Álgebra Tarea 1.4

Tomás Ricardo Basile Álvarez
316617194

6 de octubre de 2020

a)

Sean G, H grupos. Si $f : G \to H$ es un isomorfismo, probar que el orden de x y de $f(x)$ es igual, para todo $x \in G$.

Tenemos dos casos dependiendo de si el orden de x es finito o no:

- **x de orden finito:** Digamos que el orden de x es $n \in \mathbb{N}$. Lo que significa que $x^n = e_G$ y que para todo natural r con $0 < r < n$ se tiene que $x^r \neq e_G$
  Entonces, vemos que $f(x) \in H$ cumple que:

  $$\begin{aligned} f(x)^n &= f(x^n) \quad \text{(propiedad c del teorema 7.13 de las notas)} \\ &= f(e_G) \qquad \text{Porque } x^n = e_G \\ &= e_H \quad \text{Porque todo morfismo manda el cero de G al cero de H (inciso a teorema 7.13)} \end{aligned}$$

  Ya tenemos entonces que $f(x)^n = e_H$. Sin embargo, para ver que el orden de $f(x)$ es n, hay que probar también que n es el menor entero con esta propiedad, es decir, probar que para todo r con $0 < r < n$ se tiene que $f(x)^r \neq e_H$.
  Para esto, esperando una contradicción, suponemos que existe una r con $0 < r < n$ y $f(x)^r = e_H$ y entonces $f(x^r) = e_H$.
  Pero también, por las propiedades de los morfismos, $f(e_G) = e_H$

  Lo cual es una contradicción, porque f se supone inyectiva (es un isomorfismo), pero aquí se ve que no, porque está mandando a los dos elementos distintos x^r, e_G a la misma imagen. (x^r, e_G son distintos por lo dicho en el primer párrafo y porque $r < n$).

  Por tanto, debido a la contradicción, se probó que n es el mínimo entero positivo con $f(x)^n = e_H$. Lo que prueba que el orden de $f(x)$ es n y es igual al de x.

- x **de orden infinito**: Si x es de orden infinito, entonces $x^n \neq e_G$ para todo $n \in \mathbb{N}$.
  Luego, como f es inyectiva, se tiene que como $e_G \neq x^n$ entonces $f(e_G) \neq f(x^n)$ y por

tanto $e_H \neq f(x)^n$
Donde se usó que $f(x^n) = f(x)^n$ y que $f(e_G) = e_H$.
Por tanto, como $f(x)^n \neq e_H$ y la demostración anterior se vale para todo $n \in \mathbb{N}$, se probó que $f(x)$ no tiene orden finito. Entonces $f(x)$ tiene orden infinito, al igual que x

b)

Sean X, Y conjuntos finitos tales que $|X| = |Y|$. Sea $g : X \to Y$ una biyección. Definimos $f : S_X \to S_Y$ por $f(\sigma) = g \circ \sigma g^{-1}$ para todo σS_x. Prueba lo siguiente:

b1) **f está bien definida, es decir, si σ es una permutación de X entonces $g \circ \sigma \circ g^{-1}$ es una permutación de Y.**

Digamos que $\sigma : X \to X$ es una permutación de X, es decir, una función biyectiva de X en X.
Luego, por ser g biyectiva, tiene inversa y $g : X \to Y$, $g^{-1} : Y \to X$ y ambas son biyectivas (la inversa de una biyección es una biyección).
Entonces, la composición $g \circ \sigma \circ g^{-1}$ toma un elemento de $y \in Y$, lo convierte en $g^{-1}(y) \in X$, luego pasa por la permutación σ y se convierte en $\sigma(g^{-1}(y)) \in X$, para finalmente pasar por g, que lo manda a $g(\sigma(g^{-1}(x)))$ que está de vuelta en Y.
Es decir, $g \circ \sigma \circ g^{-1} : Y \to Y$.
Además, las tres funciones g, σ, g^{-1} son biyectivas, por lo que su composición es biyectiva.
Entonces, como $g \circ \sigma \circ g^{-1} : Y \to Y$ es biyectiva, es una permutación de Y.

b2) **f es una biyección entre S_X y S_Y**

Ya vimos en el inciso pasado que f toma una permutación σ de X y devuelve una permutación $g \circ \sigma \circ g^{-1}$ de Y, es decir, $f : S_X \to S_Y$.
Ya sólo falta probar que es una biyección.

