Álgebra Moderna Tarea 4.3

Tomás Ricardo Basile Álvarez
316617194

27 de noviembre de 2020

a) **Prueba que todo grupo de orden 15 es isomorfo a $\mathbb{Z}_3 \times \mathbb{Z}_5$**

Sea G el grupo de orden 15. Notamos que $15 = 3 \cdot 5$.
Veamos entonces cuántos 3-subgrupos de Sylow hay. Por el tercer teorema de Sylow, se tiene que n_3 es un divisor de $15/3 = 5$ y que $n_3 \equiv 1 \ (mod\ 3)$.
Por la primera condición, tenemos que $n_3 = 1, 5$ pero de estas dos opciones, la única que cumple $n_3 \equiv 1 \ (mod\ 3)$ es $n_3 = 1$.

Por otro lado, veamos cuántos 5-subgrupos de Sylow hay. Por el tercer teorema de Sylow, tenemos que n_5 divide a 3 y que también $n_5 \equiv 1 \ (mod\ 5)$.
Por la primera condición tenemos que $n_5 = 1, 3$. Y por la segunda condición, nos queda que necesariamente $n_5 = 1$.

Entonces, sea P el 3-subgrupo de Sylow (que tiene orden 3) y sea Q el 5-subgrupo de Sylow (que tiene orden 5).
Luego, como cada uno es el único conjunto de Sylow de su respectivo orden, esto nos asegura por el corolario 26.8 del segundo teorema de Sylow, que cada uno de estos subgrupos son normales.

Además, $P \cap Q = \{e\}$. Esto porque si la intersección fuera no trivial, tendría que ser un grupo con orden que divida a $|P| = 3$ y a $|Q| = 5$.
Entonces, como P, Q son normales y con intersección trivial, el teorema 15.11 nos asegura que $PQ \simeq P \times Q$.
Y además, por el teorema 15.4, $|PQ| = \dfrac{|P||Q|}{|P \cap Q|} = \dfrac{3 \cdot 5}{1} = 15$.
Por tanto, $PQ = G$. Y entonces, $G = PQ = P \times Q$.
Y como P tiene orden 3 (que es primo), entonces $P \simeq \mathbb{Z}_3$ y como Q tiene orden 5, entonces $Q \simeq \mathbb{Z}_5$. Por lo tanto, $G = P \times Q = \mathbb{Z}_3 \times \mathbb{Z}_5$.

b) **Se puede probar que existe un grupo de orden 21 que se describe como:**

$$G_{21} := \langle a, b | a^7 = b^3 = e,\ bab^{-1} = a^4 \rangle$$

Prueba que todo grupo de orden 21 es isomorfo a $\mathbb{Z}_3 \times \mathbb{Z}_7$ o a G_{21}

Sea G un grupo de orden 21. Notamos que $21 = 3 \cdot 7$.
Entonces, consideramos a los 3-subgrupos de Sylow. Por el tercer teorema de Sylow, tenemos que la cantidad de estos subgrupos debe de cumplir que n_3 divide a 7 y que $n_3 \equiv 1\ (mod\ 3)$.
Entonces, por la primera condición, tenemos que $n_3 = 1, 7$. Y estos dos números cumplen con la segunda condición. Por lo que $n_3 = 1, 7$.

Por otro lado, consideramos los 7-subgrupos de Sylow. Por el tercer teorema de Sylow, tenemos que n_7 divide a 3. Además, $n_7 \equiv 1\ (mod\ 7)$.
Por la primera condición, $n_7 = 1, 3$ y por la segunda, la única opción posible es $n_7 = 1$.

Esto nos da dos casos según los valores de n_3, n_7

a) Sea $n_3 = 1, n_7 = 1$.
   Digamos que P es el 3-subgrupo de Sylow y que Q es el 7-subgrupo. Como solamente hay un subgrupo de Sylow de orden 3, entonces por el corolario al segundo teorema de Sylow, P es normal. Similarmente, como solamente hay un subgrupo de Sylow de orden 7, entonces Q es normal.
   Además, se cumple que $P \cap Q = \{e\}$ ya que la intersección, tendría un orden que divide a $|P| = 3$ y a $|Q| = 7$, lo cual solamente se cumple por 1.
   Luego, por el teorema 15.4, tenemos que $|PQ| = \dfrac{|P||Q|}{|P \cap Q|} = |P||Q| = 21$.
   Entonces, PQ es igual al grupo completo G.
   Además, como ambos subgrupos son normales y con intersección trivial, el teorema 15,11 nos asegura que $PQ \simeq P \times Q$.
   Por lo tanto, $G = PQ \simeq P \times Q \simeq \mathbb{Z}_3 \times \mathbb{Z}_7$
   Esto último porque P, Q son de orden primo y por tanto son isomorfos a $\mathbb{Z}_n$.

