Álgebra Moderna Tarea 4.1

Tomás Ricardo Basile Álvarez
316617194

21 de noviembre de 2020

a) **Denotemos a un grupo cíclcio de ordem m por $C(m)$. Demuestre que $C(p^2)$ no es isomorfo a $C(p) \times C(p)$**

Si estos dos grupos fueran isomorfos, entonces tendrían la misma estructura. Sin embargo, mostraré que $C(p^2)$ tiene al menos un elemento de orden p^2 mientras que los elementos de $C(p) \times C(p)$ son de a lo sumo orden p.
Para ello, como $C(p^2)$ es cíclico, es el generado de algún $a \in C(p^2)$ y éste a entonces tiene orden p^2.

Sin embargo, veremos que los elementos de $C(p) \times C(p)$ tienen a lo sumo orden p. Tomamos un elemento arbitrario $(b, c) \in C(p) \times C(p)$, entonces $b \in C(p), c \in C(p)$. Pero cualquier elemento de un grupo se anula al elevarlo al orden del grupo, por lo que $b^{|C(p)|} = e \quad \Rightarrow \quad b^p = e$ y similarmente $c^{|C_p|} = c^p = e$. Entonces, $(b, c)^p = (e, e)$ que es el neutro de $C(p) \times C(p)$.
Por lo tanto, el elemento (b, c) tiene un orden a lo sumo p.
Con esto probamos que $C(p) \times C(p)$ no tiene elementos de orden p^2 mientras que $C(p^2)$ sí, por lo que no pueden ser isomorfos.

b) **Sea G un p-grupo finito y $H \neq \{e_G\}$ un subgrupo normal, muestre que $H \cap Z(G) \neq \{e_G\}$**

Dejemos que G actúe en sí mismo por conjugación. Como H es normal, entonces para todo $h \in H$ se tiene que $ghg^{-1} \in H$ para todo $g \in G$.
Pero notamos que $\{ghg^{-1} \ \ | g \in G\}$ es la órbita de h. Por tanto, tenemos que para todo $h \in H$ se cumple que $\mathcal{O}_h \subset H$.
Entonces, podemos considerar todas las órbitas $\mathcal{O}_h$ tal que $h \in H$ y vemos que $H = \bigcup_{h \in H} \mathcal{O}_h$.
Que $H \subset \bigcup_{h \in H} \mathcal{O}_h$ se sigue de que cada h pertenece a su propia órbita. Y que $\bigcup_{h \in H} \mathcal{O}_h \subset H$ se sigue de que $O_h \subset H$ para cada $h \in H$.

Por lo tanto, H es la unión de clases de conjugación, las cuales son disjuntas por el Lema 19.10

Luego, cada una de estas órbitas O_{h_0} tiene una cantidad de elementos dada por:

$$\begin{aligned}|\mathcal{O}_{h_0}| &= [G : S(h_0)] \quad \text{Lema 22,12, con } S(h_0) \text{ el estabilizador de } h_0 \\ &= \frac{|G|}{|S(h_0)|} \quad \text{Teorema de Lagrange, porque G es finito}\end{aligned}$$

Pero como $|G|$ es un p-grupo finito, el lema 24.4 nos asegura que tiene $|G| = p^m$ elementos para algún m. Y como $S(h_0)$ es un subgrupo de G, el teorema de Lagrange nos asegura que tiene un número de elementos que divide a p^m, como p es primo, el número de elementos de $S(h_0)$ tiene que ser entonces de la forma $|S(h_0)| = p^k$.
Luego, la órbita tiene una cantidad de elementos $|\mathcal{O}_{h_0}| = \dfrac{|G|}{|S(h_0)|} = \dfrac{p^m}{p^k} = p^i$ con i un natural.
Es decir, cada órbita tiene una cantidad de elementos que es una potencia de p o tiene solamente un elemento. Entonces, $|O_h| \equiv 0 \pmod p$ o bien $|O_h| \equiv 1 \pmod p$ para todo h.

