Algebra II (Doble grado Informática-Matemáticas)

4 de mayo de 2020

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

1.1. G-conjuntos

En la clase del miércoles de la semana pasada introducíamos los conceptos de órbita y estabilizador asociados a una acción. Concretamente para G un grupo y X un G-conjunto, definíamos la órbita de un elemento $x \in X$ como el conjunto $O(x) = \{ {}^g x / g \in G\} \subseteq X$ (recordad que dichas órbita es la clase de equivalencias del elemento x por la relación de equivalencia sobre el conjunto X asociada a la acción); mientras que el estabilizador de x como el subgrupo de G formado por aquellos elementos que dejan fijo a x, esto es, $Stab_G(x) = \{g \in G / {}^g x = x\} \leq G$.

Recordemos también que aquellos elementos $x \in X$ tales que $Stab_G(x) = G$ (o en otros términos, tales que ${}^g x = x$, $\forall g \in G$) se llaman elementos fijos por la acción y $Fix(X) = \{x \in X / {}^g x = x, \forall g \in G\} \subseteq X$ denota el conjunto de elementos fijos.

Nos ocupamos ahora de calcular órbitas y estabilizadores para tres de los ejemplos estudiados:

Ejemplo 1.1. (a) Recordemos que para cualquier grupo G, la acción por traslación de G sobre sí mismo viene dada por

$$G \times G \longrightarrow G, \quad (g, h) \mapsto {}^g h := gh.$$

Entonces, dado $h \in G$

$$O(h) = \{ {}^g h / g \in G\} = \{gh / g \in G\} = G$$

esto es $O(h) = G$ para todo $h \in G$, así pues existe una única órbita (o todas las órbitas son iguales) y por tanto la acción es transitiva (véase Definición 1.2 del 29-abril-2020). Por otro lado

$$Stab_G(h) = \{g \in G / {}^g h = h\} = \{g \in G / gh = h\} = \{1\},$$

Finalmente, el conjunto de elementos fijos por esta acción es

$$Fix(G) = \{h \in G / {}^g h = h, \forall g \in G\} = \{h \in G / gh = h, \forall g \in G\} = \emptyset.$$

(b) Sea G un grupo y consideremos la acción por conjugación de G sobre sí mismo, que recordemos está dada por

$$G \times G \longrightarrow G, \quad (g, h) \mapsto {}^g h := ghg^{-1}.$$

Entonces la órbita de un elemento $h \in G$, se llama **clase de conjugación de** h, y se denota por $cl(h)$, esto es:

$$cl(h) := O(h) = \{ {}^g h / g \in G\} = \{ghg^{-1} / g \in G\}.$$

El estabilizador de un elemento $h \in G$ por esta acción se llama el **centralizador de** h **en** G, denotado $c_G(h)$, y entonces:

$$c_G(h) := Stab_G(h) = \{g \in G / {}^g h = h\} = \{g \in G / ghg^{-1} = h\} = \{g \in G / gh = hg\}.$$

Finalmente el conjunto de elementos fijos por esta acción es

$$Fix(G) = \{h \in G / {}^g h = h, \forall g \in G\} = \{h \in G / gh = hg, \forall g \in G\} = Z(G),$$

esto es, el centro del grupo G.

Supongamos ahora que G es un grupo finito, entonces por el Teorema 1.5 de 29-abril-2020, sabemos que

$$|cl(h)| = [G : c_G(h)],$$

consecuentemente deducimos:

- El número de conjugados de h en G es $= \frac{|G|}{|C_G(h)|}$ y es un divisor de $|G|$.

Por otro lado, la la fórmula (1.2) que obtuvimos en la clase del 29-abril-2020, particularizada a este caso nos dice que

$$\boxed{\begin{array}{rcl} |G| & = & |Z(G)| + \sum_{h \notin Z(G)} |cl(h)| \\ & = & |Z(G)| + \sum_{h \notin Z(G)} [G : c_G(h)] \end{array}} \qquad (1.1)$$

Esta fórmula se conoce como **la fórmula de las clases** y veremos que tiene importantes aplicaciones en el estudio de p-grupos.