- **Inyectiva:** Debemos probar que si $f(\sigma_1) = f(\sigma_2)$, entonces $\sigma_1 = \sigma_2$.
  Sea $f(\sigma_1) = f(\sigma_2)$, luego $g \circ \sigma_1 \circ g^{-1} = g \circ \sigma_2 \circ g^{-1}$.
  Luego, aplicamos g^{-1} de ambos lados y usamos que la composición de funciones es asociativa para asociar a conveniencia:
  $g^{-1} \circ (g \circ \sigma_1 \circ g^{-1}) = g^{-1} \circ (g \circ \sigma_2 \circ g^{-1}) \quad \Rightarrow \quad (g^{-1} \circ g) \circ (\sigma_1 \circ g^{-1}) = (g^{-1} \circ g) \circ (\sigma_2 \circ g^{-1}) \ \Rightarrow \ \sigma_1 \circ g^{-1} = \sigma_2 \circ g^{-1}$
  Ahora componemos con g a la derecha:
  $(\sigma_1 \circ g^{-1}) \circ g = (\sigma_2 \circ g^{-1}) \circ g \ \Rightarrow \ \sigma_1 \circ (g^{-1} \circ g) = \sigma_2 \circ (g^{-1} \circ g) \ \Rightarrow \ \sigma_1 = \sigma_2$
  Y se probó lo que se quería.

- **Suprayectiva:** Hay que probar que si $\tau \in S_Y$, entonces existe una σ en S_X tal que $f(\sigma) = \tau$.
  Sea $\tau \in S_Y$ y consideremos $\sigma = g^{-1} \circ \tau \circ g$. Se puede ver que σ es un elemento

de S_X con un argumento muy similar al de $b1$ (Como τ, g, g^{-1} son biyecciones, entonces σ también, y además se puede ver que σ toma elementos de X y devuelve elementos de X).
Y además, se tiene que $f(\sigma) = g \circ \sigma \circ g^{-1} = g \circ (g^{-1} \circ \tau \circ g) \circ g^{-1} = (g \circ g^{-1}) \circ \tau \circ (g^{-1} \circ g) = \tau$.
Con lo que se prueba lo que se quería probar.

Como f es inyectiva y suprayectiva, es una biyección.

b3) f **es un morfismo de grupos, es decir,** $f(\sigma \circ \tau) = f(\sigma) \circ f(\tau)$

Probamos directamente esa igualdad, usando que la composición de funciones es asociativa y denotando por I_X la función identidad en X (que es el neutro de S_X):
$f(\sigma \circ \tau) = g \circ (\sigma \circ \tau) \circ g^{-1} = g \circ (\sigma \circ (I_X \circ \tau)) \circ g^{-1} = g \circ (\sigma \circ (g^{-1} \circ g \circ \tau)) \circ g^{-1}$
$= (g \circ \sigma \circ g^{-1}) \circ (g \circ \tau \circ g^{-1}) = f(\sigma) \circ f(\tau)$

c)

Sea $H_1 \leq H_2 \leq ....$ una cadena descendente de subgrupos de un grupo G. Probar que $\bigcup_{i=1}^{\infty} H_i$ es un subgrupo de G

Como vimos en el lema 6.8 de clase, y como claramente $\bigcup_{i=1}^{\infty} H_i$ es un subconjunto de G (porque cada H es un subconjunto de G), para probar que es un subgrupo solamente hay que probar que el producto es cerrado y que todo elemento tiene un inverso dentro de $\bigcup_{i=1}^{\infty} H_i$. Es decir, probamos que:

- **Si $x, y \in \bigcup_{i=1}^{\infty} H_i$ entonces $xy \in \bigcup_{i=1}^{\infty} H_i$**
  Sea $x, y \in \bigcup_{i=1}^{\infty} H_i$, entonces $x \in H_j$ para alguna $j \in \mathbb{N}$ y $y \in H_k$ para alguna $k \in \mathbb{N}$. Luego, sin pérdida de generalidad podemos suponer que $j \leq k$. Con esto, por ser una cadena de subgrupos, se tiene que $H_j \leq H_k$ y entonces, como $x \in H_j$, se concluye que $x \in H_k$.
  Luego, $x, y \in H_k$ y como H_k es un grupo, el producto es cerrado y se tiene que $xy \in H_k$. Luego, evidentemente $xy \in \bigcup_{i=1}^{\infty} H_i$ y listo.

