

PAUTA AYUDANTÍA 3 ESTRUCTURAS ALGEBRAICAS

28 DE MARZO DE 2023

Problema 1. (Lema de Cauchy) Sea G un grupo finito y p un número primo que divide a $|G|$. Considere el conjunto

$$X = \{(g_1, \dots, g_p) \in G^p \mid g_1 \cdots g_p = 1\}$$

Defina una acción de grupo conveniente de $\mathbb{Z}/p\mathbb{Z}$ en X y demuestre que G posee un elemento de orden p .

Demostración. Sea $G = \mathbb{Z}/p\mathbb{Z}$ y definamos la acción de grupo

$$G \curvearrowright X, \quad k \cdot (g_1, \dots, g_p) = (g_{1+k}, \dots, g_{p+k})$$

es decir, esta acción permuta las coordenadas de un elemento en X de manera cíclica. Veamos primero que esta acción está bien definida, es decir, si $x \in X, k \in G$ entonces $k \cdot x \in X$. Sea $(g_1, \dots, g_p) = 1$. Por definición tenemos $g_1 \cdots g_p = 1$. Multiplicando por inversos tenemos que

$$g_2 \cdots g_p = g_1^{-1} \Rightarrow g_2 \cdots g_p g_1 = 1 \Rightarrow g_{1+k} \cdots g_{p+k} = 1$$

y por tanto la acción está bien definida. Podemos entonces emplear la fórmula de clases para esta acción, obteniendo que

$$|X| = \sum_{x \in R} [G : G_x] = |X^G| + \sum_{x \in R \setminus \{X^G\}} [G : G_x]$$

donde R es un conjunto que contiene un elemento por cada órbita, y X^G denota el conjunto de puntos fijos de la acción. A continuación, notemos que $|X| = |G|^{p-1}$ puesto que para obtener un elemento de X podemos fijar las primeras $p-1$ coordenadas, y definir la última coordenada como $g_p = (g_1 \cdots g_{p-1})^{-1}$. Además, dado que $|G| = p$ es primo y $G_x \leq G$, si $x \notin X^G$ no es punto fijo de la acción entonces su estabilizador es trivial y así $G_x = \{1\}$. Obtenemos así desde la fórmula de clases que

$$p^{p-1} = |X| = |X^G| + p|(X/H) \setminus X^H|$$

y en consecuencia p divide a $|X^G|$. Ahora, $X^G \neq \emptyset$ puesto que $(1, \dots, 1) \in X^G$, así que existe $x \in X^G$ no trivial, el cual por ser punto fijo debe ser de la forma (g, \dots, g) y verificar $g^p = 1$. Como p es primo este elemento es de orden p . \square

Problema 2. Sea G un grupo finito actuando sobre un conjunto finito X . Defina el conjunto

$$E := \{(g, x) \in G \times X \mid g \cdot x = x\}$$

y para cada $g \in G$ defina su conjunto de puntos fijos

$$\text{Fix}(g) := \{x \in X \mid g \cdot x = x\}$$

Demuestre que

$$\frac{1}{|G|} \sum_{g \in G} |\text{Fix}(g)| = |X/G|$$

donde X/G denota el conjunto de órbitas de la acción $G \curvearrowright X$. ¿Qué significa lo anterior en el caso de acciones transitivas?

Demostración. Notar que podemos escribir el conjunto E como una unión disjunta de dos manera diferentes:

$$Y = \bigsqcup_{x \in X} \{g | g \cdot x = x\} = \bigsqcup_{g \in G} \{x \in X | g \cdot x = x\}$$

Notando que los conjuntos de la izquierda corresponden a los estabilizadores y los de la derecha a los conjuntos de puntos fijos tenemos

$$|Y| = \sum_{x \in X} |G_x| = \sum_{g \in G} |\text{Fix}(g)|$$

Tenemos así por el teorema de Lagrange que

$$\frac{1}{|G|} \sum_{g \in G} |\text{Fix}(g)| = \sum_{x \in X} \frac{|G_x|}{|G|} = \sum_{x \in X} \frac{1}{[G : G_x]}$$