b) Sea $n_3 = 7, n_7 = 1$.
   Como $n_7 = 1$, existe un único Q que es un 7-subgrupo de G y por tanto es cíclico y de orden 7.
   Es decir, existe una $a \in Q$ tal que $a^7 = e$. Y además, por el segundo teorema de Sylow, Q es normal en G

   Sea $P \in Syl_3(G)$. Como P tiene orden 3, es cíclico y de orden 3. Entonces, existe un $b \in G$ tal que $P = \langle b \rangle$ y por tanto, $b^3 = e$.

   Luego, $P \cap Q = \{e\}$ porque el orden de la intersección de estos dos subgrupos debe de dividir a $|P| = 3$ y a $|Q| = 7$ a la vez, lo cual implica que $|P \cap Q| = 1$.

Por tanto, por el teorema 15.4, tenemos que $|PQ| = \dfrac{|P||Q|}{|P \cap Q|} = |P||Q| = 3{\cdot}7 = 21$.
Entonces, $PQ = G$.
Por lo tanto, ya tenemos que G se puede generar con solamente a, b.

Vemos ahora como se relacionan a y b. Como Q es normal en G, y $a \in Q$, entonces el producto bab^{-1} debe de estar en Q. Esto significa que $bab^{-1} = a^m$ para un $m = 0, 1, ..., 6$.
Entonces, usaré un resultado que probé en la tarea 3.2 que dice que si $gag^{-1} = a^m$ entonces $g^k a g^{-k} = a^{m^k}$. Agrego una foto de la prueba.

Probamos primero lo que nos pide el hint. Llamamos g al elemento tal que $gag^{-1} = a^m$ (porque a es conjugado a a^m)

$$\begin{aligned} g^2ag^{-2} &= ggag^{-1}g^{-1} \\ &= g(gag^{-1})g^{-1} \\ &= g(a^m)g^{-1} \\ &= (gag^{-1})^m \quad \text{porque probamos en clase que } (gbg^{-1})^k = gb^kg^{-1} \\ &= (a^m)^m \\ &= a^{m^2} \end{aligned}$$

Luego, tenemos que $g^2ag^{-2} = a^{m^2}$, lo que significa que a es conjugado con a^{m^2}
Podemos generalizar este resultado por inducción. Ya tenemos probado el caso base y ahora probaremos que que $g^kag^{-k} = a^{m^k}$ para todo k.
Hipótesis de inducción: Suponemos que se cumple que $g^kag^{-k} = a^{m^k}$ y probaremos que $g^{k+1}ag^{-(k+1)} = a^{m^{k+1}}$.

$$\begin{aligned} g^{k+1}ag^{-(k+1)} &= gg^kag^{-k}g^{-1} \\ &= g(a^{m^k})g^{-1} \quad \text{hipótesis inductiva} \\ &= (gag^{-1})^{m^k} \\ &= (a^m)^{m^k} \\ &= (a^{m \cdot m^k}) \\ &= a^{m^{k+1}} \end{aligned}$$

Entonces, nosotros tenemos que $bab^{-1} = a^m$ y usando la demostración del otro ejercicio para $k = 3$, podemos concluir que $b^3ab^{-3} = a^{m^3}$. Pero como b tiene orden 3, esto implica que $a = a^{m^3}$ y por tanto, $a^{m^3-1} = e$. Lo que implica que $m^3 - 1$ es múltiplo del orden de a (múltiplo de 7). Podemos probar con las distintas posibilidades de m y ver cuál es un múltiplo de 7.

