Álgebra Moderna Tarea 4.5

Tomás Ricardo Basile Álvarez
316617194

5 de diciembre de 2020

a) **Sea $n \in \mathbb{N}$. Prueba que el grupo diétrico cumple que $D_{2(n)} = C_n \rtimes C_2$ donde C_n es un subgrupo normal cíclico**

Usamos la proposición 29.3 de las notas. Dice que si G es un grupo y tenemos $H \trianglelefteq G, K \leq G$ tales que $KH = G$ y $H \cap K = \{e\}$. Entonces $G \simeq H \rtimes K$.
Recordamos que:

$$D_{2(n)} = \langle s, r | s^2 = 1, r^n = 1, sr^{-1} = rs \rangle$$

Consideramos al subgrupo $\langle r \rangle \leq D_{2(n)}$. Claramente es un subgrupo de orden n y cíclico. Además, como $|D_{2(n)}| = 2n$, entonces $[D_{2(n)} : \langle r \rangle] = \dfrac{|D_{2(n)}|}{|\langle r \rangle} = \dfrac{2n}{n} = 2$.
Como es un grupo de índice 2, ya sabemos que es normal. Entonces este subgrupo $\langle r \rangle$ corresponde al C_n que pide el ejercicio.

Por otro lado, consideramos $\langle s \rangle$. Éste es un grupo cíclico de orden 2 y por tanto corresponde con el C_2 que pide el ejercicio.

Luego, para usar el teorema que enunciamos al principio, hay que probar que $\langle r \rangle \langle s \rangle = D_{2(n)}$. Para ello, notamos que cualquier elemento de $D_{2(n)}$ se puede escribir como $r^k s^m$ con $k \in \{0, 1, ..., n-1\}$, $s \in \{0, 1\}$.
Pero estos son los mismos elementos de $\langle r \rangle \langle s \rangle$.
Además, tenemos que $\langle r \rangle \cap \langle s \rangle = \{e\}$. Esto porque $s \neq r^k$ para todo $k \in \mathbb{Z}$ (proposición 3.5 f).
Entonces, ya podemos usar el teorema 29.3 para concluir que:

$$D_{2(n)} = \langle r \rangle \rtimes \langle s \rangle$$

b) **Sea $\alpha : G \to H$ un homomorfismo de grupos. Denotemos por K al kernel de α. Mostrar que si existe $\beta : H \to G$ homomorfismo de grupos tal que $\alpha \circ \beta = id_H$, entonces $G \simeq K \rtimes_\sigma H$ para algún σ**

Primero que nada, como $\beta : H \to G$ tiene inversa izquierda, entonces es una función inyectiva. Por lo tanto, si restringimos el contradominio de la función como $\beta : H \to \beta(H) \leq G$, ahora la función es biyectiva y por tanto $H \simeq \beta(H)$. El hecho de que $\beta(H) \leq G$ se sigue de que la imagen de un subgrupo bajo un homomorfismo es nuevamente un subgrupo.

Usaremos el teorema 29.3 que dice si G es un grupo y tiene dos subgrupos que se intersectan trivialmente y uno es normal, entonces G es isomorfo al producto interno de dichos subgrupos.
Entonces, vamos a probar que $G \simeq \beta(H) \rtimes K$. Para lo que hay que probar lo siguiente:

- **Probar que** $K \trianglelefteq G$: Esto se sigue de que K es el Kernel del morfismo $\alpha : G \to H$
- **Probar que** $\beta(H) \leq G$: Esto ya lo mostramos arriba.
- **Probar que** $K \cap \beta(H) = \{e\}$: El hecho de que $e \in K \cap \beta(H)$ se sigue de que ambos son grupos y por tanto contienen a e.
  Ahora suponemos que hay un elemento $g \in K \cap \beta(H)$. Como $g \in K$, entonces $\alpha(g) = e_H$. Y como $g \in \beta(H)$, entonces $g = \beta(h)$ para alg un $h \in H$.
  Juntando ambos resultados, tenemos que $\alpha(g) = e_H \quad \Rightarrow \quad \alpha(\beta(h)) = e_H$. Pero como $\alpha \circ \beta = id_H$, entonces $\alpha(\beta(h)) = e_H \quad \Rightarrow \quad h = e_H$.
  Entonces, tenemos que $g = \beta(h) = \beta(e_H) = e_G$ (esto último porque β es un morfismo y por tanto manda el elemento identidad al elemento identidad).
  Entonces concluimos que efectivamente $K \cap \beta(H) = \{e\}$

Entonces, tenemos que $G \simeq K \rtimes \beta(H)$. Pero por lo dicho al principio, tenúamos que $\beta(H) \simeq H$. Entonces podemos cambiar $\beta(H)$ por H y concluimos que $G \simeq K \rtimes \beta(H)$

c) **Encuentra todos los grupos de orden 55**

Primero notamos que $55 = 5{\cdot}11$. Y calculamos la cantidad de p-subgrupos en cada caso.

