Ayudantia 5

Profesor: Cristóbal Rivas
Ayudantes: Benajamin Martinez, Javier Pavez

Viernes 02 de Septiembre 2022

Problema 7.1: Sea G un grupo. Consideremos la acción por conjugación de G sobre G . Demostrar:

a) Sea $x \in G$, $Stab_G(x) = G$ si y solo si $x \in Z(G)$.

Demostración. Por definición de estabilizador, $Stab_G(x) = G$ si y solo si $g.x = x \forall g \in G$ (1).

Por definición de nuestra acción, (1) es equivalente a $g x g^{-1} = x \forall g \in G$ (2).

Como estamos trabajando en nuestro grupo G , (2) es equivalente a $g x = x g \forall g \in G$ (3).

Finalmente, por definición de centro, (3) es equivalente a $x \in Z(G)$. □

b) $\sum_{x_i \in Z(G)} [G : Stab_G(x_i)] = |Z(G)|$. Si $|Z(G)|$ es finito.

Demostración. Observemos las siguientes igualdades. Por el problema 7.1 a), obtenemos la primera igualdad. La segunda igualdad la conseguimos ya que solo hay una clase lateral. La última igualdad, se da recordando la hipótesis, $|Z(G)|$ es finito.

$$\begin{aligned} \sum_{x_i \in Z(G)} [G : Stab_G(x_i)] &= \sum_{x_i \in Z(G)} [G : G] \\ &= \sum_{x_i \in Z(G)} 1 \\ &= |Z(G)| \end{aligned}$$

□

c) $Z(G) \subset Stab_G(x), \forall x \in G$.

Demostración. Sea $x \in G$ fijo (puede ser cualquiera). Demostraremos que $g \in Z(G) \implies g \in Stab_G(x)$.

Sea $g \in Z(G)$ fijo (puede ser cualquier). Luego, por definición de centro, $g y = y g \forall y \in G$. En particular, lo anterior se cumple para nuestro x , o sea, $g x = x g$. Como trabajamos en nuestro grupo G , tenemos que $g x g^{-1} = x$. Recordando la acción con la que estamos trabajando, $g.x = x$. Finalmente, por definición de estabilizador, $g \in Stab_G(x)$.

Como nuestro g puede ser cualquier elemento de $Z(G)$, deducimos que $Z(G) \subset Stab_G(x)$. Como x puede ser cualquier elemento de G , concluimos que $Z(G) \subset Stab_G(x) \forall x \in G$. □

Problema 7.2: Sean p un numero primo y G un grupo de cardinalidad p^3 no abeliano. Considerando la acción por conjugación de G sobre G . Demostrar:

a) Existe al menos un grupo G con esas cualidades.

Demostración. Solo debemos recordar a Q_8 , de la primera ayudantía. Que tiene cardinalidad 2^3 y no es abeliano. □

b) $|Z(G)| = p$.

Demostración. Por Lagrange, sabemos que $|Z(G)| \mid |G|$. Luego, $|Z(G)| \in \{1, p, p^2, p^3\}$. Como sabemos que existe un grupo G con esas cualidades, demostraremos lo pedido descartando las otras opciones.

$|Z(G)| = 1$: Este caso contradice el Lema 1.95. de los apuntes del curso. Por lo que este caso esta descartado. ✓

$|Z(G)| = p^2$: Como $Z(G) \triangleleft G$, tenemos que $G/Z(G)$ es un grupo. Como G tiene cardinalidad finita, podemos usar Lagrange para ver que $|G/Z(G)| = [G : Z(G)] = \frac{|G|}{|Z(G)|} = \frac{p^3}{p^2} = p$. Luego, por el ejercicio 1. de la ayudantía 4, $G/Z(G)$ es cíclico. Finalmente, por el ejercicio 2. de la ayudantía 4, G es abeliano. Lo que contradice la hipótesis y por ende descarta este caso. ✓

$|Z(G)| = p^3$: En este caso, como $Z(G) \subset G$ y $|G| = p^3$, necesariamente $G = Z(G) := \{g \in G; gx = xg \forall x \in G\}$. Luego, $gx = xg \forall g, x \in G$. Lo que contradice nuestra hipótesis de que G no es abeliano y por ende descarta este caso. ✓

Finalmente, por descarte, necesariamente $|Z(G)| = p$. □

c) $|Stab_G(x)| = p^2, \forall x \in G - Z(G)$.

Demostración. Sea $x \in G - Z(G)$ fijo (puede ser cualquiera).

Por Lagrange, sabemos que $|Stab_G(x)| \mid |G|$. Luego, $|Stab_G(x)| \in \{1, p, p^2, p^3\}$. Como sabemos que existe un grupo G con esas cualidades, demostraremos lo pedido descartando las otras opciones.

