El grupo de homomorfismos

$Hom(\mathbb{Z}_n, \mathbb{Z}_m)$

Stella Huérfano
Profesora Universidad Nacional de Colombia
Bogotá D.C, Colombia
rshuerfanob@unal.edu.co

Sara Garavito
Estudiante Universidad Nacional de Colombia
Bogotá D.C, Colombia
rshuerfanob@unal.edu.co

Resumen

Se representa el concepto de grupo mediante algunos ejemplos haciendo énfasis en la noción de Grupo Abeliano, Grupo Cíclico, Homomorfismo de grupos e Isomorfismo de grupos. Dados dos grupos Abelianos A y B, definimos el grupo $Hom(A, B)$ (el grupo de homomorfismos entre A y B). Finalmente se calcula $Hom(A, B)$ en el caso particular en el que A y B son $\mathbb{Z}_n$ y $\mathbb{Z}_m$ respectivamente, con n y m enteros positivos.

Definición 1. *(Grupo). Decimos que un par $(G, *)$ formado por un conjunto G y una operación binaria $*$ en G, es decir, una aplicación $* : G \times G \to G$ que satisface los tres axiomas siguientes:*

1. ***Asociatividad**. Para todo a, b y $c \in G$, $(a * b) * c = a(b * c)$.*
2. ***Existencia de elemento neutro**. Existe $e \in G$, tal que para todo $a \in G$, se tiene $a * e = e * a = a$.*
3. ***Existencia de inversos**. Para todo $a \in G$ existe $\tilde{a} \in G$, tal que $a * \tilde{a} = \tilde{a} * a = e$.*

Se dice que el grupo $(G, *)$ es **Conmutativo o Abeliano** si se verifica además el siguiente axioma:

4. **Conmutatividad**. Para todo $a, b \in G$, $a * b = b * a$.

Algunos ejemplos de grupos Abelianos

Los siguientes pares son son ejemplos muy conocidos de grupos abelianos:

i) Los enteros con la suma usual, $(\mathbb{Z}, +)$.

ii) Los racionales con la suma usual, $(\mathbb{Q}, +)$.

iii) Los reales con la suma usual, $(\mathbb{R}, +)$.

iv) Los racionales no nulos con la multiplicación usual, $(\mathbb{Q} - \{0\}, \times)$.

v) Los reales no nulos con la multiplicación usual, $(\mathbb{R} - \{0\}, \times)$.

vi) El conjunto de los enteros múltiplos de m, con la suma usual, $(m\mathbb{Z}, +)$.

vii) El conjunto de las clases residuales módulo n, con la suma módulo n, $(\mathbb{Z}_n, +)$. Casos particulares de éste último ejemplo son: $(\mathbb{Z}_2, +)$ y $(\mathbb{Z}_3, +)$ con la operación "+"definida de la siguiente manera:

$+$	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$

Grupo $\mathbb{Z}_2$

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$

Grupo $\mathbb{Z}_3$

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

Grupo $\mathbb{Z}_4$

Definición 2. *(Grupo Cíclico). Sea G un grupo. Decimos que G es un grupo cíclico si existe un elemento $a \in G$ tal que cada elemento $x \in G$ puede escribirse de la forma a^n para algún entero n. En este caso el elemento a es denominado el generador de G. Si G es cíclico, G se escribe como $G = \langle a \rangle$.*

Ejemplo 1. *Sea $G = \{e, b, c, d\}$ y $(G, *)$ un grupo con la operación $*$ definida de la siguiente manera:*

$*$	e	b	c	d
e	e	b	c	d
b	b	c	d	e
c	c	d	e	b
d	d	e	b	c

Tabla 1: Grupo Abeliano cíclico, generado por el elemento b

$$
\begin{aligned}
b^0 &= e \\
b^1 &= b \\
b^2 &= b * b = c \\
b^3 &= b^2 * b = c * b = d \\
b^4 &= b^3 * b = d * b = e
\end{aligned}
$$

Existen grupos abelianos no cíclicos como los ilustrados en el siguiente ejemplo:

Ejemplo 2. *Sea G es el conjunto mencionado anteriormente, dotado con la operación $\cdot$ definida en la primera tabla a continuación, y sea H el conjunto*
$H = \{(0,0), (0,1), (1,0), (1,1)\} = \mathbb{Z}_2 \times \mathbb{Z}_2$ dotado con la suma $\oplus$, inducida por la suma en $\mathbb{Z}_2$ componente a componente. Entonces $(G, \cdot)$ y $(H, \oplus)$($(H, \oplus)$ denotado ahora como $\mathbb{Z}_2 \oplus \mathbb{Z}_2$)) son grupos.