Observación 1.2. La determinación de las clases de conjugación de un grupo G es importante para el estudio de sus *representaciones* que no estudiaremos en este curso. Veamos un ejemplo de cálculo de dichas clases.

Ejercicio 9. Relación 5: Veamos quiénes son las clases de conjugación de $D_4 = \langle r, s / r^4 = 1 = s^2, sr = r^3 s\rangle = \{1, r, r^2, r^3, s, rs, r^2 s, r^3 s\}$.

Calculamos todos los productos xyx^{-1} mediante la tabla:

x	1	r	r^2	r^3	s	rs	r^2s	r^3s
$x1x^{-1}$	1	1	1	1	1	1	1	1
xrx^{-1}	r	r	r	r^3	r^3	r^3	r^3	r^3
xr^2x^{-1}	r^2	r^2	r^2	r^2	r^2	r^2	r^2	r^2
xr^3x^{-1}	r^3	r^3	r^3	r^3	r	r	r	r
xsx^{-1}	s	r^2s	s	r^2s	s	r^2s	s	r^2s
$xrsx^{-1}$	rs	r^3s	rs	r^3s	r^3s	rs	r^3s	rs
xr^2sx^{-1}	r^2s	s	r^2s	s	r^2s	s	r^2s	s
xr^3sx^{-1}	r^3s	rs	r^3s	rs	r^3s	r^3s	rs	r^3s

de donde concluimos que hay 5 clases de conjugación que son:

- $Cl(1) = \{1\}$,
- $Cl(r) = cl(r^3) = \{r, r^3\}$,
- $Cl(r^2) = \{r^2\}$,
- $Cl(s) = cl(r^2 s) = \{s, r^2 s\}$,
- $Cl(rs) = cl(r^3 s) = \{rs, r^3 s\}$.

¿Quienes son los centralizadores de lo elementos de D_4?

Veamos otro ejercicio:

Ejercicio. Ejercicio 7. Relación 5 Demostrar que si G es un grupo finito que contiene un elemento x que tiene exactamente dos conjugados, entonces G admite un subgrupo normal propio.

Resolución. Decir que x tiene exactamente dos conjugados es decir que su clase de conjugación tiene dos elementos, esto es $|cl(x)| = 2$.

Como $[G : c_G(x)] = |cl(x)| = 2$ entonces $c_G(x)$ es un subgrupo normal de G (recuérdese que todo subgrupo de índice 2 es normal) propiamente contenido en G.

Además $c_G(x)$ es no trivial pues $x \in c_G(x)$ y como $cl(x)$ tiene dos elementos entonces $x \neq 1$ (pues el único elemento cuya clase de conjugación es unitaria es el uno del grupo).

Consecuentemente, $c_G(x)$ es un subgrupo normal propio de G.

Finalmente veamos el tercer ejemplo de cálculo de órbitas y estabilizadores

Ejemplo 1.3. Sea G un grupo y consideremos la acción por conjugación de G sobre el retículo de sus subgrupos $Sub(G)$, que recordermos está definida por:

$$G \times Sub(G) \longrightarrow Sub(G), \quad (g, H) \mapsto {}^gH := gHg^{-1}.$$

Entonces, para $H \leq G$,

$$O(H) = \{ {}^gH / g \in G\} = \{gHg^{-1} / g \in G\} = \text{ subgrupos conjugados de } H \text{ en } G,$$

y entonces

$$O(H) = H \iff H \trianglelefteq G.$$

Respecto al estabilizador, este es llamado el **normalizador de H en G**, denotado por $N_G(H)$, esto es

$$N_G(H) := Stab_G(H) = \{g \in G / {}^gH = H\} = \{g \in G / gHg^{-1} = H\} = \{g \in G / gH = Hg\},$$

teniéndose entonces que

$$N_G(H) = G \iff H \trianglelefteq G.$$

Es fácil ver que H es un subgrupo normal de su normalizador, i.e. $H \trianglelefteq H_G(H)$; además $N_G(H)$ es el mayor subgrupo normal de G en el que H es normal (Véase Ejercicios 33 y 34 de la Relación 3)

