Álgebra Moderna Tarea 3.3

Tomás Ricardo Basile Álvarez
316617194

18 de noviembre de 2020

a) **Sea Y un $G-$ conjunto. Demuestre que la acción de G en Y induce una función:**

$$\phi : G \to S_y$$
$$\sigma \to \phi(\sigma)$$

donde

$$\phi(\sigma) : Y \to Y$$
$$y \to \sigma * y$$

Donde $*$ denota la acción de G en Y. [Sugerencia: muestra que $\phi(\sigma)$ es biyectiva, así $\phi(\sigma) \in S_Y$]

Para probar que $\phi : G \to S_Y$ es efectivamente una función entre estos conjuntos, hay que probar que $\phi(\sigma) \in S_Y$.
Para ello, notamos que por cómo se define, $\phi(\sigma)$ ya es una función de Y a Y y solamente hace falta mostrar que es biyectiva para que pertenezca a S_Y.

- **Inyectiva:** Supongamos que $\phi(\sigma)(y_1) = \phi(\sigma)(y_2)$ donde $y_1, y_2 \in Y$. Hay que demostrar que esto implica que $y_1 = y_2$.

$$\begin{aligned} & \phi(\sigma)(y_1) = \phi(\sigma)(y_2) \\ \Rightarrow \ & \sigma * y_1 = \sigma * y_2 \\ \Rightarrow \ & y_1 = y_2 \end{aligned}$$

  El último paso se demostró en el lema 22.4.

- **Suprayectiva:** Digamos que $y_2 \in Y$ es un elemento arbitrario y debemos de demostrar que existe un elemento $y_1 \in Y$ tal que $\phi(\sigma)(y_1) = y_2$

Esto es fácil, simplemente consideramos el elemento y_1 definido como $y_1 = \sigma^{-1} * y_2$, que es un elemento de Y. Entonces, tendremos que:

$$\begin{aligned}
\phi(\sigma)(y_1) &= \sigma * y_1 \\
&= \sigma * (\sigma^{-1} * y_2) \\
&= (\sigma\sigma^{-1}) * y_2 \quad \text{por def 22.1 A2} \\
&= e * y_2 \\
&= y_2 \quad \text{por def 22.1 A1}
\end{aligned}$$

Con lo que se demuestra que $\phi(\sigma)$ es biyectiva.

b) **Muestra que ϕ definida en el ejercicio anterior es un homomorfismo**

Debemos de mostrar que si $\sigma_1, \sigma_2 \in G$, entonces $\phi(\sigma_1 \cdot \sigma_2) = \phi(\sigma_1) \cdot \phi(\sigma_2)$.
$\phi(\sigma_1 \cdot \sigma_2)$ y $\phi(\sigma_1) \cdot \phi(\sigma_2)$ son ambas permutaciones de Y en Y. Para probar que son iguales hay que probar que dan la misma imagen para un $y \in Y$ arbitrario.

$$\begin{aligned}
\phi(\sigma_1 \cdot \sigma_2)(y) &= (\sigma_1 \cdot \sigma_2) * y \\
&= \sigma_1 * (\sigma_2 * y) \quad \text{por def 22.1 A2} \\
&= \phi(\sigma_1)(\sigma_2 * y) \\
&= \phi(\sigma_1)(\phi(\sigma_2)(y)) \\
&= (\phi(\sigma_1) \circ \phi(\sigma_2))(y)
\end{aligned}$$

Entonces, $\phi(\sigma_1 \cdot \phi_2)$ y $\phi(\sigma_1) \circ \phi(\sigma_2)$ tienen la misma imagen al aplicarlas sobre cualquier $y \in Y$ y por tanto son iguales.

c) **Recíprocamente, si:**

$$\psi : G \to S_Y$$

es homomorfismo de grupos. Prueba que ψ induce una acción de G en Y dada por $\sigma * y := \psi(\sigma)(y)$

Para probar que se trata de una acción de grupos hay que ver primero que $\sigma * y$ da un elemento de Y para todo $\sigma \in G, y \in Y$. Para ello, vemos que $\sigma * y = \psi(\sigma)(y)$ pero $\psi(\sigma)$ es una biyección de S_Y, por lo que $\psi(\sigma)(y)$ se encuentra en Y.
Ahora hay que probar que cumple con las dos condiciones de la definición:

A1) Probar que $e * y = y \quad \forall y \in Y$.

