HOMOMORFISMOS DE ANILLOS

Let R, R' be rings. By a **ring-homomorphism** $f: R \to R'$, we shall mean a mapping having the following properties: For all $x, y \in R$,

$$f(x+y) = f(x) + f(y), \qquad f(xy) = f(x)f(y), \qquad f(e) = e'$$

(if e, e' are the unit elements of R and R' respectively).

By the **kernel** of a ring-homomorphism $f: R \to R'$, we shall mean its kernel viewed as a homomorphism of additive groups, i.e. it is the set of all elements $x \in R$ such that $f(x) = 0$. [redacted]

$f: R \mapsto R'$ homomorfismo:

1) $f(x+y) = f(x) + f(y)$

2) $f(xy) = f(x)f(y)$

3) $f(1) = 1$

<u>Proposición</u> $\ker f = \{x \in R \,/\, f(x) = 0\}$ es un ideal

<u>Dem.</u>

1) $x, y \in \ker f \Rightarrow \begin{cases} f(x) = 0 \\ f(y) = 0 \end{cases} \Rightarrow f(x+y) = f(x) + f(y) = 0 \Rightarrow x+y \in \ker f$

2) $a \in R, x \in \ker f \Rightarrow f(ax) = f(a)f(x) = f(a) \cdot 0 = 0 \Rightarrow ax \in \ker f$

3) $f(0) = f(0+0) = f(0) + f(0) \Rightarrow f(0) = 0 \Rightarrow 0 \in \ker f$.

<u>Observación</u>: Como siempre, $f: R \mapsto R'$ es injectiva $\Leftrightarrow \ker f = \{0\}$ (Al fin y al cabo un homomorfismo de anillos es, en particular, un homomorfismo de grupos).

UN EJEMPLO IMPORTANTE

$$ev_\alpha : \mathbb{Q}[X] \longmapsto \mathbb{C} \qquad (\alpha \in \mathbb{C})$$

$$p(x) = \sum_{i=0}^{n} a_i x^i \longmapsto p(\alpha) = \sum_{i=0}^{n} a_i \alpha^i$$

<u>Comprobación</u>:

a) $ev_\alpha(1)=1$

b) $ev_\alpha(p(x)+q(x)) = ev_\alpha\left(\underbrace{\sum a_i x^i}_{p(x)} + \underbrace{\sum b_i x^i}_{q(x)}\right) =$

$= ev_\alpha\left(\sum (a_i+b_i) x^i\right) = \sum (a_i+b_i)\alpha^i = \sum a_i\alpha^i + \sum b_i \alpha_i$

$= ev_\alpha(p(x)) + ev_\alpha(q(x))$

c) $ev_\alpha(p(x)\cdot q(x)) = ev_\alpha\left(\left(\sum a_i x^i\right)\left(\sum b_j x^j\right)\right) =$

$= ev_\alpha\left(\sum_{i,j} a_i b_j x^{i+j}\right) = \sum a_i b_j \alpha^{i+j} = \left(\sum a_i \alpha^i\right)\left(\sum b_j \alpha^j\right)$

$= ev_\alpha(p(\alpha))\cdot ev_\alpha(q(\alpha))$

La misma demostración prueba el siguiente resultado más general:

- Sea A un subanillo de un anillo conmutativo L y sea $\alpha \in L$. Entonces existe un único homonomorfismo de anillos $ev_\alpha : A[X] \longmapsto L$ caracterizado por $\begin{cases} a \longmapsto a, \text{ si } a \in A \\ x \longmapsto \alpha \end{cases}$ (Prop. Univ) definido (necesariamente) por la fórmula

$$\boxed{ev_\alpha\left(\sum a_i x^i\right) = \sum a_i \alpha^i}$$

Pregunta: ¿Quién es el núcleo del homomorfismo $ev_{\sqrt{5}}$: $\mathbb{Q}[X] \longrightarrow \mathbb{R}$?

$$X \longmapsto \sqrt{5}$$

$$p(X) \longmapsto p(\sqrt{5})$$

$X-\sqrt{5} \in \operatorname{Ker} f$? pero $X-\sqrt{5} \notin \mathbb{Q}[X]$

Sabemos que $\operatorname{Ker} f = (q(x))$ donde $q(x)$ es un polinomio no nulo de grado mínimo en $\operatorname{Ker} f$.

Podemos tomar $q(x) = x^2-5 \in \mathbb{Q}[X]$.

Claramente $q(x) \in \operatorname{Ker} f$, pues $q(\sqrt{5}) = 0$.

Pero, ¿podría haber otro polinomio $p(x) \in \operatorname{Ker} f$ de grado < 2?