- $m = 0 \quad \Rightarrow \quad m^3 - 1 = -1$. No es múltiplo de 7
- $m = 1 \quad \Rightarrow \quad m^3 - 1 = 0$. Sí es múltiplo de 7.
- $m = 2 \quad \Rightarrow \quad m^3 - 1 = 7$. Sí es múltiplo de 7
- $m = 3 \quad \Rightarrow \quad m^3 - 1 = 26$. No es múltiplo de 7
- $m = 4 \quad \Rightarrow \quad m^3 - 1 = 67$. Sí es múltiplo de 7
- $m = 5 \quad \Rightarrow \quad m^3 - 1 = 124$. No es múltiplo de 7
- $m = 6 \quad \Rightarrow \quad m^3 - 1 = 215$. No es múltiplo de 7

Entonces, solamente nos quedan las posibilidades que $m = 1, 2, 4$.
Si $m = 1$, entonces $bab^{-1} = a \quad \Rightarrow \quad ba = ab$. Como estos dos elementos son los

generadores, esto implica que todo el grupo es conmutativo. Sin embargo, en un grupo conmutativo todos los subgrupos son normales, lo que contradice que en este caso $n_3 = 7 \neq 1$ y por tanto los 3-subgrupos de Sylow no son normales.

El caso en que $m = 4$ nos da justamente el grupo que buscamos. Pues ya tendríamos que $|a| = 7, |b| = 3$, que estos dos elementos son generadores y que $bab^{-1} = a^4$. Por tanto, nos quedaría que:

$$G = \langle a, b | a^7 = b^3 = e, bab^{-1} = a^4 \rangle = G_{21}$$

Si $m = 2$, nos queda el grupo con $G = \langle a, b | a^7 = b^3 = e, bab^{-1} = a^2 \rangle$.
Pero este grupo es igual al anterior. Basta con notar que podemos cambiar b por b^2 y seguirá siendo un generador (porque b y b^2 generan lo mismo ya que $|b| = 3$) y seguirá teniendo orden 3. Entonces, llamemos $u = b^2$. Y veamos qué resultado obtenemos que uau^{-1}

$$\begin{aligned} uau^{-1} &= b^2ab^{-2} = b(bab^{-1})b^{-1} = b(a^2)b^{-1} \\ &= baab^{-1} = bab^{-1}bab^{-1} = (bab^{-1})(bab^{-1}) = a^2a^2 \\ &= a^4 \end{aligned}$$

Entonces, tenemos que el conjunto G se puede generar con a y u y tenemos:

$$G = \langle a, u | a^7 = u^3 = e \ , uau^{-1} = a^4 \}$$

Por lo que es igual al G_{21} de antes.

c) **Sea G un grupo de orden 231. Probar que cualquier 11-subgrupo de Sylow de G está contenido en $Z(G)$**

Vemos que $231 = 3 \cdot 7 \cdot 11$. Veamos cuántos 11-subgrupos tiene.
Por el tercer teorema de Sylow, tenemos que $n_{11} | (231/11) \ \Rightarrow \ n_{11} | 21$. Y tenemos también que $n_{11} \equiv 1 \pmod{11}$.
Por la primera condición, debemos de tener que n_{11} es 1 , 3 , 7 o 21. Sin embargo, la segunda condición nos obliga a que $n_{11} = 1$.

Sea P dicho grupo de orden 11 (que es el único grupo de orden 11). Y como 11 es primo, P se ve como el generado de un elemento de orden 11, digamos que $P = \langle a \rangle$. Luego, por el corolario al segundo teorema de Sylow, como P es el único grupo de este orden, tenemos que P es normal en G.

Entonces, sea $g \in G$. El hecho de que P sea normal implica que $gag^{-1} \in P$ Entonces, tenemos que $gag^{-1} = a^j$ para algún $j = 0, 1, ..., 10$.
Buscamos probar que $j = 1$ para concluir que $ga = ag$.
Primero nos deshacemos del caso $j = 0$. Porque si $gag^{-1} = a^0 \ \Rightarrow \ gag^{-1} = e \ \Rightarrow \ ga =$

$g \Rightarrow a = e$. Lo que es una contradicción.