$\cdot$	e	b	c	d
e	e	b	c	d
b	b	e	d	c
c	c	d	e	b
d	d	c	b	e

Grupo abeliano no cíclico $(G, \cdot)$

$+$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,0)$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,1)$	$(0,1)$	$(0,0)$	$(1,1)$	$(1,0)$
$(1,0)$	$(1,0)$	$(1,1)$	$(0,0)$	$(0,1)$
$(1,1)$	$(1,1)$	$(1,0)$	$(0,1)$	$(0,0)$

Grupo $\mathbb{Z}_2 \oplus \mathbb{Z}_2$

Definición 3. *(Homomorfismo de grupos). Dados dos grupos* $(A, *)$ *y* $(B, \cdot)$ *y una función* $\phi : A \to B$*, decimos que* ϕ *es un homomorfismo de grupos de* A *en* B *si para todo* a_1 *y* $a_2 \in A$ *se tiene que* $\phi(a_1 * a_2) = \phi(a_1) \cdot \phi(a_2)$.

Proposición 1. *Si* $\phi : G \to K$ *es un homomorfismo de grupos, entonces* ϕ *satisface:*

i) $\phi(e_G) = e_K$.

ii) $(\phi(g))^{-1} = \phi(g^{-1})$ *para* $g \in G$.

Demostración.

i) Si $e_G^2 = e_G$ y sea $\phi(e_G) = k$, $k \in K$, entonces

$$\begin{aligned} k^2 &= \phi(e_G)\phi(e_G) \\ k^2 &= \phi(e_G^2) \\ k^2 &= \phi(e_G) \\ k^2 &= k. \end{aligned}$$

Puesto que e_K es el único elemento idempotente de K, se tiene que $k = e_K$.

ii)

$$\begin{aligned} e_K &= \phi(e_G) \\ e_K &= \phi(gg^{-1}) \\ e_K &= \phi(g)\phi(g^{-1}) \end{aligned}$$

Así

$$(\phi(g))^{-1} = \phi(g)^{-1}.$$

Ejemplos de algunos homomorfismos de grupos:

i) La función $\phi : G \to K$ que envía todo G en el elemento neutro de K, es el homomorfismo cero o constante y se escribe $0 : G \to K$.

ii) Si G es un grupo, la función identidad $\phi = I$, $I : G \to G$ es un homomorfismo.

iii) Sea G un grupo. $x \in G$, si $n \in \mathbb{Z}^+$, definimos

$$\underbrace{x \cdot x \cdots x}_{n \text{ veces}} = x^n$$

La función ϕ, $\phi : (\mathbb{Z}, +) \to (G, \cdot)$ es un homomorfismo. Si se tiene $(G, +)$ en vez de $(G, \cdot)$, escribimos nx en lugar de x^n.

iv) La función $\phi = e^x$ es un homomorfismo del grupo de los reales con la suma usual, $(\mathbb{R}, +)$ en el grupo de los reales positivos con la multiplicación usual, $(\mathbb{R}^+, \times)$.

$$e^x : (\mathbb{R}, +) \to (\mathbb{R}^+, \times)$$

$$x + y \to e^{x+y} = e^x e^y$$

Proposición 2. *Si $\phi : G \to K$ y $\psi : K \to L$ son homomorfismos, también lo es la función compuesta $\psi \circ \phi : G \to L$.*

Demostración.
$\psi \circ \phi(g_1 g_2) = \psi(\phi(g_1 g_2)) = \psi(\phi(g_1)\phi(g_2)) = \psi(\phi(g_1))\psi(\phi(g_2))$.

Definición 4. *Un homomorfismo $\phi : A \to B$ es un isomorfismo si y sólo si ϕ es biyectiva, en este caso decimos que A es isomorfo a B lo cual se denota $A \cong B$.*

Obsérvese que el grupo del ejemplo 1 y $\mathbb{Z}_4$ son el "mismo" grupo salvo por los nombres de los elementos. Es decir $G \cong \mathbb{Z}_4$. También podemos decir que $G \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$ (en el ejemplo 2).
La función $\phi = e^x$ del ejemplo *iii* de homomorfismos, es un isomorfismo de los reales con la suma usual, $(\mathbb{R}, +)$ en el grupo de los reales positivos con la multiplicación usual, $(\mathbb{R}^+, \times)$. Es decir, $(\mathbb{R}, +) \cong (\mathbb{R}^+, \times)$.