Luego, como H es un subgrupo de G, también tiene una cantidad de elementos que es una potencia de p (y no es un solo elemento porque $H \neq \{e\}$) , entonces $|H| \equiv 0 \pmod p$
Sin embargo, como probamos antes, H es la unión disjunta de varias órbitas con representantes $h_1, h_2, ...h_l$. Por lo tanto:

$$\begin{aligned}|H| &= |\mathcal{O}_{h_1} \cap \mathcal{O}_{h_2} \cap \cdots \cap \mathcal{O}_{h_l}| \\ &= |\mathcal{O}_{h_1}| + |\mathcal{O}_{h_1}| + \cdots + |\mathcal{O}_{h_1}| \quad \text{porque las órbitas son disjuntas}\end{aligned}$$

Como tenemos que el lado izquierdo es equivalente a 0 módulo p, el lado derecho también debe de serlo. Sin embargo, sabemos que H contiene al menos una órbita con un solo elemento (la clase de conjugación de $e \in H$) y todas las órbitas con más de un elemento tienen un número de elementos que es múltiplo de p.
Probaré que tiene que haber al menos otra órbita con orden 1. Supongamos que $\mathcal{O}_e$ fuera la única órbita con un elemento, entonces al hacer la suma $\mathcal{O}_{h_1}| + |\mathcal{O}_{h_1}| + \cdots + |\mathcal{O}_{h_1}|$ en módulo p, todas las demás órbitas serían equivalentes a 0 en mod p y el resultado final nos daría 1. Lo que contradice que $|H| \equiv 0 \ (mod\ p)$.

Por tanto, debe de haber por lo menos una órbita distinta de $\{e\}$ que contenga un solo elemento. Si dicha órbita es $\mathcal{O}_{h_s}$, entonces por el lema 19,10 hemos probado que $h_s \in Z(G)$.
Por tanto H y $Z(G)$ se intersectan por lo menos en dicho elemento h_s.

c **Sea $K \trianglelefteq G$ tal que G/K es un $p-$grupo finito. Mostrar que G tiene un subgrupo normal de índice p.**

Como G/K es un g-grupo finito, entonces por el Lema 24.4, tiene un orden de $|G/K| = p^m$ para un entero positivo m.
Luego, como $p^{m-1}||G/K|$, entonces el teorema 25.2 nos asegura que G/K tiene un subgrupo de orden p^{m-1}, llamémosle $M \leq G/K$, con $|M| = p^{m-1}$

Y es más, el corolario 22.11 dice que si L es un grupo finito y p el menor primo que divide a $|L|$. Entonces todo grupo $T \leq L$ de índice p es normal en L.
Podemos aplicar este teorema para M en vez de T y G/K en vez de L. Vemos que se cumplen las hipótesis porque p es el menor primo que divide a $|G/K| = p^m$ y $M \leq G/K$ es un subgrupo de índice $[G/K : M] = \dfrac{|G/K|}{|M|} = \dfrac{p^m}{p^{m-1}} = p$.
Entonces, $M \leq G/K$ tiene índice p y $M \trianglelefteq G/K$.

Consideramos ahora el teorema de correspondencia (18.3). Que dice que si tenemos una familia de subgrupos de G dada por $X := \{H \leq G \,|K \leq H\}$ y una familia de subgrupos de G/K dada por $Y := \{M \leq G/K\}$. Entonces existe una función $\phi : X \to Y$ con $\phi(H) = H/K$ que es una biyección entre X y Y.
En nuestro caso tenemos un conjunto $M \leq G/K$ (que es un elemento del conjunto Y), entonces el teorema de correspondencia nos asegura que le corresponde un subgrupo $H \leq G$ con $K \leq H$ (un elemento del conjunto X), de tal forma que $\phi(H) = H/K = M$.

Entonces, ya tenemos un grupo $H \leq G$, que probaremos que cumple con lo que se busca:

- **Es normal en G**: El inciso c) del teorema de correspondencia asegura que la función ϕ preserva la normalidad. En particular, tenemos que $\phi(H) = M \trianglelefteq G/K = \phi(G)$. Es decir, $\phi(H) \trianglelefteq \phi(G)$ y el inciso nos dice que podemos quitar las ϕ y se preserva la normalidad, entonces $H \trianglelefteq G$.
- **Es de índice** p: El índice de H en G es:

$$\begin{aligned}[G : H] &= |G/H| \\ &= |(G/K)/(H/K)|\end{aligned}$$

  Esto por el 3er teorema de isomorfismos.
  Luego, por el teorema de Lagrange tenemos:

$$\begin{aligned}[G : H] &= |(G/K)/(H/K)| \\ &= \frac{|G/K|}{|H/K|} \\ &= \frac{p^m}{p^{m-1}} \\ &= p\end{aligned}$$

d) **Sea $\langle p\rangle = \{0, p, 2p, ..., (p-1)p\} \leq \mathbb{Z}_{p^2}$ subgrupo aditivo. Definamos una operación sobre el producto cartesiano $G = \langle p\rangle \times \mathbb{Z}_{p^2}$ por $(x, y)(z, w) = (x + z, y + w - yz)$. Muestra que G es un grupo no abeliano de orden p^3.**

Comprobamos cada una de las condiciones para que sea un grupo:

- **La operación es cerrada:** Sean $(x, y), (z, w) \in \langle p\rangle \times \mathbb{Z}_{p^2}$ dos elementos arbitrarios. Entonces:

$$(x, y)(z, w) = (x + z, y + w - yz)$$

Y como $x, z \in \langle p\rangle$, entonces $x + z \in \langle p\rangle$ porque $\langle p\rangle$ es un grupo bajo la suma módulo p^2. Por otro lado, $y + w - yz$ es la suma de puros elementos de $\mathbb{Z}_{p^2}$, y por las propiedades de grupo de $\mathbb{Z}_{p^2}$, la suma es cerrada.
Entonces, $x+z \in \langle p\rangle$ y $y+w-yz \in \mathbb{Z}_{p^2}$. Por lo tanto, $(x+z, y+w-yz) \in \langle p\rangle \times \mathbb{Z}_{p^2}$ y la suma es cerrada.

- **La operación tiene neutro:**
Consideramos como neutro al elemento $(0, 0)$ que claramente pertenece a $\langle p\rangle \times \mathbb{Z}_{p^2}$.
Y vemos que efectivamente es un neutro:

$$(x, y)(0, 0) = (x + 0, y + 0 - y(0)) = (x, y)$$
$$(0, 0)(x, y) = (0 + x, 0 + y - 0(y)) = (x, y)$$

- **Asociatividad:** Sean $(x_1, y_1), (x_2, y_2), (x_3, y_3) \in \langle p\rangle \times \mathbb{Z}_{p^2}$. Entonces:

$$\begin{aligned}(x_1, y_1)((x_2, y_2)(x_3, y_3)) &= (x_1, y_1)(x_2 + x_3, y_2 + y_3 - y_2x_3) \\ &= (x_1 + (x_2 + x_3), y_1 + (y_2 + y_3 - y_2x_3) - y_1(x_2 + x_3)) \\ &= (x_1 + x_2 + x_3, y_1 + y_2 + y_3 - y_2x_3 - y_1x_2 - y_1x_3)\end{aligned}$$

Y por otro lado:

$$\begin{aligned}((x_1, y_1)(x_2, y_2))(x_3, y_3) &= (x_1 + x_2, y_1 + y_2 - y_1x_2)(x_3, y_3) \\ &= ((x_1 + x_2) + x_3, (y_1 + y_2 - y_1x_2) + y_3 - (y_1 + y_2 - y_1x_2)x_3) \\ &= (x_1 + x_2 + x_3\ ,\ y_1 + y_2 - y_1x_2 + y_3 - y_1x_3 - y_2x_3 + y_1x_2x_3) \\ &= (x_1 + x_2 + x_3\ ,\ y_1 + y_2 + y_3 - y_2x_3 - y_1x_2 - y_1x_3 + y_1x_2x_3)\end{aligned}$$

Vemos que los dos resultados son casi iguales, excepto por el término $y_1x_2x_3$ en el segundo. Sin embargo, esto no es problema, ya que este término vale 0. Esto debido a que como $(x_2, y_2), (x_3, y_3) \in \langle p\rangle \times \mathbb{Z}_{p^2}$
Entonces $x_2, x_3 \in \langle p\rangle$, lo que siginifica que son ambos múltiplos de p. Entonces, $y_1x_2x_3$ es un múltiplo de p^2. Esto siginifica que $y_1x_2x_3$ es equivalente a 0 en módulo p^2.