- **Probar que si $a \in \bigcup_{i=1}^{\infty} H_i$ entonces $a^{-1} \in \bigcup_{i=1}^{\infty} H_i$**
  Sea $a \in \bigcup_{i=1}^{\infty} H_i$, entonces $a \in H_j$ para alguna $j \in \mathbb{N}$. Y como H_j es un grupo, es cerrado bajo inversos, por lo que $a^{-1} \in H_j$. Esto claramente implica que $a^{-1} \in \bigcup_{i=1}^{\infty} H_i$ y listo.

d)

Mostrar que el conjunto $\{x \in D_{2n} | x^2 = 1\}$ no es un subgrupo de D_{2n} para $n \geq 3$

Consideramos los elementos $s, sr \in D_{2n}$ con s, r como han sido definidos para grupos diédricos en las notas. Probamos primero que estos elementos pertenecen al conjunto $\{x \in D_{2n}|x^2 = 1\}$. Para lo que hay que probar que al multiplicarlos por sí mismos se obtiene la identidad:

- **Probar que** $s^2 = 1$
  Esto ya se vió en las notas y es de hecho una de las realaciones generadoras de D_{2n}

- **Probar que** $(sr)^2 = 1$
  $(sr)^2 = (sr)(sr) = s(rs)s = s(sr^{-1})r$ Por la relación generadora de D_{2n} que dice que $rs = sr^{-1}$
  $= (ss)(r^{-1}r) = (s^2)1 = s^2 = 1$

Luego, $s, sr \in \{x \in D_{2n}|x^2 = 1\}$. Sin embargo, si este conjunto fuera un grupo, debería de cumplir que el producto es cerrado. Pero cuando tomamos el producto de estos dos elementos, nos queda: $s(sr) = s^2r = (1)r = r$.
Y claramente $r \notin \{x \in D_{2n}|x^2 = 1\}$ porque se vió en las notas que el orden de r es n y se supone que $n \geq 3$, por lo que es imposible que $r^2 = 1$.
Lo que prueba que el producto en $\{x \in D_{2n}|x^2 = 1\}$ no es cerrado y por tanto no es un subgrupo.

e)

Sea $n \geq 3$. Para cada $\alpha \in S_n$ considera la matriz:

$$E_\alpha := [e_{\alpha(1)}\ e_{\alpha(2)}\ \cdots\ e_{\alpha(n)}]$$

Donde e_i es la iésima columa de la matriz identidad. Por 6.11(d), sabemos que $\mathcal{S}_n = \{E_\alpha|\alpha \in S_n\}$ es un grupo de $n!$ elementos.
Muestra que el conjunto $\mathcal{A}_n = \{A \in \mathcal{S}_n|\det A = 1\}$ es un subgrupo de $\mathcal{S}_n$ de $\frac{n!}{2}$ elementos.
Hint. Considera las funciones:

$$\det :\ \mathcal{S}_n \to \mathbb{Z}\ ,\ a \to \det A$$
$$f : \mathcal{S}_n \to S_n, A \to AE_{(1,2)}$$

.

Probar que $\mathcal{A}_n$ es un subgrupo es sencillo. Pues como damos ya por hecho que $\mathcal{S}_n$ es un grupo y claramente $\mathcal{A}_n \subset \mathcal{S}_n$, lo único que hay que probar es que el producto es cerrado en $\mathcal{A}_n$ y que cada elemento de $\mathcal{A}_n$ tiene un inverso ahí mismo:

- **Producto es Cerrado:**
  Consideramos a $A, B \in \mathcal{A}_n$ dos elementos arbitrarios. Como pertenecen a $\mathcal{A}_n$, cumplen que $\det(A) = \det(B) = 1$. Luego, su producto es el producto de matrices usual AB que tiene un determinante de:
  $\det(AB) = \det(A)\det(B) = (1)(1) = 1$
  Donde se usó que el determinante separa productos (es un morfismo del grupo general lineal a los reales) como vimos en las notas.
  Como AB tiene determinante 1, entonces $AB \in \mathcal{A}_n$ y listo.

- **Una matriz $A \in \mathcal{A}_n$ tiene inverso en $\mathcal{A}_n$**
  Sea $A \in \mathcal{A}_n$, que por tanto tiene $\det(A)$.
  Como $A \in \mathcal{S}_n$ y como se tomó por supuesto que $\mathcal{S}_n$ es un grupo, entonces existe $A^{-1} \in \mathcal{S}_n$. Por lo tanto, ya solamente hace falta probar que $\det(A^{-1}) = 1$ para probar que $A^{-1} \in \mathcal{A}_n$

  Como $AA^{-1} = I_n$ (Matriz identidad de nxn) y $\det(I_n) = 1$, tenemos que
  $1 = \det(I_n) = \det(AA^{-1}) = \det(A)\det(A^{-1})$
  Por lo que $\det(A^{-1}) = \dfrac{1}{\det(A)} = \dfrac{1}{1} = 1$
  Por lo que $A^{-1} \in \mathcal{A}_n$

Ya tenemos entonces que $\mathcal{A}_n$ es un grupo.
Solamente hace falta probar que $\mathcal{A}_n$ tiene $\dfrac{n!}{2}$ elementos.