Definición 5. *(El grupo de Homomorfismos). Dados dos grupos abelianos $(A, *)$ y $(B, \cdot)$, el conjunto de todos los homomorfismos ϕ entre A y B se denota por $Hom(A, B)$.*

$$Hom(A, B) = \{\varphi : A \to B \mid \varphi \text{ es un homomorfismo}\}$$

Si φ, $\psi \in Hom(A, B)$, entonces $(\varphi + \psi)(x) = \varphi(x) \circ \psi(x)$, esto es, la función $\varphi + \psi : A \to B$, es decir, $(\varphi + \psi) \in Hom(A, B)$.

Cuando definimos para $n \in \mathbb{Z}$ y $\varphi \in Hom(A, B)$, la función $(n\varphi) : A \to B$ se expresa

$$\underbrace{\varphi(x) + \varphi(x) + \cdots + \varphi(x)}_{n \text{ veces}} = (n\varphi(x))$$

entonces $Hom(A, B)$ se denota $Hom_{\mathbb{Z}}(A, B)$ y se llama el $\mathbb{Z}-$**módulo** de homomorfismos de A en B.

Ejercicio 1. *Consideremos los posibles homomorfismos de $\mathbb{Z} \to \mathbb{Z}_3$*

$$Hom_{_{\mathbb{Z}}}(\mathbb{Z}, \mathbb{Z}_3) = \{f : \mathbb{Z} \to \mathbb{Z}_3 \mid f \text{ es un homomorfismo}\}$$

$$f : \mathbb{Z} \to \mathbb{Z}_3$$

$$z \to f(z) = \begin{cases} [0]_3 \\ [1]_3 \\ [2]_3 \end{cases}$$

Sabemos que sí

$$f : \mathbb{Z} \to \mathbb{Z}_n$$

$$n \to f(n) = f(\underbrace{1+1+1+\cdots+1}_{n-veces})$$

$$f(n) = \underbrace{f(1)+f(1)+\cdots+f(1)}_{n-veces}$$

$$f(n) = nf(1)$$

$$-n \to f(-n) = -f(n) = -nf(1)$$

$f_0 : \mathbb{Z} \longrightarrow \mathbb{Z}_3$

$0, 1, 2, \vdots, n \longrightarrow f_0(0) = [0]_3$

$f_1 : \mathbb{Z} \longrightarrow \mathbb{Z}_3$

$0 \longrightarrow f_1(0) = [0]_3$
$1 \longrightarrow f_1(1) = [1]_3$
$2 \longrightarrow f_1(2) = [2]_3$
$3, 4, 5$

$f_1(1) = [1]_3$
$f_1(2) = f_1(1+1) = f_1(1) + f_1(1) = 2f_1(1) = 2[1]_3 = [2]_3$
$f_1(3) = 3[1]_3 = [0]_3$
$f_1(4) = 4[1]_3 = [1]_3$

$f_2 : \mathbb{Z} \longrightarrow \mathbb{Z}_3$

$0 \longrightarrow [0]_3$
$1, 3$
$2 \longrightarrow [1]_3$
$4 \longrightarrow [2]_3$

$f_2(1) = [2]_3 = 2\,[1]_3 = 2f_1(1)$
$f_2(2) = f_2(1) + f_2(1) = [2]_3 + [2]_3 = [4]_3 = 4\,[1]_3 = 4f_1(1)$
$f_2(3) = [6]_3 = 6\,[1]_3 = 6f_1(1) = [0]_3$

$Hom_{\mathbb{Z}}(\mathbb{Z},\mathbb{Z}_3) = \{f_0, f_1, f_2\}$ es un grupo abeliano cíclico, $Hom_{\mathbb{Z}}(\mathbb{Z},\mathbb{Z}_3) = \langle f_1 \rangle$

$$Hom_{\mathbb{Z}}(\mathbb{Z},\mathbb{Z}_3) = \{0f_1, 1f_1, 2f_1\} \approxeq \mathbb{Z}_3$$

