TP 5.2 - Morfismos

▼ 1. Analizar si las siguientes funciones son homomorfismos entre las estructuras algebraicas indicadas y en caso afirmativo hallar núcleo e imagen

- Una función entre dos estructuras algebraicas (grupos, anillos, etc.) es un homorfismo si respeta/preserva la operación de esas estructuras
  - Para una función $f : G \to H$ entre dos grupos, f es un homorfismo si para cualquier $a, b \in G$:

$$f(a * b) = f(a) * f(b)$$

  - Donde $*$ es la operación del grupo G y también la de H.
- El núcleo de un homorfismo es el conjunto de elementos de G que se envían al elemento neutro de H.

$$Nu(f) = \{g \in G : f(g) = e_H\}$$

  - Todos los elementos cuya imagen es el neutro del codominio.
- La imagen de un homorfismo es el conjunto de todos los valores en el codominio H que f puede tomar al evaluar elementos en G:

$$Im(f) = \{b \in H : \exists a \in G, f(a) = b\}$$

  - La imagen de f muestra "hasta dónde" llega el homorfismo en H y es un subgrupo de H.

(a) $f : G \to F$ dada por $f(x) = 2^x$ y siendo los grupos $G = (\mathbb{R}, +)$ los reales con la suma usual, $F = (\mathbb{R}_0, \cdot)$ los reales sin el 0 con el producto usual

Para que f sea un homorfismo tenemos que ver si $f(x+y) = f(x) \cdot f(y)$ para todo $x, y \in G$.

$$f(x+y) = 2^{x+y}$$

- Por propiedades de las potencias, esto lo podemos reescribir como:

$$2^{x+y} = 2^x \cdot 2^y = f(x) \cdot f(y)$$

- Por lo tanto, f es un homorfismo de grupos.

El núcleo de f son aquellos elementos de G que van hacía el neutro de F (el neutro de la multiplicación en $\mathbb{R}_0$ es 1):

$$Nu(f) = \{x \in \mathbb{R} : f(x) = 1\}$$

- Entonces:

$$f(x) = 1 \to 2^x = 1 \to x = 0$$

- Por lo tanto $Nu(f) = \{0\}$

La imagen de f es el conjunto de valores posibles de $f(x) = 2^x$ cuando $x \in \mathbb{R}$:

$$Im(f) = \{2^x : x \in \mathbb{R}\} = (0, +\infty)$$

(b) $f : G \to F$ dada por $f(x) = -x$ y siendo los grupos $G = (\mathbb{Z}, *)$ los enteros con la operación $a * b = a + b + ab$, $F = (\mathbb{Z}, \circ)$ los enteros con la operación $a \circ b = a + b - ab$

Para que f sea un homorfismo hay que verificar si $f(a * b) = f(a) \circ f(b)$, para todo $a, b \in G$.

$$f(a * b) = f(a + b + ab) = -(a + b + ab) = -a - b - ab$$

- Calculamos $f(a) \circ f(b)$:

$$f(a) = -a \qquad f(b) = -b$$

- Entonces:

$$f(a) \circ f(b) = (-a) \circ (-b) = -a + (-b) - (-a)(-b) = -a - b - ab$$

- Como $f(a * b) = f(a) \circ f(b)$, podemos decir que f es un homorfismo.

El núcleo de f es el conjunto de los elementos de G que se corresponden con el neutro de F (el neutro de $(\mathbb{Z}, \circ)$ es 0):

$$Nu(f) = \{a \in \mathbb{Z} : f(a) = 0\}$$

- Entonces:

$$f(a) = 0 \rightarrow -a = 0 \rightarrow a = 0$$

- Por lo tanto $Nu(f) = \{0\}$

La imagen de f es el conjunto de todos los valores posibles de $f(a) = -a$ cuando $a \in \mathbb{Z}$.

- Como $-a$ recorre todos los enteros cuando a recorre todos los enteros:

$$Im(f) = \mathbb{Z}$$

(c) $f : (P(A), \cup) \rightarrow (P(A), \cap)$ dada por $f(X) = X^c$ (siendo A cualquier conjunto, $P(A)$ indica el conjunto de partes de A y X^c el complemento de un conjunto)

Para que f sea un homorfismo, necesitamos verificar si $f(X \cup Y) = f(X) \cap f(Y)$ para todo $X, Y \subseteq A$.