El conjunto de elementos fijos por está acción es

$$\begin{aligned} Fix(Sub(G)) &= \{H \in Sub(G)/\, {}^{g}H = H, \forall g \in G\} \\ &= \{H \in Sub(G)/gHg^{-1} = H, \forall g \in G\} \\ &= \{H \in Sub(G)/H \trianglelefteq G\}. \end{aligned}$$

Finalmente, supongamos ahora que G es un grupo finito, entonces aplicando de nueve el Teorema 1.5 de 29-abril-2020, tendremos que

$$|O(H)| = [G : N_G(H)],$$

y concluimos entonces que

- el número de conjugados de un grupo H es un divisor de $|G|$ y coincide con índice de su normalizador.

1.2. p-grupos.

Introducimos en esta sección los conceptos de p-grupo y de p-subgrupo para cuyo estudio serán importante los resultados anteriores relativos a G-conjuntos

Definición 1.4. *Sea p un número primo. Un grupo finito G (no trivial) se dice un* **p-grupo** *si el orden de todo elemento de G es una potencia de p.*

Ejemplo 1.5.

1. El grupo cíclico c_{p^n}, $n \geq 1$ es un p-grupo pues si $x \in C_{p^n}$ entonces $ord(x)|p^n$, con lo que $ord(x) = p^m$ con $m \leq n$.

2. Sea $G = C_p \times \overset{n)}{\ldots} \times C_p$, el producto directo del grupo cíclico C_p con sigo mismo n veces, $n \geq 1$. Entonces si $x = (x_1, \ldots, x_n) \in G$ sabemos que $ord(x) = \text{m. c. m.}\{ord(x_1), \ldots, ord(x_n)\}$. Como para todo $i = 1, \ldots, n$, $x_i \in C_p$ será
$$orde(x_i) = \begin{cases} 1 = p^0, & \text{si } x_i = 1 \\ p, & \text{si } x_i \neq 1, \end{cases}$$
con lo que $ord(x) = \text{m. c. m.}\{ord(x_1), \ldots, ord(x_n)\} = p^m$, con $m \leq n$. Consecuentemente se trata de un p-grupo.

Observación 1.6. Notemos que en el ejemplo 2 anterior podríamos haber procedido como en el ejemplo 1. Concretamente, exactamente el mismo que en el ejemplo 1 nos dice que si G es un grupo con $|G| = p^n$, p un número primo y $n \geq 1$, entonces G es un p-grupo. El teorema de Cauchy que demostramos a continuación nos permitirá demostrar el recíproco para grupos finitos.

Teorema 1.7. *(Teorema de Cauchy:) Sea G un grupo finito. Para todo divisor primo p de $|G|$, existe un elemento de G de orden p (y entonces un subgrupo de orden p, el generado por dicho elemento).*

Demostración. Sea

$$X := \{(x_1, \ldots, x_p) \in G \times \overset{p)}{\ldots} \times G / x_1 x_2 \ldots x_p = 1\}.$$

Es claro que si $|G| = n$ entonces $|X| = n^{p-1}$.

Sea $\sigma = (1\,2\,\ldots\,p) \in S_p$ y $H = \langle\sigma\rangle = \{\sigma^j / 0 \leq j \leq p-1\}$

Definimos una acción de H sobre el conjunto X:

$$H \times X \to X,\ (\sigma^j, (a_1, \ldots, a_p)) \mapsto {}^{\sigma^j}(a_1, \ldots, a_p)$$

por recurrencia como sigue:

$$\begin{cases} {}^{id}(a_1, \ldots, a_p) = (a_1, \ldots, a_p) \\ {}^{\sigma}(a_1, \ldots, a_p) = (a_{\sigma(1)}, \ldots, a_{\sigma(p)}) = (a_2, \ldots, a_p, a_1) \\ {}^{\sigma^j}(a_1, \ldots, a_p) = {}^{\sigma}({}^{\sigma^j}(a_1, \ldots, a_p)) = (a_{j+1}, \ldots, a_p, a_1, \ldots, a_j) \text{ para } 2 \leq j \leq p-1. \end{cases}$$

(Ejercicio: demostrar que se trata en efecto de una acción de H sobre X).