$+$	f_0	f_1	f_2
f_0	f_0	f_1	f_2
f_1	f_1	f_2	f_0
f_2	f_2	f_0	f_1

Sí continuamos con el procedimiento para $Hom_{\mathbb{Z}}(\mathbb{Z},\mathbb{Z}_n)$, ¿Cuál será el grupo de $Hom_{\mathbb{Z}}(\mathbb{Z},\mathbb{Z}_n)$?. Teniendo en cuenta el ejercicio anterior se puede deducir

$$\begin{aligned} f_{n-1} : \mathbb{Z} &\longrightarrow \mathbb{Z}_n \\ 1 &\longrightarrow f_{n-1}(1) = (n-1)f_1 \\ &\vdots \\ n &\longrightarrow f_{n-1}(1) = (n-1)nf_1 = [0]_n \end{aligned}$$

$$Hom_{\mathbb{Z}}(\mathbb{Z},\mathbb{Z}_n) = \{0, 1f_1, 2f_1, 3f_1, \cdots, (n-1)f_1\} = \langle f_1 \rangle \approxeq \mathbb{Z}_n$$

Así $Hom_{\mathbb{Z}}(\mathbb{Z},\mathbb{Z}_n)$ es un grupo abeliano cíclico de n elementos generado por f_1.

Ejemplo 3. *Ahora consideremos los posibles homomorfismos de $\mathbb{Z}_m$ en $\mathbb{Z}$, $Hom_{\mathbb{Z}}(\mathbb{Z}_m,\mathbb{Z})$.*

$$\begin{aligned} f_0 : \mathbb{Z}_3 &\longrightarrow \mathbb{Z} \\ x &\longrightarrow f_0([x]) = 0 \end{aligned}$$

$$\begin{aligned} f_1 : \mathbb{Z}_3 &\to \mathbb{Z} \\ [0]_3 &\longrightarrow 0 \\ [1]_3 &\longrightarrow 1 \\ [2]_3 &\longrightarrow 2 \\ [3]_3 &\longrightarrow 3 \end{aligned}$$

$$f_1([2]_3) = f_1([1]_3 + [1]_3) = f_1([1]_3) + f_1([1]_3) = 2$$
$$f_1([3]_3) = f_1([0]_3)$$

$3 = 0$ *Lo cual es una contradicción !!*

Luego no es posible que $f_1([1]) = 1$

Supongamos que $f_1([1]_n) = k, k \in \mathbb{Z}$

$$\begin{aligned} f_1 : \mathbb{Z}_n &\to \mathbb{Z} \\ [1]_n &\to f_1([1]_n) = k \end{aligned}$$

$$
\begin{array}{c}
n[1]_n = [n]_n = [0]_n \text{ , luego} \\
[n]_n \longrightarrow f_1([n]_n) = f_1(n[1]_n) = nf_1([1]_n) \\
\shortparallel \\
[0] \longrightarrow f_1([0]_n) = 0 = nf_1([1]_n), \textit{donde} \\
0 = nk. \quad \text{Pero esto se tiene sí y solo sí } k = 0.
\end{array}
$$

Luego para cualquier homomorfismo $f : \mathbb{Z}_n \to \mathbb{Z}$,

$$f([m]_n) = 0, \text{ con } m \neq 0, \text{ entonces}$$

$$f(m[1]_n) = mf([1]_n) = 0$$

$$\text{por tanto, } f([1]_n) = 0.$$

$$\text{De esta manera, } Hom_{\mathbb{Z}}(\mathbb{Z}_m, \mathbb{Z}) \cong \{0\}$$

Proposición 3. *Dados $m, n \in \mathbb{N}$, entonces*

$$Hom_{\mathbb{Z}}(\mathbb{Z}_n, \mathbb{Z}_m) = \{f_{0d}, f_{1d}, f_{2d}, \cdots, f_{(k-1)d}\}$$

donde $k = m.c.d(m, n)$ y $d = \frac{m}{k}$. Es decir los homomorfismos que pertenecen a $Hom_{\mathbb{Z}}(\mathbb{Z}_n, \mathbb{Z}_m)$ se pueden expresar como:

$$
\begin{array}{rcl}
f_r : \mathbb{Z}_n & \longrightarrow & \mathbb{Z}_m \\
[1]_n & \longrightarrow & f_r([1]_n) = [r]_m, \textit{donde} \\
\multicolumn{3}{c}{r = pd,\ p = 0, 1, 2, \cdots, k-1.}
\end{array}
$$

Prueba: vamos a probar que $f_r([1]_n) = [r]_m$

$$
\begin{array}{c}
f_r([0]_n) = f_r([n]_n) \\
f_r([0]_n) = f_r([nr]_n) \\
f_r([0]_n) = [0]_m
\end{array}
$$

Esta última igualdad se tiene sí $nr = tm, \quad n(pd) = tm$.