Consideramos la cantidad de subgrupos de orden 5, n_5. Por el tercer teorema de Sylow, tenemos que n_5 divide a 11 y que $n_5 \equiv 1 \ (mod\ 5)$.
Por la primera condición, tenemos que $n_5 = 1, 11$ y la segunda condición no agrega más restricciones.

Consideramos la cantidad de subgrupos de orden 11, n_{11}. Por el tercer teorema de Sylow, tenemos que n_{11} divide a 5 y que $n_{11} \equiv 1 \ (mod\ 11)$.

Por la primera condición, tenemos que $n_{11} = 1, 5$. Y por la segunda condición tenemos que $n_{11} = 1$.

Luego, tenemos dos casos.

- $n_5 = 1, n_{11} = 1$
  Sea P el grupo de orden 5 y sea Q el grupo de orden 11. Entonces, por el corolario 26.8, como cada uno de estos subgrupos es el único de su orden correspondiente, entonces son normales. $P, Q \trianglelefteq G$.

  Además, su intersección es vacía, pues $P \cap Q$ tiene que tener un orden que divida a $|P| = 5, |Q| = 11$. Y por tanto debe de tener orden 1.
  Entonces, por el teorema 15.4, tenemos que $|PQ| = \dfrac{|P||Q|}{|P \cap Q|} = |P||Q| = 5 \cdot 11 = 55$
  Luego, $PQ = G$. Y por el teorema 15.11, y como los grupos son normales, tenemos que $PQ \simeq P \times Q$.

  Entonces, $G \simeq P \times Q$.
  Pero como P tiene orden 5, entonces $P \simeq \mathbb{Z}_5$, y como Q tiene orden 11, entonces $Q \simeq \mathbb{Z}_{11}$. Por lo tanto:

  $$G \simeq \mathbb{Z}_5 \times Z_{11}$$

- $n_5 = 11, n_{11} = 1$
  Sea P alguno de los grupos de orden 5 y sea Q el grupo de orden 11. Como Q es el único p-grupo de su orden, entonces Q es normal. Además, por ser de orden 11, Q es cíclico y se puede ver como $Q = \langle q \rangle = \{e, q, ..., q^{10}\}$
  Luego, consideramos un $p \in P$.
  Como Q es normal, debemos de tener que $p^{-1}qp \in Q$ y por tanto $p^{-1}qp = q^i$ para algún $i \in \{0, 1, 2, ..., 10\}$.
  Usaremos varias veces que si $p^{-1}qp = q^i \quad \Rightarrow \quad p^{-k}qp^k = q^{i^k}$ (1) (propiedad mostrada en el corolario 30.10 y en la tarea 3.2b).
  Entonces:

  $$\begin{aligned} & p^{-1}qp = q^i \\ & \Rightarrow\ p^{-5}qp^5 = q^{5^i} \quad \text{por (1)} \\ & \Rightarrow\ q = q^{i^5} \quad \text{porque } p \text{ tiene orden 5} \\ & \Rightarrow\ q^{i^5-1} = e \\ & \Rightarrow\ i^5 - 1 \equiv 0 \pmod{11} \quad \text{porque } q \text{ tiene orden 11} \end{aligned}$$

  Probamos para los valores de i entre 0 y 10 para ver cuáles cumplen con la condición necesaria de arriba y desechamos los que no. Para los que son válidos, podemos ver que p, q generan a G (porque $G \simeq P \times Q$). Y podemos encontrar las relaciones generadoras usando que $p^{-1}qp = q^i \ \Rightarrow \ qp = pq^i$

  - $i = 0 \quad \Rightarrow 0^5 - 1 \equiv -1 \pmod{11}$ no es válido.

