Algebra II (Doble grado Informática-Matemáticas)

5 de mayo de 2020

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

1.1. G-conjuntos

1.2. p-Grupos

En la clase de ayer introdujimos el concepto de p-grupo, para p un número primo, y demostrábamos que, en el caso finito, los p-grupos finitos son aquellos que tienen orden una potencia de p.

Estamos ahora interesados en los subgrupos de un grupo que sean p-grupos a los que llamaremos p-subgrupos.

Definición 1.1. *Sea G un grupo y p un número primo. Un subgrupo H de G que sea p-grupo lo llamaremos un p-***subgrupo**.

Nos centraremos en el resto del tema en el estudio de los p-subgrupos de grupos finitos. Veremos que la determinación de los p-subgrupos de un grupo finito y, en particular, de lo que llamaremos p-subgrupos de Sylow, nos proporciona bastante información sobre dicho grupo, como por ejemplo su resolubilidad ó su simplicidad.

Destacamos en la observación siguiente la existencia de p-subgrupos

Observación 1.2. El teorema de Cauchy (Teorema 1.7, 4-mayo-2020) nos dice que para G un grupo finito y cada primo p divisor de $|G|$ existe $a \in G$ tal que $ord(a) = p$. En otros términos, para cada primo p divisor de $|G|$, existe un subgrupo suyo de orden p y entonces un p-subgrupo de G.

El primer teorema de Sylow, que vemos a continuación, extiende el teorema de Cauchy, a las potencias de p que dividen a $|G|$.

Teorema 1.3. *(Primer teorema de Sylow) Sea G un grupo finito y ses $|G| = n$ y p un número primo. Entonces para toda potencia p^i tal que $p^i|n$, existe $H \leq G$ con $|H| = p^i$.*

Demostración. Hacemos inducción en i.

Para $i = 1$, como $p|n = |G|$ el resultado se sigue del Teorema de Cauchy.

Sea $i > 1$ con $p^i|n$, y supongamos el resultado cierto para todo grupo finito cuyo orden sea divisible por p^j con $j < i$.

Veamos entonce el caso $i > 1$: Hacemos inducción en $n = |G|$.

Como $p^i \mid n = |G|$, el primer caso es $|G| = p^i$ y entonces basta tomar $H = G$.

Sea $n > p^i$ y supongamos el resultado cierto para todo grupo de orden $m < n$ y divisible por p^i.

Veamos que también es cierto el teorema cuando $|G| > p^i$. Distinguimos dos casos:

Caso 1: Existe un subgrupo $K \lneq G$ tal que p no divive a $[G : K]$. Como $n = |G| = [G : K]|K|$, entonces necesariamente $p^i \mid |K|$ y como $|K| < n$ (pues K está propiamente contenido en G), por hipótesis de inducción en el orden del grupo, existe un subgrupo $H \leq K$, y entonces también subgrupo de G, tal que $|H| = p^i$.

Caso 2: Para todo subgrupo $K \leq G$ se tiene que $p \mid [G : K]$. Por la fórmula de las clases (fórmula (1.1) en 4-mayo-2020) sabemos que

$$|Z(G)| = |G| - \sum_{h \notin Z(G)} [G : c_G(h)],$$

y entonces p divide a $|Z(G)|$. Aplicando el Teorema de Cauchy a $Z(G)$, existirá $N \leq Z(G)$ tal que $|N| = p$.

Como $N \leq Z(G)$ entonces $N \trianglelefteq G$ (hacedlo como ejercicio)y podemos considerar el grupo cociente G/N cuyo orden es $|G/N| = \frac{|G|}{|K|} = \frac{n}{p}$, y por tanto divisible por p^{i-1}. Por hipótesis de inducción en la pontencia de p, existe $L \leq G/N$ tal que $|L| = p^{i-1}$.

Sabemos que $L = H/N$ para $N \lhd H \leq G$ (véase Proposición 1.1 del 23-marzo-2020) y entonces

$$|H| = |H/N|\,|N| = p^{i-1}p = p^i,$$

y por tanto H es el grupo buscado.

$\square$

Damos entonces la siguiente:

Definición 1.4. *Sea G un grupo finito y p un número primo divisor de $|G|$. Sea p^k la máxima potencia de p que divide al orden de G (i.e., $|G| = p^k m$ con $\text{m. c. d.}(p, m) = 1$). Todo subgrupo $\mathcal{P}$ de G con $|\mathcal{P}| = p^k$ se llamará un* **p-subgrupo de Sylow de** *G.*

En otros términos, un p-subgrupo de Sylow de G es un p-subgrupo cuyo orden es la máxima potencia de p que divide al orden de G.

