Homomorfismos de anillos

Facultad de Ciencias UNAM

Introducción

En esta sección introducimos el concepto de homomorfismos de anillos. Obviamente, los homomorfismos de anillos juegan el mismo rol en la teoría de anillos que los homomorfismos de grupos en la teoría de grupos. Por ejemplo, son funciones que preservan la estructura de anillos y a través de ellos definimos nuestro concepto de "anillos equivalentes" o mas precisamente "anillos isomorfos".

Homomorfismos de anillos

Definición

- Supongamos que $(R, +, \times)$ y $(R', +', \times')$ son anillos. Una función $\varphi : R \to R'$ es un **homomorfismo de anillos** si para toda $x, y \in R$
  - $\varphi(x + y) = \varphi(x) +' \varphi(y)$
  - $\varphi(x \times y) = \varphi(x) \times' \varphi(y)$
- El **kernel** de un homomorfismo de anillos $\varphi : R \to R'$ es el subconjunto de R

$$\ker \varphi := \left\{ x \in R \mid \varphi(x) = 0_{R'} \right\} = \varphi^{-1}\left(\{0_{R'}\} \right)$$

- Un **isomorfismo de anillos** es un homomorfismo de anillos biyectivo. Si $\varphi : R \to R'$ es un isomorfismo de anillos, decimos que R y R' son **anillos isomorfos** y escribimos $R \cong R'$.

Observación

Como un anillo tiene dos operaciones, es natural que pidamos que un homomorfismo de anillos preserve ambas operaciones. Mas aun, como los isomorfismos son biyecciones, dos anillos son isomorfos si en lo único en lo que difieren es en el nombre de sus elementos y en el nombre de sus operaciones. Como todas las propiedades que estudiaremos en teoría de anillos están definidas a partir de estas propiedades, de verdad podremos decir que el concepto de isomorfismo es un concepto de equivalencia adecuado.

También notemos que la condición $\varphi(x+y) = \varphi(x) +' \varphi(y)$ nos dice que φ es un homomorfismo entre los grupos abelianos $(R, +)$ y $(R, +')$. Por lo tanto, en lo que sigue podemos invocar (y esperar) resultados a partir de este hecho. Por ejemplo, la siguiente proposición.

Los homomorfismos de anillos respetan neutros e inversos aditivos

Proposición 1

Si $\varphi : R \to R'$ es un homomorfismo de anillos, entonces

1. $\varphi(0_R) = 0_{R'}$.
2. $\varphi(-x) = -\varphi(x)$ para toda $x \in R$.

Demostración.

1. $\varphi(0_R) + \varphi(0_R) = \varphi(0_R + 0_R) = \varphi(0_R)$. Por lo tanto, sumando $-\varphi(0_R)$ en ambos lados de la ecuación, obtenemos $\varphi(0_R) = 0_{R'}$.
2. $\varphi(x) + \varphi(-x) = \varphi(x - x) = \varphi(0_R) = 0_R$. Por lo tanto, $\varphi(x)$ es el inverso aditivo de $\varphi(-x)$. En otras palabras, $\varphi(-x) = -\varphi(x)$.

□

Homomorfismos e imágenes directas

Proposición 2

Si $\varphi : R \to R'$ es un homomorfismo de anillos, entonces

1. $\varphi(R)$ es un subanillo de R'.
2. Si φ es inyectiva, entonces R y $\varphi(R)$ son isomorfos.

Demostración.

1. Sea $x, y \in \varphi(R)$, entonces existen $a, b \in R$ tales que $x = \varphi(a)$ y $y = \varphi(b)$. Entonces, como R es anillo, $a - b \in R$ y $a \times b \in R$. Por lo tanto,

$$x - y = \varphi(a) - \varphi(b) = \varphi(a - b) \in \varphi(R)$$
$$x \times y = \varphi(a) \times \varphi(b) = \varphi(a \times b) \in \varphi(R)$$

2. Si φ es inyectiva, entonces la restricción $\varphi : R \to \varphi(R)$ es una biyección y por lo tanto, es un isomorfismo.

□

φ es inyectivo si y solo si $\ker \varphi = 0$

Proposición 3

Si $\varphi : R \to R'$ es un homomorfismo de anillos, entonces

$$\varphi \text{ es inyectivo } \iff \ker \varphi = 0.$$

Demostración.