Veamos cuáles son los elementos fijos por esta acción: Para ello, calculamos, para cada $(a_1, \ldots, , a_p) \in X$, su órbita por esta acción, esto es $O((a_1, \ldots, , a_p)) = \{ {}^{\sigma^j}(a_1, \ldots, , a_p) / 0 \leq j \leq p-1\}$ con lo que

$$O((a_1, \ldots, , a_p)) = \\ = \{(a_1, \ldots, , a_p), (a_2, a_3 \ldots, , a_p, a_1), (a_3, a_4 \ldots, , a_p, a_1, a_2) \ldots, (a_p, a_1, \ldots, a_{p-1})\},$$

y entonces, según vimos en la Observación 1.8 de la clase del 29-abril-2020,

$$\begin{aligned} (a_1, \ldots, , a_p) \in Fix(X) &\iff O((a_1, \ldots, , a_p)) = \{(a_1, \ldots, , a_p)\} \\ &\iff a_1 = a_2 = \cdots = a_p \end{aligned}$$

Por tanto al menos hay un elemento fijo. Basta considerar el elemento $(1, 1, \ldots, 1) \in X$.

Por otro lado si $(a_1, \ldots, , a_p) \notin Fix(X)$ entonces $O((a_1, \ldots, , a_p))$ tiene mas de un elemento y como $|O((a_1, \ldots, , a_p))|$ es un divisor de $|H| = p$ (véase Teorema 1.5 del 29-abril-2020), necesariamente habrá de ser $|O((a_1, \ldots, , a_p))| = p$.

Sabemos que (véase fórmula (1.2) en Observación 1.8 de la clase del 29-abril-2020)

$$|X| = |Fix(X)| + \sum_{(a_1, \ldots, ap) \notin Fix(X)} |O((a_1, \ldots, a_p))|$$

y entonces si r el número de elementos fijos y s el número de órbitas no unitarias (y entonces de cardinal p), tendremos

$$|X| = n^{p-1} = r + sp.$$

Como $p|n$ entonces que $p|(n^{p-1} - sp)$, es decir $p|r$ y por tanto $r \geq 2$. Consecuentemente existe $(a, , a, \ldots, , a) \in Fix(X)$ distinto del elemento $(1, , 1 \ldots, 1)$. Pero por definición del conjunto X, si $(a, a, \ldots, a) \in X$ entonces $a^p = 1$. Consecuentemente, $\exists a \in G$, $a \neq 1$, tal que $a^p = 1$ y entonces $ord(a) = p$, lo que acaba la demostración. □

Como primera aplicación de este teorema deducimos que los p-grupos finitos son aquellos cuyo orden es una potencia de p.

Corolario 1.8. *Sea p un número primo y G un grupo finito no trivial. Entonces*

$$G \text{ es un } p\text{-grupo} \iff |G| = p^n \text{ para algún } n \geq 1.$$

Demostración. La implicación hacia la izquierda ya la hemos visto en la Observación 1.6 de esta clase.

Veamos la implicación hacia la derecha: Supongamos G un p-grupo. Por definición todo elemento de G tiene orden una potencia de p.

Sea q un número primo divisor de $|G|$. Por el teorema de Cauchy, existe $a \in G$ tal que $ord(a) = q$. Como G es un p-grupo, habrá de ser $ord(a) = p^r$, $r \geq 1$. Entonces $q = ord(a) = p^r \Rightarrow r = 1$, y $p = q$.