NO: Si $\underset{\neq 0}{p(X)} = a + bX \in \mathbb{Q}[X]$, $p(\sqrt{5}) = a + b\sqrt{5} \neq 0$, pues $\sqrt{5} \notin \mathbb{Q}$.

Luego $\operatorname{Ker} f = (x^2-5)$

$(a+b\sqrt{5}=0 \Rightarrow \sqrt{5} = -\frac{a}{b} \in \mathbb{Q})$

OJO: $\mathbb{R}[X] \xrightarrow{\varphi} \mathbb{R}$

$p(X) \longmapsto p(\sqrt{5})$

$\operatorname{Ker} \varphi = (X-\sqrt{5})$

También en este contexto tenemos un teorema de isomorfía, claro:

Teorema: Sea $f: A \longmapsto B$ hom. de anillos

Entonces la aplicación:

$$\bar{f}: A/\operatorname{Ker} f \longrightarrow \operatorname{Im} f \subset B$$
$$\bar{a} \longmapsto f(a)$$

es un isomorfismo de anillos (i.e. un homomomomorfismo biyectivo) de modo que $\bar{f}^{-1}$ es también homomorf.

Demostración: Ya sabemos que

$$\bar{f}: A/_{\operatorname{Ker} f} \longmapsto \operatorname{Im} f = f(A)$$

es una aplicación bien definida y de hecho un homomorfismo de grupos. Luego sólo falta ver que $\bar{f}(\bar{a}\cdot\bar{b}) = \bar{f}(\bar{a})\bar{f}(\bar{b})$.

Bien, $\bar{f}(\bar{a}\cdot\bar{b}) = \bar{f}(\overline{ab}) = f(ab) = f(a)f(b) = \bar{f}(\bar{a})\bar{f}(\bar{b})$

- $\bar{f}(\bar{1}) = f(1) = 1$

c.q.d.

<u>Pregunta</u>: ¿Qué nos dice esto sobre el ejemplo anterior $f: \mathbb{Q}[X] \longrightarrow \mathbb{R}$?

$$X \longmapsto \sqrt{5}$$
$$p(X) \longmapsto p(\sqrt{5})$$

Nos dice que: $\dfrac{\mathbb{Q}[X]}{(X^2-5)} \simeq \operatorname{Im} f \subseteq \mathbb{R}$

max.

$$X + (X^2-5) \longleftrightarrow \sqrt{5}$$
$$3/2 \longleftrightarrow 3/2$$

donde $\operatorname{Im} f = \{\underbrace{a_0 + a_1\sqrt{5} + a_2(\sqrt{5})^2 + a_3(\sqrt{5})^3 + \dots + a_n(\sqrt{5})^n}_{p(\sqrt{5})} / a_i \in \mathbb{Q}\}$

¿es un cuerpo?

$\frac{1}{\sqrt{5}} = \frac{\sqrt{5}}{5}$ $\mathbb{Q}[\sqrt{5}]$

$= \{a + b\sqrt{5} / a, b \in \mathbb{Q}\} = \mathbb{Q}[\sqrt{5}] = \mathbb{Q}(\sqrt{5})$

Sí es un cuerpo porque es isom a $\dfrac{\mathbb{Q}[X]}{(X^2-5)}$ ← maximal: $\dfrac{1}{a+b\sqrt{5}} = \dfrac{a-b\sqrt{5}}{a^2-5b^2} = \dfrac{a}{a^2-5b^2} + \dfrac{-b}{a^2-5b^2}\cdot\sqrt{5}$

• ¿Y qué dice el T. de isomorfía sobre el homomorfismo $\varphi: \mathbb{R}[X] \longrightarrow \mathbb{C}$?

$$X \longmapsto i$$
$$p(X) \longmapsto p(i)$$

Pues, razonando como antes, vemos que

$$\operatorname{Ker} \varphi = (X^2+1) \Rightarrow$$

$$\frac{\mathbb{R}[X]}{(X^2+1)} \simeq \operatorname{Im} \varphi = \mathbb{C}$$

$$a + bX + (\ ) \longleftrightarrow a + bi$$

OTRO HOMOMORFISMO IMPORTANTE

- Cualquier homomorfismo de anillos $\varphi: A \longmapsto B$ induce un homomorfismo $\bar{\varphi}: A[X] \longmapsto B[X]$ caracterizado por $\begin{cases} X \longmapsto X \\ a \longmapsto \varphi(a), \text{ si } a \in A \end{cases}$

Luego $\bar{\varphi}\left(\sum a_i X^i\right) = \sum \varphi(a_i) X^i$.