- $i = 1 \quad \Rightarrow 1^5 - 1 \equiv 0 \ \ (mod\, 11)$ es válido.

$$G = \langle p, q \mid p^5 = q^{11} = e, qp = pq\rangle$$

Entonces p, q conmutan pero como son los generadores, eso implica que todo el grupo G es conmutativo. Esto contradice el hecho de que haya 11 subgrupos de orden 5 (porque si fuera abeliano, todos los subgrupos serían normales, pero en este caso, los de orden 5 no los son).

- $i = 2 \quad \Rightarrow 2^5 - 1 \equiv 9 \ \ (mod\, 11)$ no es válido.

- $i = 3 \quad \Rightarrow 3^5 - 1 \equiv 0 \ \ (mod\, 11)$ es válido.

$$G = \langle p, q | p^5 = q^{11} = e, qp = pq^3\rangle$$

- $i = 4 \quad \Rightarrow 4^5 - 1 \equiv 0 \ \ (mod\, 11)$ es válido.

$$G = \langle p, q | p^5 = q^{11} = e, qp = pq^4\rangle$$

Pero si denotamos ahora $u = p^4$ entonces u genera lo mismo que p (porque p es de orden 5 y entonces u también por ser 5 coprimo con 4) y se cumple que $u^{-1}qu = p^{-4}qp^4 = q^{4^4}$ (propiedad (1) y que $p^{-1}qp = q^4$).
$\Rightarrow \quad u^{-1}qu = q^{256} = q^{11*23}q^3 = q^3$ (porque q tiene orden 11). Y entonces $qu = uq^3$
Entonces, el grupo es igual a:

$$G = \langle u, q | u^5 = q^{11} = e, qu = uq^3\rangle$$

Que es igual al grupo que ya habíamos considerado para $i = 3$. Por lo que este caso no nos da ninguna nueva posibilidad.

- $i = 5 \quad \Rightarrow 5^5 - 1 \equiv 0 \ \ (mod\, 11)$ es válido.

$$G = \langle p, q | p^5 = q^{11} = e, qp = pq^5\rangle$$

Pero si ahora denotamos $u = p^2$ entonces u genera lo mismo que p (porque p es de orden primo) y se cumple que $u^{-1}qu = p^{-2}qp^2 = q^{5^2}$ (propiedad (1) y que $p^{-1}qp = q^5$).
Entonces $u^{-1}qu = q^{25} = q^{2*11}q^3 = q^3$. Y entonces tenemos que $qu = uq^3$.
Por tanto, el grupo es igual a:

$$G = \langle u, q | u^5 = q^{11} = e, qu = uq^3\rangle$$

Que es igual al grupo que ya habíamos considerado para $i = 3$.

- $i = 6 \quad \Rightarrow 6^5 - 1 \equiv 9 \ \ (mod\, 11)$ no es válido.
- $i = 7 \quad \Rightarrow 7^5 - 1 \equiv 9 \ \ (mod\, 11)$ no es válido.
- $i = 8 \quad \Rightarrow 8^5 - 1 \equiv 9 \ \ (mod\, 11)$ no es válido.
- $i = 9 \quad \Rightarrow 9^5 - 1 \equiv 0 \ \ (mod\, 11)$ es válido.

$$G = \langle p, q | p^5 = q^{11} = e, qp = pq^9\rangle$$

Pero denotamos ahora $u = p^3$ entonces u genera lo mismo que p. Y se cumple que $u^{-1}qu = p^{-3}qp^3 = q^{9^3}$ (propiedad (1) y que $p^{-1}qp = q^9$)
Entonces $u^{-1}qu = q^{9^3} = q^{726} = q^{66*11+3} = q^3$.
Y entonces $qu = uq^3$.
Entonces, el grupo es igual a:

$$G = \langle u, q | u^5 = q^{11} = e \ , qu = uq^3 \rangle$$

Que es igual al grupo que ya habíamos considerado para $i = 3$.

Entonces, tenemos que la única opción en este caso es:

$$G = \langle p, q | p^5 = q^{11} = e \ , qp = pq^3 \rangle$$

Por lo tanto, en total encontramos dos posibilidades para G:

$$G \simeq \mathbb{Z}_5 \times \mathbb{Z}_{11}$$
$$G = \langle p, q | p^5 = q^{11} = e \ , qp = pq^3 \rangle$$

.

d) **Mostrar que existen exactamente 4 homomorfismos distintos de $\mathbb{Z}_2$ en $Aut(\mathbb{Z}_8)$**

Por el lema 30.2, tenemos que $Aut(\mathbb{Z}_8) \simeq \mathbb{Z}_8^*$. Entonces veremos mejor los morfismos de $\mathbb{Z}_2$ con $\mathbb{Z}_8^*$.
Consideremos que el morfismo es $\phi : \mathbb{Z}_2 \to \mathbb{Z}_8^*$
Primero que nada si ϕ es un homomorfismo, se debe de cumplir (teorema 7.13 a)) que $\phi(e)$ es al identidad de $\mathbb{Z}_8^*$, que es $\bar{1}$.