Luego usamos el mismo truco que en el ejercicio pasado. Tenemos que $gag^{-1} = a^j$. Y por lo de la tarea 3.2 mencionado en el ejercicio pasado, esto implica que $g^k a g^{-k} = a^{j^k}$ para todo k.
En particular, lo podemos hacer para $k = 231$, que al ser el orden del grupo, cualquier elemento del conjunto se anula al elevarlo a la 231.
Entonces $g^{231} a g^{-231} = a^{j^{231}} \Rightarrow a = a^{j^{231}}$. Entonces, tenemos que $a^{j^{231}-1} = e$.
Entonces, como el orden de a es 11, debemos de tener que $j^{231} - 1$ es un múltiplo de 11.
Para ver qué números j entre 1 y 10 cumplen esto, no se me ocurrió ningún método o teorema de teoría de núeros o algo así. Así que lo comprobaré a fuerza bruta. Como las potencias son tan grandes, hice las cuentas en Mathematica.

- $j = 1 \Rightarrow j^{231} - 1 = 1 - 1 = 0$, que es un múltiplo de 11.
- $j = 2 \Rightarrow 2^{231} - 1 \equiv 1 \ (mod\ 11)$
- $j = 3 \Rightarrow 3^{231} - 1 \equiv 2 \ (mod\ 11)$
- $j = 4 \Rightarrow 4^{231} - 1 \equiv 3 \ (mod\ 11)$
- $j = 5 \Rightarrow 5^{231} - 1 \equiv 4 \ (mod\ 11)$
- $j = 6 \Rightarrow 6^{231} - 1 \equiv 5 \ (mod\ 11)$
- $j = 7 \Rightarrow 7^{231} - 1 \equiv 6 \ (mod\ 11)$
- $j = 8 \Rightarrow 8^{231} - 1 \equiv 8 \ (mod\ 11)$
- $j = 9 \Rightarrow 9^{231} - 1 \equiv 8 \ (mod\ 11)$
- $j = 10 \Rightarrow 10^{231} - 1 \equiv 9 \ (mod\ 11)$

Entonces, el único caso en que $j^{231} - 1$ es un múltiplo de 11 sucede cuando $j = 1$. Por lo tanto, el único caso posible es $gag^{-1} = a^j = a$.
Entonces, para todo $g \in G$, se cumple que $gag^{-1} = a \Rightarrow ga = ag$.
Entonces, a conmuta con todos los elementos de G. Y por tanto, todos los elementos de $P = \langle a \rangle$ conmutan con todos los $g \in G$.
Esto implica que el grupo P de orden 11 (único grupo de orden 11 que tiene G) está contenido en $Z(G)$.

.

d) **Sea G un grupo de orden 30. Mostrar que G tiene un subgrupo normal cíclico de índice 2**

Notamos que $30 = 2 \cdot 3 \cdot 5$. Y consideramos la cantidad de p-subgrupos de Sylow.

Para $p = 3$, tenemos que la cantidad de 3-subgrupos de Sylow debe de cumplir n_3 debe dividir a $30/3 = 10$. Y además, $n_3 \equiv 1 \pmod 3$.
Por la primera condición, tenemos que $n_3 = 1, 2, 5, 10$ pero por la segunda condición, nos queda que $n_3 = 1, 10$.

Para $p = 5$, por el tercer teorema de Sylow, debemos de tener que n_5 divide a $30/5 = 6$. Y además, que $n_5 \equiv 1 \pmod 5$.
La primera condición implica que $n_5 = 1, 2, 3, 6$. Pero la seugunda nos deja solamente con las posibilidades que $n_5 = 1, 6$.

Eso nos deja unos cuantos casos:

- $n_3 = 10, n_5 = 6$.
  Esto implica que hay 10 grupos de orden 3. Cada uno de estos grupos es cíclico y se ve como $\{e, g, g^2\}$, donde g (y por tanto g^2) tienen orden 3. Además, cualquier par de estos grupos sólo se intersectan en $\{e\}$ (porque la intersección tiene que tener orden 1 o 3, pero si tiene orden 3, implica que los grupos son iguales). Entonces, para cada uno de los 10 grupos de orden 3, tenemos 2 elementos de distintos de orden 3. Para un total de 20 elementos de orden 3.
  Similarmente, como $n_5 = 6$, entonces debemos de tener 6 grupos de orden 5. Y todos los elementos de estos grupos tienen orden 5. Además, se intersectan trivialmente por el mismo argumento de antes. Entonces, tenemos $4 \times 6 = 24$ elementos distintos de orden 5.
  Para un total de $20 + 24 = 44$ elementos distintos en el grupo. Lo cual es una contradicción.