- Calculamos $f(X \cup Y)$:

$$f(X \cup Y) = (X \cup Y)^c$$

- Por propiedades de los componentes, sabemos que $(X \cup Y)^c$ es lo mismo que $X^c \cap Y^c$.

$$f(X \cup Y) = (X \cup Y)^c = X^c \cap Y^c = f(X) \cap f(Y)$$

- Entonces f es un homorfismo.

El núcleo de f es el conjunto de elementos en $P(A)$ que se corresponden con el neutro de $(P(A), \cap)$.

- El neutro de la intersección es A. Para todo $X \subseteq A \rightarrow X \cap A = X$.

$$Nu(f) = \{X \subseteq A : f(X) = A\}$$

- Entonces:

$$f(X) = A \rightarrow X^c = A \rightarrow X = \emptyset$$

- Por lo tanto, $Nu(f) = \{\emptyset\}$

La imagen de f es el conjunto de todos los valores posibles de $f(X) = X^c$ cuando $X \subseteq A$:

$$Im(f) = \{X^c : X \subseteq A\} = P(A)$$

▼ 2. Sea $f : G \rightarrow H$ un homomorfismo de grupos. Demostrar que el núcleo y la imagen de f son subgrupos de G y H respectivamente

Para demostrar que el núcleo y la imagen de un homomorfismo de grupos $f : G \rightarrow H$ hay que analizar si cumplen las propiedades correspondientes de un subgrupo.

¿$Nu(f)$ es subgrupo de G?

- El núcleo de f se define como:
  - Siendo e_H el neutro en H.

$$Nu(f) = \{g \in G : f(g) = e_H\}$$

- Podemos ver que $f(e_G) = e_H$, siendo e_G el neutro en G. Por lo tanto, $Nu(f)$ tiene elemento neutro.
- Sean $a, b \in Nu(f)$, es decir:

$$f(a) = e_H \quad \& \quad f(b) = e_H$$

- Considerando ab^{-1}, vamos a ver si $f(ab^{-1}) = e_H$
- Como f es un homomorfismo:

$$f(ab^{-1}) = f(a)f(b^{-1})$$

- Por las propiedades de los homomorfismos y sabiendo que $f(b) = e_H$:

$$f(b^{-1}) = (f(b))^{-1} = e_H^{-1} = e_H$$

- Por lo tanto:

$$f(ab^{-1}) = f(a)f(b^{-1}) = e_H e_H = e_H$$

- Lo que demuestra que $ab^{-1} \in Nu(f)$, o sea, $Nu(f)$ está bien definida y contiene los inversos de sus elementos.

- $Nu(f)$ es subgrupo de G, ya que demostramos que cumple las características para serlo.

¿$Im(f)$ es subgrupo de H?

- La imagen de f se define como:

$$Im(f) = \{h \in H : \exists g \in G, f(g) = h\}$$

- Sabemos que $f(e_G) = e_H$, donde e_G es el neutro en G y e_H el neutro en H, es decir, $e_H \in Im(f)$. Por lo tanto, el elemento neutro de $Im(f)$ es e_H.
- Sean $y_1, y_2 \in Im(f)$, existen $g_1, g_2 \in G$ tales que:

$$y_1 = f(g_1) \quad \& \quad y_2 = f(g_2)$$

  - Vamos a demostrar que $y_1 y_2^{-1} \in Im(f)$.
  - Como f es un homomorfismo:

$$y_1 y_2^{-1} = f(g_1)f(g_2)^{-1} = f(g_1)f(g_2^{-1}) = f(g_1 g_2^{-1})$$

  - Como $g_1 g_2^{-1} \in G$, esto implica que $y_1 y_2^{-1} \in Im(f)$, lo que demuestra que $Im(f)$ está bien definida y la existencia de los inversos para sus elementos.

- $Im(f)$ es subgrupo de G, ya que demostramos que cumple las características para serlo.