$\Longrightarrow$) Supongamos que $a \in \ker \varphi$. Entonces $\varphi(a) = 0_{R'} = \varphi(0_R)$. Pero como φ es inyectiva, entonces $a = 0$. Por lo tanto, $\ker \varphi = 0$.

$\Longleftarrow$) Supongamos que $a, b \in R$ son tales que $\varphi(a) = \varphi(b)$. Entonces $\varphi(a - b) = \varphi(a) - \varphi(b) = 0_{R'}$. Pero como $\ker \varphi = 0$, entonces $a - b = 0$. Por lo tanto, $a = b$.

$\square$

Una propiedad importante del kernel de un homomorfismo de anillos

Proposición 4

Si $\varphi : R \to R'$ es un homomorfismo de anillos, entonces

- $\ker \varphi$ es un subanillo de R.
- Si $\alpha \in \ker \varphi$ y $r \in R$, entonces $\alpha \times r, r \times \alpha \in \ker \varphi$.

Demostración. Sean $a, b, \alpha \in \ker \varphi$ y $r \in R$. Entonces

$$\varphi(a - b) = \varphi(a) - \varphi(b) = 0_{R'} - 0_{R'} = 0_{R'}$$
$$\varphi(\alpha \times r) = \varphi(\alpha) \times \varphi(r) = 0_{R'} \times \varphi(r) = 0_{R'}$$

Análogamente, $\varphi(r \times \alpha) = 0_{R'}$. En otras palabras, $a - b \in \varphi$ y $\alpha \times r, r \times \alpha \in \ker \varphi$. □

Homomorfismos de anillos que respetan la unidad

Proposición 5

Supongamos que R, R' son anillos con unidad y que $\varphi : R \to R'$ es un homomorfismo de anillos. Si $\varphi(1_R) = 1_{R'}$, y $x \in R$ es invertible, entonces

$$\varphi(x^{-1}) = \varphi(x)^{-1}.$$

En particular, $x \in R$ invertible implica $\varphi(x) \neq 0$.

Demostración. Para toda $x \in R$ invertible tenemos

$$\varphi(x) \cdot \varphi(x^{-1}) = \varphi(x \cdot x^{-1}) = \varphi(1_R) = 1_{R'}.$$

Análogamente, $\varphi(x^{-1}) \cdot \varphi(x) = 1_{R'}$ y por lo tanto, $\varphi(x^{-1}) = \varphi(x)^{-1}$. $\square$

Homomorfismos de anillos que no respetan la unidad

Proposición 6

Supongamos que R, R' son anillos con unidad y que $\varphi : R \to R'$ es un homomorfismo de anillos. Si $\varphi(1_R) \neq 1_{R'}$, entonces $\varphi(1_R)$ es un divisor de 0.

En particular, si R' es un dominio entero, entonces todo homomorfismo de R (un anillo con unidad) en R' respeta la unidad.

Demostración. Como $\varphi(1_R) \neq 1_R$, entonces $\varphi(1_R) - 1_R \neq 0$ y por lo tanto, las siguientes igualdades demuestran que $\varphi(1_R)$ es un divisor de 0.

$$\begin{aligned}\varphi(1_R) \cdot (\varphi(1_R) - 1_{R'}) &= \varphi(1_R) \cdot \varphi(1_R) - \varphi(1_R) \\ &= \varphi(1_R \cdot 1_R) - \varphi(1_R) = \varphi(1_R) - \varphi(1_R) = 0_{R'}.\end{aligned}$$

□

Dos homomorfismos suprayectivos

- Supongamos que $n \in \mathbb{Z}_{\geq 2}$. La proyección canónica $\pi : \mathbb{Z} \to \mathbb{Z}_n$, $k \mapsto [k]_n$ es un homomorfismo de anillos: para toda $k, l \in \mathbb{Z}$ y $\bullet = +, \times$

$$\pi\left(k \bullet_{\mathbb{Z}} l\right) = [k \bullet_{\mathbb{Z}} l]_n = [k]_n \bullet_{\mathbb{Z}_n} [l]_n = \pi(k) \bullet_{\mathbb{Z}_n} \pi(l)$$