Consecuentemente p es el único primo que divide a $|G|$ con lo que $|G| = p^n$, para algún, $n \geq 1$. □

Otro teorema importante en la teoría de p-grupos es el siguiente:

Teorema 1.9. *(Teorema de Burnside) Sea p un número primo. Si G es un p-grupo finito no trivial entonces $|Z(G)| \geq p$. En particular $Z(G)$ es un subgrupo no trivial de G.*

Demostración. Supongamos que $|G| = p^n$ con $n \geq 1$.

Si G es abeliano entonces $Z(G) = G$, con lo que $|Z(G)| = p^n \geq p$.

Supongamos G no abeliano, entonces $Z(G)$ es un subgrupo propiamente contenido en G, Por la fórmula (1.1) de las clases, sabemos que

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

Ahora, si $h \notin G$ entonces $[G : c_G(h)] \geq 1$ (pues si $[G : c_G(h)] = 1 \Rightarrow G = c_G(h) \Rightarrow h \in Z(G)$). Como $[G : c_G(h)]$ es un divisor del orden de $|G| = p^n$, entonces $[G : c_G(h)] = p^r$ con $1 \leq r \leq n$. Consecuentemente p es un divisor de $[G : c_G(h)]$, para todo $h \notin Z(G)$ con lo que p divide a $\sum_{h \notin Z(G)} [G : c_G(h)]$

Concluimos entonces que p es un divisor de $|G| - \sum_{h \notin Z(G)} [G : c_G(h)] = |Z(G)|$ con lo que $|Z(G)| \geq p$ y es por tanto un subgrupo no trivial de G, como queríamos demostrar. □

Destacamos dos corolarios al teorema de Burside

Corolario 1.10. *Sea p un número primo y G un grupo con $|G| = p^2$, entonces G es un grupo abeliano.*

Demostración. Por el teorema de Burnside $Z(G)$ es un subgrupo no trivial de G. Entonces $|Z(G)| = p$ ó $|Z(G)| = p^2$.

Si $|Z(G)| = p$ será $Z(G)$ un subgrupo propiamente contenido en G. Entonces existirá un elemento $a \in G$ tal que $a \notin Z(G)$. Como $Z(G) \leq c_G(a) = \{g \in G / ga = ag\}$ y $a \in c_G(a)$ entonces también $Z(G)$ es un subgrupo propio de $c_G(a)$, así habrá de ser $|c_G(a)| = p^2$ (pues como para el centro, $c_G(a)$ es un subgrupo no trivial de G y $|c_G(a)| > p$). Pero entonces $c_G(a) = G \Rightarrow a \in Z(G)$, lo que es una contradicción.

Consecuentemente, $|Z(G)| = p^2 \Rightarrow G = Z(G)$. Esto es, G es abeliano, como queríamos demostrar.

□

Finalmente tenemos

Corolario 1.11. *Todo p-grupo finito es resoluble*

Demostración. Supongamos G un p-grupo finito y sea $|G| = p^n$, $n \geq 1$.

Hacemos inducción en n. Si $n = 1$, entonces $|G| = p \Rightarrow G \cong C_p$, el grupo cíclico de orden p, con lo que G es abeliano y por tanto resoluble.

Sea $n > 1$ y supongamos que todo p-grupo de orden $< p^n$ es resoluble.

En primer lugar si G es abeliano entonces es resoluble y no hay nada que demostrar. Supongamos pues que G no abeliano.

Consideramos $Z(G)$. Sabemos que $Z(G)$ es un subgrupo normal de G y, por el teorema de Burnside, es un subgrupo no trivial de G. Entonces $|Z(G)| = p^r$ con $1 \leq r < n$ (pues $Z(G)$ está propiamente contenido en G) y, por hipótesis de inducción, $Z(G)$ es resoluble. Como $|G/Z(G)| = p^{n-r}$ con $n - r < n$ (pues $r > 1$), también por hipótesis de inducción, $G/Z(G)$ es resoluble.

Aplicando el apartado 2 de la Proposición 1.4 de la clase del 15-abril-2020, como $Z(G) \trianglelefteq G$ siendo $Z(G)$ y $G/Z(G)$ resolubles. entonces G es también resoluble, cómo queríamos demostrar. □