▼ 3. Sea $(G, *)$ un grupo. Demostrar que la función $f : G \to G$ definida por $f(a) = a^2$ es un homomorfismo si y sólo si G es abeliano (recordar un ejercicio de grupos abelianos de la primera parte del TP 5)

CONSULTAR

Si f es homomorfismo, entonces G es abeliano.

- Al ser f homomorfismo, significa que para cualquier $a, b \in G$ se cumple:

$$f(a * b) = f(a) * f(b)$$
$$(a * b)^2 = a^2 * b^2$$
$$(a * b) * (a * b) = (a * a) * (b * b)$$

- Asociatividad:

$$a * (b * a) * b = a * (a * b) * b$$

- Cancelamos a y b en ambos lados de la ecuación:

$$b * a = a * b$$

- Como obtuvimos que $b * a = a * b$, entonces G es abeliano (se cumple la conmutatividad).

Si G es abeliano, entonces f es homomorfismo.

- Al ser G abeliano se cumple que $a * b = b * a$, para todo $a, b \in G$.
- Queremos probar que $f(a * b) = f(a) * f(b)$ para todo $a, b \in G$.
- Sabiendo que $f(a) = a^2$

$$f(a * b) = (a * b)^2 = (a * b) * (a * b)$$

- Como en G se cumple la conmutatividad:

$$(a * b) * (a * b) = a * a * b * b = a^2 * b^2 = f(a) * f(b)$$

- Por lo tanto, si G es abeliano, se cumple que f es homomorfismo, es decir, $f(a * b) = f(a) * f(b)$ para cualquier $a, b \in G$.

Demostramos que $f(a) = a^2$ es un homomorfismo *si y sólo si* G es abeliano.

▼ 4. Si H_1, H_2 son dos subgrupos de un grupo conmutativo G, probar que la aplicación $f : H_1 \times H_2$ dada por $f(a, b) = ab$, es un morfismo de gruposG

Como H_1 y H_2 son subgrupos de G, cualquier par (a, b) siendo $a \in H_1$ y $b \in H_2$, entonces $a, b \in G$.

- Como G es abeliano, $ab \in G$, es decir $f(a, b)$ es elemento de G.

Tenemos que demostrar que para todo $(a_1, b_1), (a_2, b_2) \in H_1 \times H_2$.

- Siendo $a_1, a_2 \in H_1$ y $b_1, b_2 \in H_2$:

$$f((a_1, b_1) \cdot (a_2, b_2)) = f(a_1, b_1) \cdot f(a_2, b_2)$$

- Desarrollamos $f((a_1, b_1) \cdot (a_2, b_2))$:

$$f((a_1, b_1) \cdot (a_2, b_2)) = f(a_1a_2, b_1b_2) = (a_1a_2)(b_1b_2)$$

- Conmutatividad (Como G es abeliano):

$$(a_1a_2)(b_1b_2) = (a_1b_1)(a_2b_2) = f(a_1b_1) \cdot f(a_2, b_2)$$

Se demostró que $f((a_1, b_1) \cdot (a_2, b_2)) = f(a_1, b_1) \cdot f(a_2, b_2)$, por lo tanto f es un morfismo de grupos.

▼ 5. Si $f : G_1 \to G_2$ es un morfismo de grupos entonces es monomorfismo si y sólo si $Nu(f) = \{e_1\}$.

Si f es un monomorfismo, entonces $Nu(f) = \{e_1\}$.

- Suponiendo que f es un monomorfismo, o sea, que es inyectivo (a cada elemento del dominio le corresponde un único elemento del codominio).
- El núcleo de f es el conjunto de todos los elementos de G_1 que se corresponden con el neutro de G_2, es decir:

$$Nu(f) = \{g \in G_1 : f(g) = e_2\}$$

- Si $f(g) = e_2$, para algún $g \in G_1$, entonces debe ser que $g = e_1$ (neutro de G_1). Si existiese otro elemento distinto que e_1 que se corresponda con e_2, no se estaría cumpliendo la inyectividad (propiedad de monomorfismos).
- Entonces, podemos decir que:

$$Nu(f) = \{e_1\}$$

Si $Nu(f) = \{e_1\}$, entonces f es monomorfismo

- Suponiendo que $Nu(f) = \{e_1\}$ queremos demostrar que f es un monomorfismo, o sea, que a todo elemento del dominio le corresponde un único elemento en el codominio.
    - Para todos $g_1, g_2 \in G_1$

$$f(g_1) = f(g_2) \to g_1 = g_2$$

- Supongamos que $f(g_1) = f(g_2)$:

$$f(g_1) = f(g_2) \to f(g_1) \cdot f(g_2)^{-1} = e_2$$

    - Siendo e_2 el neutro de G_2
- Como f es un morfismo de grupos:

$$f(g_1 \cdot g_2^{-1}) = f(g_1) \cdot f(g_2)^{-1} = e_2$$

- Por la definición de núcleo, esto significa que $g_1 \cdot g_2^{-1} \in Nu(f)$.
- Por hipótesis, tenemos que $Nu(f) = \{e_1\}$, por lo tanto, podemos decir que:

$$g_1 \cdot g_2^{-1} = e_1$$

- Esto implica que $g_1 = g_2$, ya que $g_1 \cdot g_2^{-1} = e_1$, significa que g_1 y g_2 son el mismo elemento en G_1.

▼ 6. Sea $(G, *)$ un grupo. Demostrar que la función $f : G \to G$ definida por $f(a) = a^{-1}$ es un isomorfismo si y sólo si G es abeliano.

Si f es un isomorfismo, entonces G es abeliano.

- Como f es un morfismo de grupos, se cumple que:
    - Para todo $a, b \in G$

$$f(a * b) = f(a) * f(b)$$

- Como $f(a) = a^{-1}$

$$f(a * b) = (a * b)^{-1} \quad \& \quad f(a) * f(b) = a^{-1} * b^{-1}$$

- Por la definición de f, tenemos:

$$(a * b)^{-1} = a^{-1} * b^{-1}$$

- Propiedad general de los inversos en un grupo:

$$(a * b)^{-1} = b^{-1} * a^{-1}$$

- Entonces, la igualdad quedaría como:

$$b^{-1} * a^{-1} = a^{-1} * b^{-1}$$

- Esto implica que G es conmutativo (abeliano), debido a que los inversos conmutan. Podemos deducir que para cualquier $a, b \in G : a * b = b * a$.

Si G es abeliano, entonces f es isomorfismo.

- Queremos probar que $f(a) = a^{-1}$ es un isomorfismo, para eso tenemos que probar que f es un morfismo de grupos y es biyectivo.
- Como G es abeliano, para cualquier $a, b \in G$

$$f(a * b) = (a * b)^{-1} = a^{-1} * b^{-1} = f(a) * f(b)$$

  - Podemos ver que f es un morfismo de grupos.
- Si $f(a) = f(b)$, entonces $a^{-1} = b^{-1}$, lo que implica que $a = b$, por lo tanto, f es inyectivo.
- Para cada $c \in G$, existe un $a \in G$ tal que $f(a) = c$
  - Si tomamos $a = c^{-1}$, ya que $f(c^{-1}) = (c^{-1})^{-1} = c$
  - Por lo tanto, f es sobreyectivo.
- Como f es un morfismo de grupos, es inyectivo y sobreyectivo, podemos decir que es un isomorfismo.

▼ 7. Sea R una relación de congruencia sobre un semigrupo $(S, *)$ y $(S/R,)$ el

semigrupo cociente correspondiente. Demostrar que la función $f_R : S \to S/R$ definida por $f_R(a) = \bar{a}$ es un homomorfismo.

Para demostrar que $f_R : S \to S/R$, que se define como $f_R(a) = \bar{a}$ es un homomorfismo de semigrupos, debemos probar que:

- Para todo $a, b \in S$

$$f_R(a * b) = f_R(a) \cdot f_R(b)$$

- S es un semigrupo con la operación $*$, y S/R es el conjunto cociente con la operación inducida, que podemos denotar como $\cdot$.