Por otro lado, debemos de tener que $\phi(1) = i$ para un $i \in \mathbb{Z}_8^*$.
Pero como $1 \in \mathbb{Z}_2$ tiene orden 2, entonces $\phi(1) \in \mathbb{Z}_8^*$ también debe de tener orden 2.
Entonces $(\phi(1))^2 = \bar{1} \ \Rightarrow \ i^2 = \bar{1}$
Lo que nos deja con las posibilidades que $i = 1$ (porque $1^2 = 1 \equiv 1 \ \ (mod\ 8)$), $i = 3$ (porque $3^2 = 9 \equiv 1 \ (mod\ 8)$) , $i = 5$ (porque $5^2 = 25 \equiv 1 \ (mod\ 8)$) , $i = 7$ (porque $7^2 = 49 \equiv 1 \ (mod\ 8)$).
Entonces, eso nos deja con 4 opciones para los morfismos:

a) $\phi(\bar{0}) = \bar{1}, \phi(\bar{1}) = \bar{1}$.
   Que es el morfismo que manda todo a la identidad.
b) $\phi(\bar{0}) = \bar{1}, \phi(\bar{1}) = \bar{3}$
   Vemos que es un morfismo porque 'separa' todos los productos posibles:
   - $\phi(\bar{0} + \bar{0}) = \phi(\bar{0}) = \bar{1} = \bar{1} \cdot \bar{1} = \phi(\bar{0}) \cdot \phi(\bar{0})$
   - $\phi(\bar{0} + \bar{1}) = \phi(\bar{1}) = \bar{3} = \bar{1} \cdot \bar{3} = \phi(\bar{0}) \cdot \phi(\bar{1})$
   - $\phi(\bar{1} + \bar{0}) = \phi(\bar{1}) = \bar{3} = \bar{3} \cdot \bar{1} = \phi(\bar{1}) \cdot \phi(\bar{0})$
   - $\phi(\bar{1} + \bar{1}) = \phi(\bar{0}) = \bar{1} = \bar{9} = \bar{3} \cdot \bar{3} = \phi(\bar{1}) \cdot \phi(\bar{1})$
c) $\phi(0) = 1, \phi(1) = 5$ Vemos que es un morfismo porque 'separa' todos los productos posibles:
   - $\phi(\bar{0} + \bar{0}) = \phi(\bar{0}) = \bar{1} = \bar{1} \cdot \bar{1} = \phi(\bar{0}) \cdot \phi(\bar{0})$

- $\phi(\bar{0}+\bar{1}) = \phi(\bar{1}) = \bar{5} = \bar{1}\cdot\bar{5} = \phi(\bar{0})\cdot\phi(\bar{1})$
- $\phi(\bar{1}+\bar{0}) = \phi(\bar{1}) = \bar{5} = \bar{5}\cdot\bar{1} = \phi(\bar{1})\cdot\phi(\bar{0})$
- $\phi(\bar{1}+\bar{1}) = \phi(\bar{0}) = \bar{1} = \bar{25} = \bar{5}\cdot\bar{5} = \phi(\bar{1})\cdot\phi(\bar{1})$

d) $\phi(0) = 1, \phi(1) = 7$ Vemos que es un morfismo porque 'separa' todos los productos posibles:

- $\phi(\bar{0}+\bar{0}) = \phi(\bar{0}) = \bar{1} = \bar{1}\cdot\bar{1} = \phi(\bar{0})\cdot\phi(\bar{0})$
- $\phi(\bar{0}+\bar{1}) = \phi(\bar{1}) = \bar{7} = \bar{1}\cdot\bar{7} = \phi(\bar{0})\cdot\phi(\bar{1})$
- $\phi(\bar{1}+\bar{0}) = \phi(\bar{1}) = \bar{7} = \bar{7}\cdot\bar{1} = \phi(\bar{1})\cdot\phi(\bar{0})$
- $\phi(\bar{1}+\bar{1}) = \phi(\bar{0}) = \bar{1} = \bar{49} = \bar{7}\cdot\bar{7} = \phi(\bar{1})\cdot\phi(\bar{1})$