$|Stab_G(x)| = 1$: Dado que trabajamos con la acción por conjugación, tenemos que $id_G \cdot x = id_G \cdot x \cdot (id_G)^{-1} = x$ y $x \cdot x = x \cdot x \cdot x^{-1} = x$. Luego, hay dos elementos que pertenecen al estabilizador de x .

A priori estos dos elementos pueden ser iguales, pero $x \notin Z(G)$ por hipótesis, y $id_G \in Z(G)$ porque $Z(G)$ es un subgrupo de G . Por lo que hay dos elementos distintos que pertenecen al estabilizador y por ende este caso es inverosímil. ✓

$|Stab_G(x)| = p$: Consideremos el problema 7.1 c) y el problema 7.2 b), por ambos, necesariamente $Stab_G(x) = Z(G)$. Pero anteriormente dijimos que $x \in Stab_G(x)$ y $x \notin Z(G)$, por lo que no pueden ser iguales y por ende este caso es inverosímil. ✓

$|Stab_G(x)| = p^3$: Como $Stab_G(x) \subset G$ y G tiene cardinalidad p^3 , necesariamente $Stab_G(x) = G$. Pero por el problema 7.1 a), esto contradice nuestra hipótesis de que $x \notin Z(G)$. Por lo que este caso se da por descartado. ✓

Finalmente, por descarte, necesariamente $|Stab_G(x)| = p^2$. □

d) Escribir la ecuación de clases de G .

Demostración. La ecuación de clase nos dice (1):

$$|G| = \sum_{i=1}^n |C(g_i)| \quad (1)$$

Donde $\{g_1, g_2, \dots, g_n\}$ es un conjunto que fijaremos, tal que $C(g_i) \cap C(g_j) = \emptyset$ cuando $i \neq j$, y $G = \cup_{i=1}^n C(g_i)$. Notar que podemos asegurar que son finitos g 's porque G es finito.

Ahora, por la proposición 1.87 de los apuntes de la clase, tenemos que $|C(g_i)| = [G : Stab_G(g_i)]$ para todo i . Luego, notemos que si para algún i , $g_i \in Z(G)$, entonces en el problema 7.1 b) nos dimos cuenta que $|C(g_i)| = [G : Stab_G(g_i)] = [G : G] = 1$. Además, como $g_i \cdot g_i = (g_i) \cdot (g_i) \cdot (g_i)^{-1} = g_i$, deducimos que $C(g_i) = \{g_i\}$. Esto significa que los elementos del centro no están en ninguna otra clase de conjugación.

Por la elección de nuestros g 's, necesariamente deben estar todos los elementos del centro, por lo que nuestros g 's nos quedan $\{g_1, g_2, \dots, g_n\} = (\cup_{x \in Z(G)} \{x\}) \cup (\cup_{i=1}^m \{x_i\}) = Z(G) \cup (\{x_1, x_2, \dots, x_m\})$. Donde $x_i \notin Z(G)$ para todo i y cumplen las mismas propiedades que los g 's (ya que podemos escogerlos como correspondientes g 's). Notar que existe algún x , ya que demostramos que el centro del grupo no es todo el grupo.

Así, nuestra ecuación de clase nos queda

$$\begin{aligned} |G| &= \sum_{i=1}^n |C(g_i)| \\ &= \sum_{x \in Z(G)} |C(x)| + \sum_{i=1}^m |C(x_i)| \end{aligned}$$

Que por el problema 7.1 b) obtenemos

$$= |Z(G)| + \sum_{i=1}^m |C(x_i)|$$

Como los $x_i \notin Z(G)$ y $|C(x_i)| = [G : \text{Stab}_G(x_i)]$, el problema 7.2 c) nos dice que $|C(x_i)| = [G : \text{Stab}_G(x_i)] = \frac{|G|}{|\text{Stab}_G(x_i)|} = \frac{p^3}{p^2} = p$. Además, el problema 7.2 b) nos dice que $Z(G) = p$. Luego, nuestra ecuación de clase nos queda

$$\begin{aligned} |G| &= |Z(G)| + \sum_{i=1}^m |C(x_i)| \\ &= p + \sum_{i=1}^m p \\ &= p + mp \end{aligned}$$

Así solo nos queda la duda de cuanto vale m , o sea, cuantas clases de conjugación de elementos que no están en el centro hay. Como $|G| = p^3$, solo hay que despejar m , y nos queda (2) (para el gusto de cada quien).

$$\begin{aligned} |G| &= p + \underbrace{p + \cdots + p}_{\frac{p^3-p}{p}} \\ &= \underbrace{1 + \cdots + 1}_p + \underbrace{p + \cdots + p}_{\frac{p^3-p}{p}} \end{aligned} \quad (2)$$

Nota: Esto significa que hay $p^2 + p - 1$ -clases de conjugación. □

Problema 7.3: Sea G un grupo cíclico.

a) Demostrar que existe un epimorfismo de $\mathbb{Z}$ a G .