Dem: $e * y = \psi(e)(y)$.
Pero como ψ es un homeomorfismo y e es el neutro de G, entonces $\psi(e)$ será el neutro de S_Y, es decir, la permutación identidad. Por lo que $\psi(e)(y) = y$.
Entonces, $e * y = y$

A2) Probar que $a * (b * y) = (ab) * y \quad \forall y \in Y, \forall a, b \in G$

Dem:

$$\begin{aligned} a * (b * y) &= \psi(a)(b * y) \\ &= \psi(a)(\psi(b)(y)) \\ &= (\psi(a) \circ \psi(b))(y) \end{aligned}$$

Pero como ψ es un homeomorfismo, $\psi(a) \circ \psi(b) = \psi(ab)$. Entonces lo anterior es igual a $\psi(ab)(y)$.
Por lo tanto

$$a * (b * y) = \psi(ab)(y) = (ab) * y$$

Con esto queda probado lo que se pedía.

d) **Muestra que todo grupo de orden 15 es cíclico. [Sugerencia: Teorema de Cauchy prueba que $bab^{-1} = a^k$ para algún k**

Como 3 es un primo que divide a 15, el teorema de Cauchy nos asegura que existe un elemento b de orden 3. Y como 5 es un primo que divide a 15, el teorema de Cauchy nos asegura que existe un elemento a de orden 5.
Luego, tenemos a los subgrupos $\langle b \rangle$ de orden 3 y $\langle a \rangle$ de orden 5.

Luego usamos el corolario 22.11 que dice que si G es un grupo finito y p el menor primo dividiendo a $|G|$. Entonces, todo $H \leq G$ con $[G : H] = p$ es un subgrupo normal de G.
En este caso, 3 es el menor primo factor de 15. Y $\langle a \rangle$ tiene un índice de $[G : \langle a \rangle] = |G|/|\langle a \rangle| = 15/5 = 3$.
Entonces, esto implica que $\langle a \rangle$ es un subgrupo normal.
Lo que quiere decir que el conjugado de todo elemento de $\langle a \rangle$ vuelve a ser un elemento de $\langle a \rangle$.
Entonces:

$$\begin{aligned} & bab^{-1} \in \langle a \rangle \\ \Rightarrow \quad & bab^{-1} = a^k \end{aligned}$$

para un entero k.

Ahora probamos por inducción que $b^n a b^{-n} = a^{k^n}$
El caso base ya lo tenemos arriba. Y ahora suponemos que se cumple la hipótesis de inducción $b^n a b^{-n} = a^{k^n}$ y con ello demostramos que:

$$\begin{aligned} b^{n+1} a b^{-(n+1)} &= b^{n+1} a b^{-n-1} \\ &= b b^n a b^{-n} b^{-1} \\ &= b(b^n a b^{-n}) b^{-1} \\ &= b(a^{k^n}) b^{-1} \quad \text{por la hipótesis de inducción} \\ &= (bab^{-1})^{k^n} \\ &= (a^k)^{k^n} \quad \text{por el caso n=1} \\ &= a^{k \cdot k^n} \\ &= a^{k^{n+1}} \end{aligned}$$

Entonces queda probado el caso para $n+1$.
Entonces ya hemos probado por inducción que $b^n a b^{-n} = a^{k^n}$

Luego, si usamos este teorema con $n = 3$, tenemos que:

$$\begin{aligned} & b^3 a b^{-3} = a^{k^3} \\ \Rightarrow \quad & eae = a^{k^3} \quad \text{porque} \quad \text{b tiene orden 3} \\ \Rightarrow \quad & a = a^{k^3} \\ \Rightarrow \quad & a^{k^3 - 1} = e \end{aligned}$$

Pero como a tiene orden 5, esto implica que $k^3 - 1$ es un múltiplo de 5.

Veremos ahora que si $k^3 - 1$ es múltiplo de 5, entonces $k^3 \equiv 1 \pmod{5}$, lo que implica que $k \equiv 1 \ (mod\ 5)$
Entonces, como a tiene orden 5, esto implica que $a^k = a$

Luego, tenemos que $bab^{-1} = a^k \Rightarrow bab^{-1} = a \Rightarrow ba = ab$

Entonces, como esto significa que a y b conmutan, podemos probar que $(ab)^n = (ab)(ab)(ab)\cdots(ab) = a^n b^n$. Porque simplemente reordenamos los productos para que $(ab)(ab)(ab)\cdots(ab) = aa\cdots abb\cdots b$.

Luego, veamos cuál es el orden de ab.
El orden no puede ser 5 porque $(ab)^5 = a^5 b^5 = eb^3 b^2 = eb^2 = b^2 \neq e$
Y no tiene orden 3 porque $(ab)^3 = a^3 b^3 = a^3 e = a^3 \neq e$
Tampoco tiene orden 1, porque eso implicaría que $ab = e \Rightarrow a = b^{-1}$ pero esto es imposible porque a tiene orden 5 y b^{-1} orden 3.

Entonces, como ab debe de tener un orden que sea divisor de 15 pero no puede tener orden 1 , 3, 5, luego ab tiene orden 15.

Entonces el grupo es generado por ab.