En este caso, es claro que nr es un múltiplo de n y también nr es múltiplo de m. Es decir, existe algún $p, \quad 0 \preceq p \preceq k-1$,
tal que

$$nr = p(m.c.m(m, n))$$

sabemos que,

$$m.c.m(m, n) = \frac{mn}{m.c.d(m, n)}$$

reemplazando la última ecuación en la primera ecuación tenemos que

$$nr = p\,\frac{mn}{m.c.d(m, n)}$$

Luego $nr = p\frac{mn}{k}$ sí y sólo sí $r = p(\frac{m}{k})$ luego $r = pd$, por lo tanto,

$f_r([1]_n) = [pd]_m$, $0 \preceq p \preceq k-1$, $k = m.c.d(m,n)$

Así $f_r([1]_n) = [r]_m$ □

Veamos que f_r es homomorfismo, recordemos que $d = \frac{m}{k}$, $k = m.c.d(m,n)$ y $r = pd$.
$f_r([1]_n) = [r]_m$
$f_{pd}([1]_n) = [pd]_m$
$f_r([0]_n) = f_{pd}([0]_n) = f_{pd}([n]_n) = [npd]_m = [npd]_m = [np\frac{m}{k}]_m$ como $k|n$, $p\frac{k}{n} \in \mathbb{Z}$, sea $k_1 = p\frac{k}{n}$
$f_r([0]_n) = [k_1 m]_m$
$f_{pd}([0]_n) = [0]_m$, por lo tanto, f_{pd} es un homomorfismo bien definido
Luego,

$$Hom_{\mathbb{Z}}(\mathbb{Z}_n, \mathbb{Z}_m) = \{f_{0d}, f_{1d}, f_{2d}, \cdots, f_{(n-1)d}\} \approx \mathbb{Z}_k$$

Veamos que sí $Hom_{\mathbb{Z}}(\mathbb{Z}_n, \mathbb{Z}_m)$ es isomorfo a $\mathbb{Z}_k$, $k = m.c.m(m,n)$ entonces,

$Hom_{\mathbb{Z}}(\mathbb{Z}_n, \mathbb{Z}_m)$ es generado por f_d, pues $f_p([1]_n) = [pd]_m$ por definición, luego $f_d([1]_n) = [d]_m$.

Sea $[x] \in \mathbb{Z}_n$, entonces

$$\begin{aligned} f_d([x]_n) &= x f_d([1]_n) \\ &= x[pd]_m \\ &= px[d]_m \\ &= px f_d([1]_n) \\ &= p f_d([x]_n) \end{aligned}$$

Se ha mostrado que $f_{pd} = p f_d$
Luego f_d es el generador de $Hom_{\mathbb{Z}}(\mathbb{Z}_n, \mathbb{Z}_m)$

$$Hom_{\mathbb{Z}}(\mathbb{Z}_n, \mathbb{Z}_m) = \{f_{0d}, f_{1d}, f_{2d}, \cdots, f_{(n-1)d}\} = \langle f_d \rangle$$

Así $Hom_{\mathbb{Z}}(\mathbb{Z}_n, \mathbb{Z}_m)$ es un grupo cíclico de k elementos, por tanto isomorfo a $\mathbb{Z}_k$.
$Hom_{\mathbb{Z}}(\mathbb{Z}_n, \mathbb{Z}_m) \approx \mathbb{Z}_k$.

Bibliografía

[1] HILTON, P., *A course in Homological Algebra*, Springer-Verlag, Nex York, 1971.

[2] HILTON, P., *Curso de álgebre moderna*, Reverté, Barcelona, 1982.

[5] HERSTEIN I., *Álgebra Moderna*, Trillas, México. 1994.

[3] LANG, S., *Álgebra*, Addison-Wesley Publishing Company, Amsterdan, 1965.

[4] LANG, S., *Undergraduate Algebra*. Springer-Verlag, Nex York, 1987.