mathcal{P}_1)]$ (véase Teorema 1.5 en la clase del 29-abril-2020). Como

$$\begin{aligned} Stab_G(\mathcal{P}_1) &= \{g \in G / {}^{g}\mathcal{P}_i = \mathcal{P}_1\} = \{g \in G / g\mathcal{P}_1 g^{-1} = \mathcal{P}_1\} \\ &= \{g \in G / g\mathcal{P}_1 = \mathcal{P}_1 g\} = N_G(\mathcal{P}_1), \end{aligned}$$

tenemos que

$$|T| = [G : N_G(\mathcal{P}_1)].$$

A partir de la serie $\mathcal{P}_1 \leq N_G(\mathcal{P}_1) \leq G$ será $[G : \mathcal{P}_1] = [G : N_G(\mathcal{P}_1)][N_G(\mathcal{P}_1) : \mathcal{P}_1]$ y entonces $|T| = [G : N_G(\mathcal{P}_1)]$ es un divisor de $[G : \mathcal{P}_1] = m$ (pues $\mathcal{P}_1$ es un p-subgrupo de Sylow de G).

Consecuentemente

$$|T| \mid m \ \Rightarrow\ \text{m. c. d.}(|T|, p) = 1 \quad \text{ó, equivalentemente, } p \nmid |T|. \tag{1.1}$$

Veamos ahora la demostración de los apartados del teorema:

(a): Sea H un p-subgrupo de G, que suponemos no trivial. Será entonces $|H| = p^r$ con $1 \leq r \leq k$.

Por definición de T, es claro que G actúa sobre T por conjugación. Consideramos la acción de H sobre T obtenida por restricción a H de la acción de G, esto es

$$H \times T \to T,\ (h, \mathcal{P}) \mapsto {}^{h}\mathcal{P} := h\mathcal{P}h^{-1}. \tag{1.2}$$

Entonces como el comjunto de órbitas constituye una partición de T tendremos que

$$|T| = \sum_{\mathcal{P} \in T} |O(\mathcal{P})| = \sum_{\mathcal{P} \in T} [H : Stab_H(\mathcal{P})].$$

Por otro lado, para cada $\mathcal{P} \in T$, se tiene que $Stab_H(\mathcal{P}) = \{h \in H / {}^{h}\mathcal{P} = \mathcal{P}\} = \{h \in H / h\mathcal{P} = \mathcal{P}h\} = H \cap N_G(\mathcal{P})$. Puesto que $H \cap N_G(\mathcal{P})$ es un p-subgrupo de $N_G(\mathcal{P})$ (pues está contenido en H y entonces es un p-grupo), aplicando el Lema 1.8 de la clase de ayer (5-mayo-2020), tenemos que $H \cap N_G(\mathcal{P}) \leq P$ y entonces $H \cap N_G(\mathcal{P}) \leq H \cap \mathcal{P}$. Como obviamente $H \cap \mathcal{P} \leq H \cap N_G(\mathcal{P})$, concluimos que $H \cap N_G(\mathcal{P}) = H \cap \mathcal{P}$. Sustituyendo en la fórmula anterior obtenemos

$$|T| = \sum_{\mathcal{P} \in T} [H : H \cap \mathcal{P}]. \tag{1.3}$$

Analizando esta igualdad observamos que cada uno de los sumandos del segundo miembro es un divisor de $|H| = p^r$ y por tanto una potencia de p, como por (1.1) $p \nmid |T|$, entonces necesariamente existe $\mathcal{P} \in T$ tal que $[H : H \cap \mathcal{P}] = 1$, es decir, $H = H \cap \mathcal{P} \Rightarrow H \leq \mathcal{P}$, lo que demuestra (a).

(b): Sean $\mathcal{P}_1, \mathcal{P}_2$ dos p-subgrupos de Sylow de G. Tomando $H = \mathcal{P}_2$, por el apartado (a), existe $\mathcal{P} \in T$ tal que $\mathcal{P}_2 \leq \mathcal{P}$. Como tanto $\mathcal{P}_2$ y $\mathcal{P}$ son p-subgrupos de Sylow de G ambos tienen orden p^k con lo que $\mathcal{P}_2 = \mathcal{P}$.

Finalmente, como $\mathcal{P} \in T = O(\mathcal{P}_1)$ entonces existe $g \in G$ tal que $\mathcal{P} = g\mathcal{P}_1 g^{-1}$ y en definitiva $\mathcal{P}_2 = g\mathcal{P}_1 g^{-1}$, lo que demuestra (b).

(c): Por el apartado anterior los conjunto S y T coincidenm con lo que $n_p = |S| = |T|$. Aplicando entonces (1.1), obtenemos que $n_p \mid m$.