- Supongamos que A es un anillo y X es un conjunto no vacío. Para toda $c \in X$, sea $E_c : A^X \to A$ tal que $E_c(f) = f(c)$ para toda $f \in A^X$. Veamos que E_c es un homomorfismo de anillos: para toda $f, g \in A^X$ y $\bullet = +, \times$

$$E_c(f \bullet_{A^X} g) = (f \bullet_{A^X} g)(c) = f(c) \bullet_A g(c) = E_c(f) \bullet_A E_c(g)$$

□

Dos homomorfismos inyectivos

- Supongamos que R es un anillo y S es un subanillo de R. La inclusión $S \hookrightarrow R$ es un homomorfismo inyectivo.
- Sea $\iota : \mathbb{Z}_2 \to \mathbb{Z}_6$ tal que $[0]_2 \overset{\iota}{\mapsto} [0]_6$ y $[1]_2 \overset{\iota}{\mapsto} [3]_6$. Veamos que ι es un homomorfismo de anillos. Claramente, si alguna de las ecuaciones que queremos verificar involucra a $[0]_2$, entonces esta se satisface trivialmente. Por lo tanto, basta verificar las siguientes ecuaciones.

$$\iota\left([1]_2 + [1]_2\right) = \iota\left([0]_2\right) = [0]_6 = [6]_6 = [3+3]_6 = [3]_6 + [3]_6 = \iota([1]_2) + \iota([1]_2)$$

y

$$\iota\left([1]_2 \times [1]_2\right) = \iota\left([1]_2\right) = [3]_6 = [9]_6 = [3\times 3]_6 = [3]_6 \times [3]_6 = \iota\left([1]_2\right) \times \iota\left([1]_2\right)$$

En particular, acabamos de demostrar que los homomorfismos de anillos *no* necesariamente mandan unidades en unidades. Sin embargo, como uno esperaría, los isomorfismos *si* respetan unidades.

$\mathbb{C}$ esta contenido en $\mathbb{H}$ y en $M_2(\mathbb{R})$

- Claramente, $\mathbb{R} + i\mathbb{R} \subset \mathbb{H}$ y $\mathbb{C}$ son isomorfos.
- Sea $R := \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a, b \in \mathbb{R} \right\} \subset M_2(\mathbb{R})$ y $\varphi : R \to \mathbb{C}$ tal que

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \overset{\varphi}{\mapsto} a + ib.$$

Es fácil verificar que φ es inyectiva, suprayectiva, y que respeta la suma. Veamos que respeta la multiplicación.

$$\varphi\left(\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \cdot \begin{pmatrix} c & d \\ -d & c \end{pmatrix}\right) = \varphi\left(\begin{pmatrix} ac - bd & ad + bc \\ -bc - ad & -bd + ac \end{pmatrix}\right) =$$

$$(ac - bd) + i\,(ad + bc) = (a + ib) \cdot (c + id) =$$

$$\varphi\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \cdot \varphi\begin{pmatrix} c & d \\ -d & c \end{pmatrix}$$

Un homomorfismo de grupos abelianos que no es homomorfismo de anillos

Supongamos que $n \in \mathbb{Z} \setminus \{0, 1\}$ definimos $\varphi : \mathbb{Z} \to \mathbb{Z}$ por $k \mapsto nk$. Entonces, para toda $x, y \in \mathbb{Z}$

$$\varphi(x + y) = n(x + y) = nx + ny = \varphi(x) + \varphi(y)$$

pero

$$\varphi(xy) = n(xy) \neq n^2(xy) = (nx)(ny) = \varphi(x)\varphi(y)$$

Análogamente, si $\lambda \in \mathbb{R} \setminus \{0, 1\}$, entonces $\phi : \mathbb{R} \to \mathbb{R}$ dada por $t \mapsto \lambda t$ no es homomorfismo de anillos, *pero* sí es lineal (en el sentido usual de álgebra lineal).

Homomorfismos entre campos que respetan unidades

Lema 7

Supongamos que F y F' son campos. Si $\varphi : F \to F'$ es un homomorfismo de anillos tal que $\varphi(1_F) = 1_{F'}$, entonces φ es inyectiva.