La operación $\cdot$ en S/R está definida como:

$$\bar{a} \cdot \bar{b} = \overline{a * b}$$

- R es una relación de congruencia sobre S, lo que garantiza que la operación $\cdot$ este bien definida en S/R.

Entonces, para que f_R sea un homomorgismo, debemos probar que para todo $a, b \in S$:

$$f_R(a * b) = f_R(a) * f_R(b)$$

- Por definición de f_R:

$$f_R(a * b) = \overline{a * b}$$

- Usando la definición de f_R y la operación en S/R

$$f_R(a) \cdot f_R(b) = \bar{a} \cdot \bar{b}$$

- Por la definición de la operación en S/R:

$$\bar{a} \cdot \bar{b} = \overline{a * b}$$

- Entonces, la igualdad quedaría como:

$$f_R(a * b) = \overline{a * b} = \bar{a} \cdot \bar{b} = f_R(a) \cdot f_R(b)$$

Demostramos que para todo $a, b \in S$ que $f_R(a * b) = f_R(a) \cdot f_R(b)$. Por lo tanto, f_R es un homomorfismo de semigrupos.

▼ 8. Sea z un número complejo. ¿Cuándo será un isomorfismo de grupos la aplicación $f : \mathbb{C} \to \mathbb{C}$ siendo $\mathbb{C}$ el conjunto de los números complejos, dada por $f(x) = z.x$?

Para que f sea un isomorfismo de grupos debe:

- Ser un morfismo de grupos, es decir que para todo $x, y \in \mathbb{C}$ $f(x + y) = f(x) + f(y)$.
- Debe ser inyectiva y sobreyectiva (biyectiva).

<u>¿Es morfismo?</u>

La estructura de grupo en $\mathbb{C}$ que voy a usar es $(\mathbb{C}, +)$, entonces hay que probar que:

$$f(x + y) = f(x) + f(y)$$
$$f(x + y) = z \cdot (x + y) = z \cdot x + z \cdot y = f(x) + f(y)$$

- Podemos ver que f preserva la suma, entonces es un morfismo de grupo.

<u>¿Es inyectiva?</u>

Para que f sea inyectiva, se tiene que dar que si $f(x) = f(y)$, entonces $x = y$.

- Entonces, si $f(x) = f(y)$

$$f(x) = f(y) \to z \cdot x = z \cdot y \to z \cdot (x - y) = 0$$

- Si $z \neq 0$, esto implica que $x - y = 0 \to x = y$.
- Entonces, f es inyectiva si $z \neq 0$.

<u>¿Es sobreyectiva?</u>

Para que f sea sobreyectiva, cada elemento $w \in \mathbb{C}$ existe un $x \in \mathbb{C} : f(x) = w$.

- Sabiendo la definición de f, podemos resolver x en términos de w como:

$$x = \frac{w}{z}$$

- Si $z \neq 0$, la división es válida para cualquier $w \in \mathbb{C}$, lo que implica que f es sobreyectiva.

Demostramos que f es un isomorfismo de grupos (cuando $z \neq 0$).

▼ 9. Probar que hay un isomorfismo entre en grupo de las matrices $2x2$ con la suma habitual de matrices y el grupo de cuaternas reales $\mathbb{R}^4$ con la suma usual

Del enunciado tenemos:

- Conjunto real de las matrices 2×2, de la forma $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, con la suma usual de matrices.
- Conjunto $\mathbb{R}^4$, de la forma (a, b, c, d), con la suma usual.
- Nos pide probar un isomorfismo entre ambos grupos.
  - Debe ser un morfismo de grupos, es decir, $f(a * b) = f(a) * f(b)$.
  - Debe ser inyectivo y sobreyectivo.

Se define la función f como:

$$f(\begin{pmatrix} a & b \\ c & d \end{pmatrix}) = (a, b, c, d)$$

- Toma una matriz cualquiera 2×2 y la mapea a una 4-terna $\mathbb{R}^4$.

¿Es un morfismo de grupos?