Demostración:

1) $\bar{\varphi}(1) = \varphi(1) = 1$

2) $\bar{\varphi}\left(\underbrace{\sum a_i X^i} + \underbrace{\sum b_i X^i}\right) = \bar{\varphi}\left(\sum (a_i + b_i) X^i\right) = \sum \varphi(a_i + b_i) X^i =$
$= \sum \varphi(a_i) X^i + \sum \varphi(b_i) X^i = \underbrace{\bar{\varphi}\left(\sum a_i X^i\right)} + \underbrace{\bar{\varphi}\left(\sum b_i X^i\right)}$

3) $\bar{\varphi}\left(\underbrace{\left(\sum a_i X^i\right)}\underbrace{\left(\sum b_j X^j\right)}\right) = \bar{\varphi}\left(\sum a_i b_j X^{i+j}\right) = \sum \varphi(a_i b_j) X^{i+j}$
$= \sum \varphi(a_i)\varphi(b_j) X^{i+j} = \left(\sum \varphi(a_i) X^i\right)\left(\sum \varphi(b_j) X^j\right) = \underbrace{\bar{\varphi}\left(\sum a_i X^i\right)} \cdot \underbrace{\bar{\varphi}\left(\sum b_j X^j\right)}$

Ejemplo: $\varphi: A \mapsto A/I \Rightarrow \bar{\varphi}: A[X] \mapsto (A/I)[X]$
$a \longmapsto \bar{a}$ $\qquad \sum a_i X^i \mapsto \sum \bar{a}_i X^i$

(siempre supravectivo)

Un caso particularmente interesante es el del homomorfismo $\mathbb{Z} \xrightarrow{\varphi} \mathbb{Z}/(n)$ y su asociado $\mathbb{Z}[X] \xrightarrow{\bar{\varphi}} \mathbb{Z}/(n)[X]$
$a \mapsto \bar{a}$ $\qquad \sum a_i X^i \longmapsto \sum \bar{a}_i X^i$

$\begin{cases} \varphi(1) = \bar{1} \\ \varphi(a+b) = \overline{a+b} = \bar{a} + \bar{b} = \varphi(a) + \varphi(b) \\ \varphi(a \cdot b) = \overline{a \cdot b} = \bar{a} \cdot \bar{b} = \varphi(a) \cdot \varphi(b) \end{cases}$

Calculemos el núcleo de $\bar{\varphi}$:

$$\operatorname{Ker}\bar{\varphi} = \left\{ \sum a_i X^i \in \mathbb{Z}[X] \,/\, \sum \bar{a_i} X^i = 0 \right\} = \left\{ \sum a_i X^i \,/\, \bar{a_i} = 0, \forall i \right\}$$

$$= \left\{ \sum a_i X^i \in \mathbb{Z}[X] \,/\, a_i \in (n) \right\} = (n) \subseteq \mathbb{Z}[X].$$

En este caso el T. de isomorfía dice que

$$\mathbb{Z}[X] / (n) \cong \mathbb{Z}/(n)\,[X]$$

es un conjunto de polinomios:

$$(n) = \left\{ \left(\sum a_i x^i\right) n \,/\, a_i \in \mathbb{Z} \right\}$$

es un conjunto de números:

$$(n) = \left\{ a\, n \,/\, a \in \mathbb{Z} \right\}$$

HOMOMORFISMOS DE $\mathbb{Z}$ EN OTRO ANILLO

¿Cuántos homomorfismos puede haber de $\mathbb{Z}$ en otro anillo R?

(Notación: Si $a \in R$ y $n \in \mathbb{N}$, ponemos $\begin{cases} na = \underbrace{a + \cdots + a}_{n} \\ (-n)a = \underbrace{(-a) + \cdots + (-a)}_{n} \end{cases}$

Let $f: \mathbf{Z} \to R$ be a ring homomorphism. By definition we must have $f(1) = e$. Hence necessarily for every positive integer n we must have

$e = 1_R$

$$f(n) = f(\underbrace{1 + \cdots + 1}_{n}) = \underbrace{f(1) + \cdots + f(1)}_{n} = ne,$$

and for a negative integer $m = -k$,

$$f(-k) = -f(k) = -(ke).$$

Thus there is ~~one and only one~~ at most one ring homomorphism of $\mathbf{Z}$ into a ring

aunque debemos comprobar que éste lo es:

i) $f(1) = e = 1_R = 1$

ii) $f(m+n) = (m+n)e = (\underbrace{e + \cdots + e}_{m+n}) = (\underbrace{e + \cdots + e}_{m}) + (\underbrace{e + \cdots + e}_{n}) = f(m) + f(n)$

iii) $f(mn) = (\underbrace{e + \cdots + e}_{mn}) = (\underbrace{e + \cdots + e}_{m})(\underbrace{e + \cdots + e}_{n}) = f(m)f(n)$