Demostración. Veamos que $\ker \varphi = 0$.

$$\begin{aligned} x \in \ker \varphi &\iff \varphi(x) = 0 \\ &\implies x \text{ no es invertible} && \text{(por la proposición 5)} \\ &\iff x = 0 && \text{(pues } F \text{ es campo)} \end{aligned}$$

Como un homomorfismo de anillos es inyectivo si y solo si su kernel es trivial, lo anterior implica lo deseado. □

Los homomorfismos $X \to X$ con X un sistema numérico

Proposición 8

En lo que sigue, "homomorfismo" significa "homomorfismo de anillos".

1. Si $\varphi : \mathbb{Z} \to \mathbb{Z}$ es un homomorfismo no trivial, entonces $\varphi = \mathrm{id}_{\mathbb{Z}}$.
2. Si $\varphi : \mathbb{Q} \to \mathbb{Q}$ es un homomorfismo no trivial, entonces $\varphi = \mathrm{id}_{\mathbb{Q}}$.
3. Si $\varphi : \mathbb{R} \to \mathbb{R}$ es un homomorfismo no trivial, entonces $\varphi = \mathrm{id}_{\mathbb{R}}$.
4. Existe un isomorfismo $\mathbb{C} \to \mathbb{C}$ distinto a la identidad.

Demostración.

1. Primero nota que, $\varphi(1) = \varphi(1 \cdot 1) = \varphi(1) \cdot \varphi(1) = \varphi(1)^2$ y por lo tanto, $\varphi(1) \in \{0, 1\}$.

   Pero $\varphi(1) \neq 0$ porque de lo contrario, $\varphi(k) = \varphi(k \cdot 1) = \varphi(k) \cdot \varphi(1) = 0$ para toda $k \in \mathbb{Z}$. Contradiciendo φ no nulo.

   Por lo tanto, $\varphi(1) = 1$. De donde, $\varphi(2) = \varphi(1) + \varphi(1) = 1 + 1 = 2$ y por inducción $\varphi(n) = n$ para toda $n \in \mathbb{N}$.

   Finalmente, usando que $\varphi(-n) = -\varphi(n)$ (c.f. proposición 1), obtenemos lo deseado.

2. Supongamos que $m, n \in \mathbb{Z} \setminus \{0\}$. Entonces,

$$\varphi\left(\frac{m}{n}\right) = \varphi(m) \cdot \varphi\left(\frac{1}{n}\right) = \varphi(m) \cdot \frac{1}{\varphi(n)} = \frac{m}{n}$$

Donde la segunda igualdad se cumple por la proposición 5, y la ultima igualdad se cumple por el inciso anterior.

3. Antes que nada, notemos que como $\varphi(1) = 1$ y $\mathbb{R}$ es campo, entonces el lema 2 implica que φ es inyectiva. En particular, para toda $y \in \mathbb{R}$

$$y \neq 0 \implies \varphi(y) \neq 0 \implies \varphi(y)^2 > 0.$$

Usando esto, veamos que φ es creciente. Sean $x, x' \in \mathbb{R}$.

$$x < x' \implies 0 < x' - x \implies \exists y \in \mathbb{R} \setminus \{0\} \left(y^2 = x' - x\right) \implies$$
$$0 < \varphi(y)^2 = \varphi(y^2) = \varphi(x' - x) = \varphi(x') - \varphi(x) \implies \varphi(x) < \varphi(x').$$

Ahora si, veamos que $\varphi(x) = x$ para toda $x \in \mathbb{R}$. Supongamos que $x \in \mathbb{R}$. Sabemos que existen sucesiones $(r_n)_{n\in\mathbb{N}}, (s_n)_{n\in\mathbb{N}} \subset \mathbb{Q}$ tales que (1) $\lim_{n\to\infty} r_n = x$, (2) $\lim_{n\to\infty} s_n = x$, y (3) $r_n < x < s_n$ para toda $n \in \mathbb{N}$. En particular, como φ es creciente

$$\varphi(r_n) < \varphi(x) < \varphi(s_n)$$

Por el inciso anterior, esto implica

$$r_n < \varphi(x) < s_n$$

Tomando el limite cuando $n \to \infty$,

$$x = \lim_{n\to\infty} r_n \leq \varphi(x) \leq \lim_{n\to\infty} s_n = x$$

En particular, $\varphi(x) = x$ para toda $x \in \mathbb{R}$.