.

e) **Sean k un campo y G el grupo de las matrices triangulares superiores en $GL_3(k)$. Probar que G es el producto semidirecto $U \rtimes D$, donde U es el conjunto de las matrices triangulares superiores con 1s sobre la diagonal y D el conjunto de matrices diagonales en $GL_3(k)$.**

Usaremos el teorema 29.3. Que dice que si $U \trianglelefteq G$ y $D \leq G$ tales que $UD = G$ y $U \cap D = \{e\}$. Entonces $G \simeq U \rtimes D$.
Entonces tenemos varias cosas que demostrar:

- $D \leq G$. Vemos que el producto en D es cerrado. Tomamos dos matrices diagonales y vemos que el producto es diagonal:
$$\begin{pmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{pmatrix}\begin{pmatrix} d & 0 & 0 \\ 0 & e & 0 \\ 0 & 0 & f \end{pmatrix} = \begin{pmatrix} ad & 0 & 0 \\ 0 & be & 0 \\ 0 & 0 & cf \end{pmatrix}$$
- $U \leq G$. Tomamos dos matrices de U y vemos que el resultado está en U:
$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & d+a & e+af+b \\ 0 & 1 & f+c \\ 0 & 0 & 1 \end{pmatrix}$$
Este resultado es una matriz de U.
- $U \trianglelefteq G$. Vemos que para una matriz $A \in U$ y una $M \in G$ se cumple que $M^{-1}AM \in U$.
Para ello, sea: $M = \begin{pmatrix} a & b & c \\ 0 & d & e \\ 0 & 0 & f \end{pmatrix}$ y entonces $M^{-1} = \begin{pmatrix} a^{-1} & \# & \# \\ 0 & d^{-1} & \# \\ 0 & 0 & f^{-1} \end{pmatrix}$ Donde los $\#$ son valores que no nos interesan. Los valores de la diagonal son así porque M^{-1} debe de tener a los inversos de la diagonal de M sobre su diagonal (para que el producto MM^{-1} sea la matriz identidad).
Y ahora sera $A \in U$, por lo que $A = \begin{pmatrix} 1 & p & q \\ 0 & 1 & r \\ 0 & 0 & 1 \end{pmatrix}$ Luego, podemos ver que

$MAM^{-1} \in U$ notando que los elementos de la diagonal del producto de matrices triangulares se consiguen simplemente multiplicando los elementos diagonales de las matrices del producto. Entonces, tenemos que:

$$\begin{aligned} MAM^{-1} &= \begin{pmatrix} a & b & c \\ 0 & d & e \\ 0 & 0 & f \end{pmatrix} \begin{pmatrix} 1 & p & q \\ 0 & 1 & r \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} a^{-1} & \# & \# \\ 0 & d^{-1} & \# \\ 0 & 0 & f^{-1} \end{pmatrix} \\ &= \begin{pmatrix} aa^{-1} & \# & \# \\ 0 & dd^{-1} & \# \\ 0 & 0 & ff^{-1} \end{pmatrix} \\ &= \begin{pmatrix} 1 & \# & \# \\ 0 & 1 & \# \\ 0 & 0 & 1 \end{pmatrix} \end{aligned}$$

Que es una matriz de U. Por lo que $MAM^{-1} \in U$. Por tanto $U \trianglelefteq G$

- $D \cap U = \{e\}$. Sea $A \in D \cap U$. Entonces, A es una matriz diagonal, pero como $A \in U$, A debe de tener puros 1 en la diagonal. Por lo tanto, A es la matriz identidad.

- $G = UD$. Hay que probar que toda matriz $M \in G$ se puede ver como el producto de una matriz de U y una de D.
  Para ello, sea $G = \begin{pmatrix} a & b & c \\ 0 & d & e \\ 0 & 0 & f \end{pmatrix}$
  Entonces, lo podemos escribir como:

$$\begin{pmatrix} a & b & c \\ 0 & d & e \\ 0 & 0 & f \end{pmatrix} = \begin{pmatrix} 1 & b & c \\ 0 & 1 & e \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} a & 0 & 0 \\ 0 & d & 0 \\ 0 & 0 & f \end{pmatrix}$$

  Que es el producto de una matriz diagonal y una matriz de U.
  Con ello se prueba todo lo necesario para ver que $G \simeq U \rtimes D$