Para la congruencia, tomamos $H = \mathcal{P}_1$ en la acción (1.2), lo que nos dará lugar a la ecuación (1.3) para este caso, es decir

$$n_p = |T| = \sum_{\mathcal{P} \in T} [\mathcal{P}_1 : \mathcal{P}_1 \cap \mathcal{P}].$$

Razonando igual que en el apartado (a), existe al menos un $\mathcal{P} \in T$ tal que $[\mathcal{P}_1 : \mathcal{P}_1 \cap \mathcal{P}] = 1 \Rightarrow \mathcal{P}_1 = \mathcal{P}_1 \cap \mathcal{P} \Rightarrow \mathcal{P}_1 \leq \mathcal{P}$ y, como tienen el mismo orden (pues ambos son p-subgrupos de Sylow), entonces habrá de ser $\mathcal{P} = \mathcal{P}_1$.

Consecuentemente, en la fórmula anterior existe un único sumando cuyo valor es 1, el resto, es decir los correspondientes a $\mathcal{P} \neq \mathcal{P}_1$, tienen valor una potencia de p estrictamente positiva (pues $[\mathcal{P}_1 : \mathcal{P}_1 \cap \mathcal{P}]$ es un divisor de $|\mathcal{P}_1| = p^k$) y así, p es un divisor de $\sum_{\mathcal{P} \in T, \mathcal{P} \neq \mathcal{P}_1} [\mathcal{P}_1 : \mathcal{P}_1 \cap \mathcal{P}]$.

Concluimos entonces que $n_p \equiv 1 (mod\, p)$, lo que demuestra (c). □

Veamos un par de corolarios.

Corolario 1.2. *Sea Sea G un grupo finito y p un primo divisor del orden de G. Sea $\mathcal{P}$ un p-subgrupo de Sylow de G y sea n_p = número de p-subgrupos de Sylow de G.Son equivalentes los dos enunciados siguientes:*

(i) $n_p = 1$ (esto es $\mathcal{P}$ es el único p-subgrupo de Sylow de G)

(ii) $\mathcal{P}$ es un subgrupo normal de G.

Demostración. Puesto que cualquier conjugado de $\mathcal{P}$ es también un p-subgrupo de Sylow de G, entonces

$$n_p = 1 \Leftrightarrow g\mathcal{P}g^{-1} = \mathcal{P}, \text{ para todo } g \in G \Leftrightarrow \mathcal{P} \trianglelefteq G :$$

□

Corolario 1.3. *Sea G un grupo finito en el que todos sus subgrupos de Sylow son normales. Entonces G es el producto directo interno de sus subgrupos de Sylow.*

Demostración. Para la demostración haremos uso del siguiente resultado que os propongo como Ejercicio:

Sea G un grupo finito y $H_1, \ldots, H_k$, $k \geq 2$, subgrupos de G tales que $\text{m. c. d.}(|H_i|, |H_j|) = 1$ para todo $i \neq j$. Entonces $|H_1 H_2 \ldots H_k| = |H_1||H_2| \ldots |H_k|$.

Veamos entonces la demostración del corolario:

Sea $|G| = p_i^{n_1} p_2^{n_2} \ldots p_k^{n_k}$ la factorización en primos del orden de G. Para cada $i = 1, \ldots, k$, sea $\mathcal{P}_i$ un p_i-subgrupo de Sylow de G. Entonces, por hipótesis, $\mathcal{P}_i$ es él único p_i-subgrupo de Sylow de G y

(1) $\mathcal{P}_i \trianglelefteq G$, para todo $i = 1, \ldots, n$.

Por otro lado, puesto que $|\mathcal{P}_i| = p_i^{n_i}$, entonces $\mathrm{m.\,c.\,d.}(|\mathcal{P}_i|, |\mathcal{P}_j|) = 1$, para todo $i \neq j$. Por el resultado anterior, tenemos que $|\mathcal{P}_1 \ldots \mathcal{P}_k| = p_1^{n_1} \ldots p_k^{n_k} = |G|$, con lo que

(2) $G = \mathcal{P}_1 \ldots \mathcal{P}_k$.

Finalmente, tenemos que

(3) $(\mathcal{P}_1 \ldots \mathcal{P}_{i-1}) \cap \mathcal{P}_i = \{1\}$, para todo $i = 2, \ldots, k$.

En efecto

$$x \in (\mathcal{P}_1 \ldots \mathcal{P}_{i-1}) \cap \mathcal{P}_i \Rightarrow \begin{cases} ord(x) \mid |(\mathcal{P}_1 \ldots \mathcal{P}_{i-1})| = p_1^{n_1} \ldots p_{i-1}^{n_{i-1}} \\ ord(x) \mid |\mathcal{P}_i| = p_i^{n_1} \end{cases} \Rightarrow ord(x) = 1 \Rightarrow x = 1$$

Por definición, (1), (2) y (3) nos dicen que G es producto directo interno de $\mathcal{P}_1, \ldots, \mathcal{P}_k$ ó, en otros términos que $G \cong \mathcal{P}_1 \times \mathcal{P}_2 \times \cdots \times \mathcal{P}_k$, como queriíamos demostrar. (véase Definición 1.3 y Proposición 1.2 del 25-marzo-2020).

□