4. Sea $f : \mathbb{C} \to \mathbb{C}$ tal que $f(a+ib) = a - ib$. Claramente es una biyección porque $f \circ f = \mathrm{id}_{\mathbb{C}}$ y es homomorfismo de anillos porque

$$\begin{aligned} f\big((a+ib)+(c+id)\big) &= f\big((a+c)+i(b+d)\big) \\ &= (a+c) - i(b+d) \\ &= (a-ib)+(c-id) \\ &= f(a+ib)+f(c+id) \end{aligned}$$

y

$$\begin{aligned} f\big((a+ib)\cdot(c+id)\big) &= f\big((ac-bd)+i(ad+bc)\big) \\ &= (ac-bd) - i(ad+bc) \\ &= (a-ib)\cdot(c-id) \\ &= f(a+ib)\cdot f(c+id) \end{aligned}$$

Un ejemplo de anillos *no* isomorfos

Proposición 9

Los anillos $2\mathbb{Z}$ y $3\mathbb{Z}$ no son isomorfos.

Demostración. Procedamos por contradicción. Es decir, supongamos que existe un isomorfismo $\varphi : 2\mathbb{Z} \to 3\mathbb{Z}$. Entonces, $\varphi(2) = 3k$ para alguna $k \in \mathbb{Z}$ distinta de cero[1]. Usando que φ es homomorfismo obtenemos

$$\varphi(4) = \varphi(2) + \varphi(2) = 3k + 3k = 6k$$
$$\varphi(4) = \varphi(2) \times \varphi(2) = 3k \times 3k = 9k^2$$

En particular, $6k = 9k^2$. De donde, $6 = 9k$. Pero no existe $k \in \mathbb{Z}$ que satisfaga esta ecuación. Una contradicción. □

[1] La razón por la que $k \neq 0$ es que el kernel de un isomorfismo es trivial y por lo tanto, $2 \notin \ker \varphi$.

Una aplicación a teoría de números

Proposición 10

La ecuación $x^2 + y^2 = 3z^2$ no tiene soluciones no triviales en $\mathbb{Z}$.

Demostración. Supongamos que $x, y, z \in \mathbb{Z}$ son tales que $x^2 + y^2 = 3z^2$. Sin perdida de generalidad podemos asumir que x, y, z no tienen factores comunes[2]. Veamos que $x = y = z = 0$. Como para toda $n \in \mathbb{Z}$ la proyección canónica $\pi_n : \mathbb{Z} \to \mathbb{Z}_n$ es un homomorfismo, en particular para $n = 4$ tenemos

$$\pi_4(x)^2 + \pi_4(y)^2 = \pi_4\left(x^2 + y^2\right) = \pi_4\left(3z^2\right) = 3 \cdot \pi_4(z)^2 \tag{1}$$

Por otro lado, veamos que si $w \in \mathbb{Z}_n$, entonces $w^2 \in \{[0]_4, [1]_4\}$.

$$[0]_4^2 = [0]_4, \;\; [1]_4^2 = [1]_4, \;\; [2]_4^2 = [4]_4 = [0]_4, \;\; [3]_4^2 = [9]_4 = [1]_4 \tag{2}$$

[2] De lo contrario podemos dividir esta ecuación por el cuadrado de este factor común hasta obtener lo deseado.

Usando (1) y (2) es fácil verificar (por prueba y error) que $\pi_4(x) = \pi_4(y) = \pi_4(z) = [0]_4$ contradiciendo la suposición de que x, y, z no tienen factores en común. $\square$

Acabamos de dar un ejemplo particular de la siguiente (obviamente cierta) observacion: la falta de soluciones no triviales en un $\mathbb{Z}_n$ (con $n \in \mathbb{Z}_{\geq 2}$ fijo) implica la falta de soluciones en $\mathbb{Z}$. Sin embargo, el converso no es cierto. Un ejemplo sencillo (pero extremadamente difícil de verificar) de una ecuación con soluciones en cada $\mathbb{Z}_n$ pero *sin* soluciones en $\mathbb{Z}$ es

$$3x^3 + 4y^3 + 5y^3 = 0$$