Assume $R \neq \{0\}$. Let $f: \mathbf{Z} \to R$ be *the* ring homomorphism. Then the kernel of f is not all of $\mathbf{Z}$ and hence is an ideal $n\mathbf{Z}$ for some integer

$= (n)$

$\begin{cases} f: \mathbb{Z} \longmapsto R \\ \mathbb{Z}/n\mathbb{Z} \simeq f(\mathbb{Z}) \subset R \end{cases}$

$n \geqq 0$. It follows from Theorem ~~3.1~~ Isomorfía that $\mathbf{Z}/n\mathbf{Z}$ is isomorphic to the image of f. In practice, we do not make any distinction between $\mathbf{Z}/n\mathbf{Z}$ and its image in R, and we agree to say that R contains $\mathbf{Z}/n\mathbf{Z}$ as a subring.

Suppose that $n \neq 0$. *Then we have relation*

$$na = 0 \quad \textit{for all} \quad a \in R.$$

$(na = (\underbrace{e + \cdots + e}_{n})a = f(n)a = 0 \cdot a = 0)$

Indeed, $na = (ne)a = 0a = 0$. Sometimes one says that R has **characteristic** n. Thus if n is the characteristic of R, then $na = 0$ for all $a \in R$.

Definición: $ch(R) = n$ si $\operatorname{Ker}(f: \mathbb{Z} \mapsto R) = (n) \Leftrightarrow \mathbb{Z}/(n) \subset R$

Theorem 3.2. *Suppose that R is an integral ring, so has no divisors of 0. Then the integer n such that $\mathbf{Z}/n\mathbf{Z}$ is contained in R must be 0 or a prime number.* (i.e. R íntegro $\Rightarrow ch(R) = \begin{cases} 0 \\ p, \text{ primo} \end{cases}$)

Proof. Suppose n is not 0 and is not prime. Then $n = mk$ with integers $m, k \geqq 2$, and neither m, k are in the kernel of the homomorphism $f: \mathbf{Z} \to R$. Hence $me \neq 0$ and $ke \neq 0$. But $(me)(ke) = mke = 0$, contradicting the hypothesis that R has no divisors of 0. Hence n is prime.

$f(m) \cdot f(k) = f(mk) = f(n) = 0$

Supongamos $n = 6 \Leftrightarrow \operatorname{Ker} f = (6)$; $f: \mathbb{Z} \mapsto R$
$6 = 2 \cdot 3$; $2, 3 \notin (6) = \operatorname{Ker} f \Rightarrow f(2) \neq 0, f(3) \neq 0$
$0 = f(6) = \underset{\neq 0}{f(2)} \cdot \underset{\neq 0}{f(3)} \Rightarrow R$ tiene div. de cero. Contrad.

Let K be a field and let $f: \mathbf{Z} \to K$ be the homomorphism of the integers into K. If the kernel of f is $\{0\}$, then K contains $\mathbf{Z}$ as a subring, and we say that K has **characteristic** 0. If the kernel of f is generated by a prime number p, then we say that K has **characteristic** p. The field $\mathbb{F}_p =$ $\mathbf{Z}/p\mathbf{Z}$ is sometimes denoted by $\mathbf{F}_p$, and is called the **prime field**, of characteristic p. This prime field $\mathbf{F}_p$ is contained in every field of characteristic p.

- $ch(K) = 0 \Leftrightarrow \mathbb{Z} \subset K$
- $ch(K) = p \Leftrightarrow \mathbb{F}_p \subset K$

La característica de un anillo A puede interpretarse de la siguiente forma:

- $\underline{ch(A) = n \geq 2}$ si n es el número natural más pequeño tal que $\underbrace{1 + \cdots + 1}_{n} = 0$ en A.
- $\underline{ch(A) = 0}$, si lo anterior no ocurre nunca.

<u>Ejemplos</u>: $ch(\mathbb{Z}) = ch(\mathbb{Q}) = ch(\mathbb{R}) = ch(\mathbb{C}) = 0$,

- $ch(\mathbb{Z}[X]) = ch(\mathbb{Q}[X]) = ch(\mathbb{R}[X]) = ch(\mathbb{C}[X]) = 0$
- $ch(\mathbb{Q}(\sqrt{5})) = 0$
- $ch(\mathbb{Z}/(n)) = ch(\mathbb{Z}/(n)[X]) = n$
- $ch(A) = ch(A[X])$

(pues el 1 de $A[X]$ es el 1 de A)