- **Inverso:** Sea $(x, y) \in \langle p\rangle \times \mathbb{Z}_{p^2}$. Y consideramos como inverso a $(-x, -y - xy)$. Primero vemos que es un elemento de $\langle p\rangle \times \mathbb{Z}_{p^2}$. Para ello, notamos que como $x \in \langle p\rangle$, entonces $-x$ es también un múltiplo de p y pertenece a $\langle p\rangle$. Por otro lado, $-y - xy \in Z_{p^2}$ porque todos estos elementos pertenecen a $\mathbb{Z}_{p^2}$. Entonces, para probar que es el inverso, vemos que:

$$\begin{aligned}(x,y)(-x,-y-xy) &= (x-x, y+(-y-xy)-y(-x)) \\ &= (0, -xy+xy) \\ &= (0,0)\end{aligned}$$

Y por el otro lado:

$$\begin{aligned}(-x,-y-xy)(x,y) &= (-x+x\ ,\ (-y-xy)+y-(-y-xy)x) \\ &= (0, -y-xy+y+yx+x^2y) \\ &= (0, x^2y) \\ &= (0,0)\end{aligned}$$

Lo último porque $x \in \langle p \rangle$ y entonces x es múltiplo de p, por lo que x^2y es múltiplo de p^2 y por tanto es equivalente a 0 en módulo p^2.

No es Abeliano
Consideramos $(p,1) \in \langle p \rangle \times \mathbb{Z}_{p^2}$ y $(0,2) \in \langle p \rangle \times \mathbb{Z}_{p^2}$
Entonces:

$$\begin{aligned}(p,1)(0,2) &= (p+0, 1+2-1(0)) = (p,2) \\ (0,2)(p,1) &= (0+p, 2+1-2p) = (p, 3-2p)\end{aligned}$$

Y en general $3-2p \neq 2$ módulo p^2. Pues $3-2p \equiv 2p-3 \pmod p$
Pero vemos que $2 < 2p-3 < p^2$ para todo p primo (a menos que $p=2$). Por lo que tiene que ser una clase de equivalencia distinta a la del 2. En caso que $p=2$, entonces $2p-3=1$ que es distinto a 2.
Por tanto, la operación no conmuta.

Vemos ahora que tiene orden p^3. Esto debido a que primero hay que escoger un elemento de $\langle p \rangle = \{0, p, 2p, 3p, ..., (p-1)p\}$, para lo cual tenemos p opciones.
Luego hay que escoger un elemento de $\mathbb{Z}_{p^2}$, para lo cual tenemos p^2 opciones. En total, nos queda una cantidad de opciones para escoger un elemento igual a $p \cdot p^2 = p^3$. Es decir, el grupo tiene p^3 elementos.

e) **Mostrar que el grupo G del ejercicio anterior contiene un elemento de orden p^2**

Consideramos el elemento $(0,1)$ (que claramente pertenece al conjunto, porque $0 \in \langle p \rangle$ y $1 \in \mathbb{Z}_{p^2}$ y veremos que $(0,1)^n = (0,n)$. Esto lo probamos por inducción:

- **Caso base:** Claramente vemos que $(0,1)^1 = (0,1)$

- Suponemos que se cumple para n que $(0,1)^n = (0,n)$ y vamos a probar que $(0,1)^{n+1} = (0,n+1)$:

$$\begin{aligned}(0,1)^{n+1} &= (0,1)^n(0,1) \quad \text{por definición de potencia} \\ &= (0,n)(0,1) \quad \text{hipótesis inductiva} \\ &= (0+0, n+1-n(0)) \\ &= (0,n+1)\end{aligned}$$

Luego, para todo $0 < n < p^2$ se tiene que $(0,1)^n = (0,n) \neq (0,0)$ porque n es menor a p^2 y entonces no es múltiplo de p^2 y no es equivalente a 0 módulo p^2.
SIn embargo, tenemos que $(0,1)^{p^2} = (0,p^2) = (0,0)$ porque $p^2 \equiv 0 \pmod{p^2}$

Por lo tanto, p^2 es la primera potencia que anula a $(0,1)$. Por lo que $(0,1)$ tiene orden p^2.