Demostración. Por definición de grupo cíclico, $\exists a \in G$ el cual fijaremos, tal que $G = \{a^n \mid n \in \mathbb{Z}\}$. Luego, un epimorfismo natural que se nos puede ocurrir es $\varphi : \mathbb{Z} \rightarrow G, n \mapsto a^n$. Por lo que demostraremos que este es efectivamente un epimorfismo buscado.

Lo primero es demostrar que está bien definida, o sea, que efectivamente es una función.

Dado que: Puede tomar cualquier elemento de los enteros, por la definición de potencia en un grupo; siempre llegará a G , ya que por hipótesis es un grupo; la regla de asignación esta automáticamente bien definida, porque no hay dos maneras distintas de escribir un mismo entero. Necesariamente está bien definida.

De todas formas, esa última condición vamos a probarla de una manera más formal. Sean $m, n \in \mathbb{Z}$ tal que $m = n$, necesariamente tenemos que $\varphi(m) = a^m = a^n = \varphi(n)$. Donde la segunda igualdad se tiene porque las potencias están bien definidas para los enteros. ✓

En segundo lugar, demostraremos que es un homomorfismo, ocupando propiedades de potencias en un grupo.

Sean $n, m \in \mathbb{Z}$. Luego, $\varphi(n+m) = a^{n+m} = a^n a^m = \varphi(n)\varphi(m)$. Como m, n eran cualquier entero, por definición es un homomorfismo. ✓

En último lugar, pero no menos importante, debemos verificar sobreyectividad. Esto quiere decir: $\forall g \in G, \exists n_g \in \mathbb{Z}$ tal que $\varphi(n_g) = g$.

Ocupamos la definición de grupo cíclico, para recordar que si $g \in G$, entonces existe un $n_g \in \mathbb{Z}$ tal que $g = a^{n_g}$. Luego, $\varphi(n_g) = a^{n_g} = g$, lo que demuestra lo pedido. ✓

Concluimos que φ es un epimorfismo, que es lo que buscábamos. □

b) Demostrar que $G \cong \mathbb{Z}/n\mathbb{Z}$, para algún $n \in \mathbb{N}_0$.

Demostración. Considerando el epimorfismo anterior, por el primer teorema de isomorfía conseguimos que $\text{Im}(\varphi)/\ker(\varphi) \cong G$.

Dado que la función es sobreyectiva, $\text{im}(\varphi) = \mathbb{Z}$. Dado que $\text{Ker}(\varphi)$ es un subgrupo de $\mathbb{Z}$, de la primera ayudantía obtenemos que $\text{Ker}(\varphi) = n\mathbb{Z}$, para algún $n \in \mathbb{N}_0$.

Luego, $\mathbb{Z}/n\mathbb{Z} = \text{Im}(\varphi)/\ker(\varphi) \cong G$, para algún $n \in \mathbb{N}_0$. Lo que demuestra lo pedido. □

c) Deducir que: Si G tiene orden finito, entonces $G \cong \mathbb{Z}/|G|\mathbb{Z}$. Si G tiene orden infinito, entonces $G \cong \mathbb{Z}$.

Demostración. Antes que nada, recordemos que:

Si $n \in \mathbb{N}$, entonces $|\mathbb{Z}/n\mathbb{Z}| = n$. Si $n = 0$, entonces $\mathbb{Z}/0\mathbb{Z} = \mathbb{Z}/\{0\} \cong \mathbb{Z}$.

Si G tiene orden finito, como $G \cong \mathbb{Z}/n\mathbb{Z}$ para algún $n \in \mathbb{N}_0$, necesariamente tenemos que $\mathbb{Z}/n\mathbb{Z}$ tiene orden finito, por lo que $n \in \mathbb{N}$. Luego, $|G| = |\mathbb{Z}/n\mathbb{Z}| = n$. Así, obtenemos que $G \cong \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/|G|\mathbb{Z}$, lo que demuestra lo pedido.

Si G tiene orden infinito, como $G \cong \mathbb{Z}/n\mathbb{Z}$ para algún $n \in \mathbb{N}_0$, necesariamente tenemos que $\mathbb{Z}/n\mathbb{Z}$ tiene orden infinito, por lo que $n = 0$. Luego, $|G| \cong \mathbb{Z}$, lo que demuestra lo pedido. $\square$