Dado que la suma de la derecha se extiende por todo x , y que tenemos una biyección $G/G_x \xrightarrow{\sim} G_x$, es que obtenemos la conclusión:

$$\frac{1}{|G|} \sum_{g \in G} |\text{Fix}(g)| = |X/G|$$

Si G actúa sobre X de manera transitiva, tenemos entonces que X/G , y la fórmula anterior nos dice que el promedio de puntos fijos que poseen los elementos de G es 1. \square

Problema 3. Sea G un grupo.

1. Suponga que G es finito y sea p el divisor primo minimal de $|G|$. Pruebe que todo subgrupo de G con índice p es normal.
2. Suponga ahora que G es infinito y que este posee un subgrupo estricto $H \leq G$ de índice finito. Demuestre que G no es simple.

Demostración.

1. Sea H subgrupo de G de orden p . Podemos definir una acción de grupo natural de G sobre G/H como

$$G \curvearrowright G/H, \quad x \cdot gH = (xg)H$$

la cual se traduce en un morfismo de grupos $\varphi : G \rightarrow \text{Biy}(G/H)$ donde $\text{Biy}(G/H)$ denota el grupo de biyecciones del conjunto G/H . Sea $K := \ker(\varphi)$ y notemos que

$$k \in K \Rightarrow \varphi(k)(H) = kH = H \Rightarrow K \subseteq H$$

y denotemos $n := [H : K]$ el índice de K en H . Gracias a la propiedad universal del cociente tenemos que

$$G/K \hookrightarrow \text{Biy}(G/H) \Rightarrow [G : K] \text{ divide a } p!$$

puesto que $|\text{Biy}(G/H)| = p!$ y lo anterior implica que G/K es isomorfo a un subgrupo de $\text{Biy}(G/H)$. Ahora, empleando la fórmula multiplicativa de índices de subgrupos tenemos

$$[G : K] = [G : H][H : K] = np \text{ divide a } p!$$

deduciendo que $n|(p-1)!$. Ahora, dado que p es el primo más pequeño que divide al orden de G tenemos que todo divisor primo de n debe ser más grande que p (pues n divide al orden de G), pero $n|(p-1)!$ así que necesariamente $p = 1$. En consecuencia $H = K$ y dado que corresponde al kernel de un morfismo de grupos este subgrupo resulta ser normal.

2. Podemos considerar nuevamente $X := G/H$ y la acción de grupo $\varphi : G \rightarrow \text{Biy}(X)$ del punto anterior. Notemos que esta acción es transitiva, puesto que para cada par de clases $g_1H, g_2H \in X$ podemos considerar $g := g_2g_1^{-1} \in G$ y notar que $g \cdot (g_1H) = (g_2g_1^{-1}g_1)H = g_2H$, es decir, esta acción posee una única órbita. Esto se traduce entonces en que el morfismo asociado es no trivial, así que su kernel es un subgrupo normal estricto de G . Ahora, como G es infinito y $\text{Biy}(X)$ es un conjunto finito (pues por hipótesis X es finito) este morfismo no puede ser inyectivo y en consecuencia su kernel es no trivial. Así, hemos encontrado un subgrupo normal no trivial de G y así este grupo no puede ser simple. □

Problema 4. Sea G grupo finito y $G \curvearrowright X$ una acción sobre un conjunto finito X . Suponga que para todo $g \in G \setminus \{e\}$ existe un único $x \in X$ tal que $g \cdot x = x$.