Teniendo en cuenta la suma habitual de ambos conjuntos, se debe probar que:

- Siendo $A, B \in M_{2x2}(\mathbb{R})$

$$f(A + B) = f(A) + f(B)$$

- Sean:

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad B = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$$

- La suma entre ambas matrices 2×2 es:

$$A + B = \begin{pmatrix} a + a' & b + b' \\ c + c' & d + d' \end{pmatrix}$$

- La aplicación de f sobre esa suma da como resultado:

$$f(A + B) = (a + a', b + b', c + c', d + d')$$

- Ahora, si se calcula f en cada matriz de manera individual:

$$f(A) + f(B) = (a, b, c, d) + (a', b', c', d') = (a + a', b + b', c + c', d + d')$$

- De esta forma, se puede ver que $f(A + B) = f(A) + f(B)$. Por lo tanto, f es un *morfismo de grupos*.

<u>¿Es inyectiva?</u>

f es inyectiva si $f(A) = f(B)$ entonces $A = B$.

- Supongamos que:

$$f(\begin{pmatrix} a & b \\ c & d \end{pmatrix}) = f(\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix})$$

- Con la aplicación de f esto quedaría como:

$$(a, b, c, d) = (a', b', c', d')$$

- Esto significa que $a = a', b = b', c = c', d = d'$, lo que implica que $A = B$. Por lo tanto, f es inyectiva.

<u>¿Es sobreyectiva?</u>

- Para cualquier $(a, b, c, d) \in \mathbb{R}^4$, existe o se puede encontrar una matriz $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_{2x2}(\mathbb{R})$ tal que $f(\begin{pmatrix} a & b \\ c & d \end{pmatrix}) = (a, b, c, d)$.
- Por lo tanto, f es sobreyectiva ya que todo elemento del codominio es alcanzado por un elemento del dominio.

Al ser un morfismo de grupos, se inyectiva y sobreyectiva, podemos decir que f es un isomorfismo de grupos.

▼ 10. Probar que todo grupo cíclico de orden m es isomorfo a $(\mathbb{Z}_m, +)$

Un grupo cíclico orden m es aquel que posee un elemento g, mediante el cuál podemos representar todos los elementos del grupo como potencias de g

- g^k, siendo $k = \{0, 1, 2, ..., m-1\}$.
- Entonces, $G = \{g, g^2, g^3, ..., g^{m-1}, e\}$.
- El elemento neutro de G, e es igual a g^m.

$(\mathbb{Z}_m, +)$ es el grupo de enteros módulo m con la suma módulo m.

- El grupo es cíclico, ya que el 1 (o cualquier elemento coprimo con m) puede generar todos los elementos del grupo.

Sea la función $f : G \to \mathbb{Z}_m$

$$f(g^k) \equiv_m k$$

- Donde $k = 0, 1, 2, ..., m-1$
- Se debe demostrar que la función es un morfismo de grupos, que es inyectiva y sobreyectiva para decir que es un isomorfismo.

<u>¿Es un morfismo de grupos?</u>

Para que f sea un morfismo de grupos se debe probar que para todo $g^a, g^b \in G$:

$$f(g^a \cdot g^b) \equiv_m f(g^a) + f(g^b)$$

- Teniendo $f(g^a \cdot g^b)$:

$$f(g^a \cdot g^b) \equiv_m f(g^{a+b}) \equiv_m a + b$$

- Y del lado de $f(g^a) + f(g^b)$:

$$f(g^a) + f(g^b) \equiv_m a + b$$

- Podemos ver que $f(g^a \cdot g^b) = f(g^a) + f(g^b)$, entonces se demuestra que f es un morfismo de grupos.

¿Es inyectiva?

Supongamos que $f(g^a) = f(g^b)$

- Entonces, $a \equiv_m b$, lo que implica que $g^a = g^b$ en G.
  - Teniendo en cuenta que G tiene m elementos distintos.
- Por lo tanto, se puede decir que f es inyectiva.

¿Es sobreyectiva?

Para cada elemento $k \in \mathbb{Z}_m$:

- Existe un $g^k \in G$: $f(g^k) \equiv_m k$
- Por lo tanto, se puede decir que f es sobreyectiva.

Al ser f un morfismo de grupos, inyectiva y sobreyectiva, es válido afirmar que es un isomorfismo de grupos.