Entonces, como alguno de los números n_5 o n_3 valen 1.
Sea N un grupo de orden 3 y sea H un grupo de orden 5. Como alguno de los números n_5, n_3 vale 1, entonces alguno de estos grupos es normal por el segundo teorema de Sylow.
Por lo tanto, como uno de los grupos es normal, esto implica que NH es un subgrupo de G.

Luego, $N \cap H = \{e\}$ porque $|N \cap H|$ tiene que dividir a $|N| = 3$ y a $H| = 5$. Por lo tanto, $|N \cap H| = 1$. Entonces, por una propiedad que hemos visto, tenemos que $|NH| = \dfrac{|N||H|}{|N \cap H|} = \dfrac{|N||H|}{1} = |N||H| = 3 \cdot 5 = 15$.

Por tanto, G tiene un subgrupo de orden 15. Luego, por el ejercicio a), todo grupo de orden 15 es isomorfo a $\mathbb{Z}_3 \times \mathbb{Z}_5$. Pero $\mathbb{Z}_3 \times \mathbb{Z}_5$ es cíclico ya que $\mathbb{Z}_3 \times \mathbb{Z}_5 = \langle (2,1) \rangle$.
Porque $\langle (2,1) \rangle = \{(2,1), (4,2), (1,0), (3,1), (0,2), (2,0), (4,1), (1,2), (3,0), (0,1), (2,2), (4,0), (1,1), (3$
Que son todos los elementos de $\mathbb{Z}_3 \times \mathbb{Z}_5$.

Además, como $30 = 15 \cdot 2$, entonces el subgrupo de orden 15 en G tiene índice 2. Por lo tanto, se concluye que dicho grupo es normal (todo grupo de índice 2 es normal).

e) **Mostrar que existen exactamente dos grupos de orden 99**

Notamos que $99 = 3^2 \cdot 11$

Sea n_3 la cantidad de 3-subgrupos de Sylow (que en este caso tienen orden $3^2 = 9$). Entonces, por el tercer teorema de Sylow, se debe de cumplir que n_3 divide a $99/3^2 = 11$. Además, se debe de cumplir que $n_3 \equiv 1 \pmod 3$. La primera condición implica que $n_3 = 1, 11$. Pero la segunda condición implica que la única posibilidad es $n_3 = 1$.

Sea n_{11} la cantidad de 11-subgrupos de Sylow. Por el tercer teorema de Sylow, tenemos que n_{11} divide a $99/11 = 9$. Y además, debemos de tener que $n_{11} \equiv 1\ (mod\ 11)$.
Por la primera condición, tenemos que $n_{11} = 1, 3, 9$. Sin embargo, por la segunda condición, la única posibilidad es que $n_{11} = 1$.

Luego, existe exactamente un subgrupo P de orden 9 y un subgrupo Q de orden 11. Y como son los únicos p-subgrupos de sus respectivos órdenes, el segundo teorema de Sylow implica que son normales. Además, podemos ver que $P \cap Q = \{e\}$. Ya que la intersección debe de tener un orden que divida a $|P| = 9$ y a $|Q| = 11$. Entonces, el teorema 15.11 implica que $PQ \simeq P \times Q$.
Además el teorema 15.4 implica que $|PQ| = \dfrac{|P||Q|}{|P \cap Q|} = \dfrac{|P||Q|}{1} = |P||Q| = 99$. Entonces, PQ es igual a todo el grupo completo. Y por tanto, el grupo completo es isomorfo a $P \times Q$.

Como Q tiene orden 11 (que es primo) entonces $Q \simeq \mathbb{Z}_{11}$.
Por otro lado $|P| = 9$ y en la clase 24 vimos que los grupos de orden 9 son isomorfos a $\mathbb{Z}_9$ o a $\mathbb{Z}_3 \times \mathbb{Z}_3$.
Por tanto, las opciones para el grupo completo son:

- $P \times Q \simeq \mathbb{Z}_9 \times \mathbb{Z}_{11}$

- $P \times Q \simeq \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{11}$