Para esto, primero notamos que todas las matrices de $\mathcal{S}_n$ tienen determinante 1 ó -1. Esto se debe a que el determinante de la matriz identidad es 1 y como se ve en álgebra lineal, intercambiar dos columnas de una matriz solamente causa que su determinante cambie de signo. Luego, como todas las matrices de $\mathcal{S}_n$ se consiguen al permutar las columnas de la matriz identidad, y estas permutaciones se pueden ver como una composición de varios 'intercambios' de dos en dos de columnas, entonces la matriz resultante tendrá determinante 1 o -1.

Luego, $\mathcal{A}_n$ es el grupo de estas matrices con determinante 1 y definimos ahora $\mathcal{B}_n$ como el conjunto de matrices de $\mathcal{S}_n$ de determinante -1.
Por lo mencionado antes de que las matrices de $\mathcal{S}_n$ tiene determinante 1 o -1, tenemos que: $\mathcal{A}_n \cup \mathcal{B}_n = \mathcal{S}_n$ y además claramente $\mathcal{A}_n \cap \mathcal{B}_n = \emptyset$.
Ahora probaré que existe una biyección entre $\mathcal{A}_n$ y $\mathcal{B}_n$, lo que demuestra que tienen la misma cantidad de elementos y como juntos forman a $\mathcal{S}_n$, cada uno debe de tener la mitad de elementos de $\mathcal{S}_n$.

Para esto, consideramos una función $f : \mathcal{A}_n \to A_n$
Y definimos que lo que hace la función es tomar una matríz A de $\mathcal{A}_n$ y devolver $f(A)$ que es la misma matriz pero con las primeras dos columnas intercambiadas.

Probamos ahora que $f : \mathcal{A}_n \to \mathcal{B}_n$ es una biyección.

- **Probar que efectivamente manda elementos de $\mathcal{A}_n$ a elementos de $\mathcal{B}_n$:** Sea $A \in \mathcal{A}_n$, entonces A se ve como una permutación de las columnas de la matriz identidad y además $\det(A) = 1$. Luego, $f(A)$ se consigue al intercambiar las primeras dos columnas de A, por lo que $f(A)$ sigue siendo una permutación de las columnas de la matriz identidad. Y como se intercambiaron dos columnas, el determinante cambia de signo y $\det(f(A)) = -\det(A) = -1$, por lo que $f(A) \in \mathcal{B}_n$

- **Inyectividad:** Sea $A_1, A_2 \in \mathcal{A}_n$ con $A_1 \neq A_2$. Hay que probar que $f(A_1) \neq f(A_2)$
Esto es claro porque $A_1 \neq A_2$ y al aplicar f, se le intercambia las primeras dos columnas a estas matrices. Luego, si A_1 y A_2 tenían una diferencia en alguna columna que no fuera las primeras dos, $f(A_1)$ y $f(A_2)$ seguirán teniendo esa diferencia. Si A_1 y A_2 eran distintas porque tenían una diferencia en la primera columna, entonces ahora $f(A_1), f(A_2)$ tendrán la diferencia en la segunda columna. Y si A_1 y A_2 eran distintas porque tenían una diferencia en la segunda columna, entonces ahora $f(A_1), f(A_2)$ tendrán la diferencia en la primera columna.
En cualquier caso, si A_1, A_2 son distintas, entonces $f(A_1) \neq f(A_2)$

- **Suprayectivo:** Sea $B \in \mathcal{B}_n$, hay que probar que existe una $A \in \mathcal{A}_n$ tal que $f(A) = B$. Como $B \in \mathcal{B}_n$, entonces B tiene determinante -1 y B es una permutación de las columnas de la matriz identidad.
Ahora definimos una matriz A como la matriz B pero con las dos primeras columnas intercambiadas. Entonces A seguirá siendo una permutación de la matriz identidad, pero ahora con determinante 1. Por lo tanto $A \in \mathcal{A}_n$
Finalmente, por cómo se definió A, vemos claramente que $f(A) = B$ y listo.

Entonces $f : \mathcal{A}_n \to \mathcal{B}_n$ es una biyección entre estos dos conjuntos. Lo que implica que los dos conjuntos tienen la misma cantidad de elementos. Y como los dos conjuntos juntos forman a $\mathcal{S}_n$, cada uno debe de tener la mitad de elementos que $\mathcal{S}_n$ (la mitad de $n!$)
Y por tanto, $|\mathcal{A}_n| = \dfrac{n!}{2}$