1. Defina $Y := \{x \in X \mid \text{Stab}_G(x) \neq \{e\}\}$. Muestre que Y es estable bajo la acción de G .
2. Denote $n = |Y \setminus G|$ el número de órbitas de Y bajo la acción de G y una colección de elementos $y_1, \dots, y_n \in Y$, uno por cada órbita, y denote $m_i = |\text{Stab}_G(y_i)|$. Definiendo el conjunto $Z = \{(g, x) \in (G \setminus \{e\}) \times Y \mid g \cdot x = x\}$, demuestre que

$$1 - \frac{1}{|G|} = \sum_{i=1}^n \left(1 - \frac{1}{m_i}\right)$$

3. Deduzca que $n = 1$ y concluya que X tiene un único punto fijo bajo la acción de G .

Demostración.

1. Para probar que Y es estable basta con recordar que puntos en una misma órbita tienen estabilizadores conjugados, es decir, $G_{g \cdot x} = gG_xg^{-1}$. De esta manera, si $x \in Y$, como $\text{Stab}_G(x) \neq \{e\}$ entonces claramente $\text{Stab}_G(g \cdot x) \neq \{e\}$ así que $g \cdot x \in Y$.
2. Para este punto consideramos el conjunto

$$Z = \{(g, x) \in (G \setminus \{e\}) \times Y \mid g \cdot x = x\}$$

Imitando la estrategia del Problema 2 y reagrupando los términos en la misma órbita tenemos

$$|G| - 1 = \sum_{y \in Y} (|\text{Stab}_G(y_i)| - 1) = \sum_{i=1}^n |G_{y_i}| (|\text{Stab}_G(y_i)| - 1) = \sum_{i=1}^n |G| \left(1 - \frac{1}{m_i}\right)$$

y dividiendo por $|G|$ se obtiene el resultado deseado.

3. Por definición de Y , para cada i tenemos que $m_i \geq 2$ y entonces

$$1 > 1 - \frac{1}{|G|} = \sum_{i=1}^n \left(1 - \frac{1}{m_i}\right) \geq \frac{n}{2}$$

deduciendo que $n < 2$ y por lo tanto $n = 1$. Volviendo a la fórmula encontrada anteriormente, esta nos dice ahora que $|G| = m_i = |\text{Stab}_G(y_1)|$ (eligiendo sin pérdida de generalidad y_1) así que $\text{Stab}_G(y_1) = G$ que significa que y_1 es un punto fijo de la acción de G . □

Problema 5. Considere el cuerpo finito $G = \mathbb{F}_p$ con p primo y su espacio proyectivo $\mathbb{P}^n(\mathbb{F}_p)$. Demuestre que

$$|\mathbb{P}^n(\mathbb{F}_p)| = 1 + p + p^2 + \dots + p^n$$

Demostración. Recordemos que podemos definir $\mathbb{P}^n(\mathbb{F}_p)$ como el cociente de una acción de grupo. En general, si k es un cuerpo definimos la acción del grupo multiplicativo k^\times sobre k^{n+1} mediante reescalamiento $\lambda \cdot (x_1, \dots, x_n) = (\lambda x_1, \dots, \lambda x_n)$. En particular, podemos considerar el cuerpo $k = \mathbb{Z}/p\mathbb{Z}$, cuyo grupo de unidades sabemos que cumple $|(\mathbb{Z}/p\mathbb{Z})^\times| = p - 1$. Además, es claro que el único punto fijo de esta acción es 0, y el resto de puntos $x \in (\mathbb{Z}/p\mathbb{Z})^{n+1}$ cumple que su órbita posee p elementos (pues disponemos de $p - 1$ escalares para multiplicar). Recordando que siempre disponemos de una biyección $G/G_x \xrightarrow{\sim} Gx$, todo lo anterior junto a la fórmula de clases nos dice que

$$\begin{aligned} |(\mathbb{F}_p)^{p+1}| &= |(\mathbb{F}_p)^G| + \sum_{x \in k^{n+1} \setminus \{0\}} [G : G_x] \\ &= 1 + (p - 1)|\mathbb{P}^n(\mathbb{F}_p)| \end{aligned}$$

de donde deducimos

$$|\mathbb{P}^n(\mathbb{F}_p)| = \frac{p^{n+1} - 1}{p - 1} = 1 + p + p^2 + \dots + p^n$$

□