Observación 1.5. Notemos que si $\mathcal{P}$ es un p-subgrupo de Sylow de G entonces

$$\text{m. c. d.}([G : \mathcal{P}], |\mathcal{P}|) = 1,$$

pues $[G : \mathcal{P}] = m$ y $|\mathcal{P}| = p^k$.

Como consecuencia del primer teorema de Sylow tenemos:

Corolario 1.6. *(Primer teorema de Sylow ”sensu strictu“) Para todo grupo finito G y todo divisor primo p de su orden, existe un p-subgrupo de Sylow.*

Veamos un par de ejemplos.

Ejemplo 1.7.

1. Sea $n \geq 2$ y consideremos el grupo cíclico $C_n = \langle x/x^n = 1 \rangle$. Supongamos que $n = p_1^{t_1} \dots p_k^{t_k}$ es la factorización en primos de n. Para cada $j = 1, \dots, k$ los p_j-subgrupos de Sylows de C_n tienen orden $p_j^{t_j}$. Como sabemos, sólo hay uno que es

$$C_{p_j^{t_j}} = \langle x^{s_j} \rangle,$$

siendo $s_j = p_1^{t_1} \dots p_{j-1}^{t_{j-1}} p_{j+1}^{t_{j+1}} \dots p_k^{t_k}$.

2. Consideremos el grupo alternado A_4. Como $|A_4| = 12 = 3 \cdot 2^2$ entonces:

   Los 3 subgrupos de Sylow de A_4 tendrán orden 3. Son pues los subgrupos cíclicos de orden 3, esto es

$$C_3 = \langle (1\ 2\ 3) \rangle, C_3' = \langle (1\ 2\ 4) \rangle, C_3'' = \langle (1\ 3\ 4) \rangle, C_3''' = \langle (2\ 3\ 4) \rangle.$$

   Los 2-subgrupos de Sylow de A_4 tendrán orden $2^2 = 4$ y entonces sólo tiene un 2-subgrupo de Sylow que es el subgrupo de Klein

$$K = \{id, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}.$$

El segundo teorema de Sylow que veremos a continuación nos dice que cualesquiera dos p-subgrupos de Sylow de un grupo son conjugados y que todo p-subgrupo está contenido en un p-subgrupo de Sylow. También establece condiciones sobre el número de p-subgrupos de Sylow que puede haber para un grupo dado.

Para la demostración del segundo teorema de Sylow, vemos primero el siguiente lema:

Lema 1.8. *Sea $\mathcal{P}$ un p-subgrupo de Sylow de un grupo G y sea H un p-subgrupo de $N_G(\mathcal{P})$. Entonces H está contenido en $\mathcal{P}$.*

Demostración. Recordemos que $N_G(\mathcal{P}) = \{g \in G/g\mathcal{P} = \mathcal{P}g\}$ y que $\mathcal{P} \trianglelefteq N_G(\mathcal{P})$ (véase Ejercicios 33 y 34 de la Relación 3).

Aplicamos el tercer teorema de isomorfía al grupo $N_G(\mathcal{P})$ y sus subgrupos $\mathcal{P} \trianglelefteq N_G(\mathcal{P})$y $H \leq N_G(\mathcal{P})$. Tendremos que $H \cap \mathcal{P} \trianglelefteq H$ y $H/(H \cap \mathcal{P}) \cong H\mathcal{P}/\mathcal{P}$. Obtenemos entonces que

$$r := [H\mathcal{P} : \mathcal{P}] = [H : H \cap \mathcal{P}].$$

Considerando la serie $\mathcal{P} \leq H\mathcal{P} \leq G$ tendremos que

$$[G : \mathcal{P}] = [G : H\mathcal{P}][H\mathcal{P} : \mathcal{P}] \Rightarrow r \mid [G : \mathcal{P}].$$

Por otro lado $|H| = [H : H \cap \mathcal{P}]|H \cap \mathcal{P}$ con lo que también $r \mid |H|$

Como $\mathcal{P}$ es un p-subgrupo de Sylow y H es un p-grupo, entonces $[G : \mathcal{P}]$ y $|H|$ son primos relativos (véase la Observación 1.5 anterior) con lo que necesariamente $r = 1$, esto es $[H\mathcal{P} : \mathcal{P}] = 1 \Rightarrow H\mathcal{P} = \mathcal{P} \Rightarrow H \leq \mathcal{P}$, como queríamos demostrar. □

En la clase de mañana demostraremos el segundo teorema de Sylow.