# Capítulo 4
# Homomorfismos de anillos

> Les mathématiciens n'étudient pas des objets, mais des relations entre les objets.
>
> Poincaré

En álgebra normalmente no se estudian anillos por separado, sino las relaciones entre diferentes anillos. Para relacionar dos anillos sirve la noción de homomorfismo.

## 4.1 Homomorfismos

**4.1.1. Definición.** Se dice que una aplicación entre dos anillos $\phi\colon A \to B$ es un **homomorfismo** si se cumplen las siguientes condiciones:

1) se preservan las sumas: $\phi(x+y) = \phi(x) + \phi(y)$ para cualesquiera $x, y \in A$;

2) se preserva la identidad: $\phi(1_A) = 1_B$;

3) se preservan los productos: $\phi(xy) = \phi(x)\,\phi(y)$ para cualesquiera $x, y \in A$.

**4.1.2. Ejemplo.** Para todo anillo $A$ existe un único homomorfismo $A \to 0$ al anillo nulo. ▲

**4.1.3. Ejemplo.** Si $A \subseteq B$ es un subanillo, entonces la inclusión $\iota\colon A \hookrightarrow B$ es un homomorfismo. ▲

**4.1.4. Ejemplo.** Sean $A$ un dominio y $\operatorname{Frac} A$ su cuerpo de fracciones. Aunque antes estabamos identificando $A$ con el subanillo de $\operatorname{Frac} A$ formado por las fracciones $\frac{a}{1}$, sería más correcto decir que se trata de un homomorfismo inyectivo

$$\iota\colon A \hookrightarrow \operatorname{Frac} A, \quad a \mapsto \frac{a}{1}.$$ ▲

**4.1.5. Ejemplo.** Para un cuerpo $k$ tenemos una cadena de homomorfismos inyectivos

$$k \hookrightarrow k[X] \hookrightarrow k[[X]] \hookrightarrow k((X)),$$

donde $k[X]$ es el anillo de polinomios, $k[[X]]$ es el anillo de las series de potencias y $k((X))$ es el cuerpo de las series de Laurent. ▲

**4.1.6. Ejemplo.** La conjugación compleja

$$x + yi \mapsto \overline{x + yi} := x - yi$$

es un homomorfismo $\mathbb{C} \to \mathbb{C}$. ▲

**4.1.7. Ejemplo.** La proyección canónica

$$\mathbb{Z} \twoheadrightarrow \mathbb{Z}/n\mathbb{Z}, \quad a \mapsto [a]_n$$

es un homomorfismo de anillos. De hecho, $\mathbb{Z}/n\mathbb{Z}$ es un ejemplo de **anillo cociente** que vamos a introducir en la siguiente sección. ▲

**4.1.8. Ejemplo.** Sea $A$ un anillo conmutativo. Para $\underline{c} = (c_1, \ldots, c_n)$ donde $c_i \in A$ tenemos el **homomorfismo de evaluación**

$$\begin{aligned} ev_{\underline{c}} \colon A[X_1, \ldots, X_n] &\to A, \\ f = \sum_{i_1, \ldots, i_n \geq 0} a_{i_1, \ldots, i_n} X_1^{i_1} \cdots X_n^{i_n} &\mapsto f(c_1, \ldots, c_n) := \sum_{i_1, \ldots, i_n \geq 0} a_{i_1, \ldots, i_n} c_1^{i_1} \cdots c_n^{i_n}. \end{aligned}$$ ▲

**4.1.9. Observación.** *Si $\phi \colon A \to B$ y $\psi \colon B \to C$ son dos homomorfismos de anillos, entonces su composición $\psi \circ \phi \colon A \to C$ es también un homomorfismo.* □

**4.1.10. Observación.** *Sea $\phi \colon A \to B$ un homomorfismo de anillos. Se cumplen las siguientes propiedades.*

*0)* $\phi(0_A) = 0_B$,

*1)* $\phi(-x) = -\phi(x)$ *para todo* $x \in A$,

*2) para todo $x$ invertible en $A$ el elemento $\phi(x)$ es invertible en $B$ y se cumple $\phi(x^{-1}) = \phi(x)^{-1}$.*

$$\begin{array}{ccc} A^\times & \overset{\phi^\times}{\dashrightarrow} & B^\times \\ \downarrow & & \downarrow \\ A & \xrightarrow{\phi} & B \end{array}$$

*Demostración.* En la parte 0), basta notar que

$$\phi(0_A) = \phi(0_A + 0_A) = \phi(0_A) + \phi(0_A),$$

así que $\phi(0_A) = 0_B$ por la cancelación. En la parte 1), notamos que

$$\phi(x) + \phi(-x) = \phi(x + (-x)) = \phi(0_A) = 0_B.$$

En fin, la parte 2) es un análogo multiplicativo de 1) y se demuestra de la misma manera:

$$\phi(x^{-1})\,\phi(x) = \phi(x^{-1}\,x) = \phi(1_A) = 1_B, \quad \phi(x)\,\phi(x^{-1}) = \phi(x\,x^{-1}) = \phi(1_A) = 1_B.$$ ■

**4.1.11. Ejemplo.** Para todo anillo $A$ existe un único homomorfismo $\phi \colon \mathbb{Z} \to A$ desde el anillo de los enteros. En efecto, por la definición, $\phi(1) = 1_A$, y luego para todo $n \in \mathbb{Z}$ se tiene necesariamente

$$\phi(n) = \begin{cases} \underbrace{1_A + \cdots + 1_A}_{n}, & n > 0, \\ -(\underbrace{1_A + \cdots + 1_A}_{-n}), & n < 0, \\ 0, & \phi = 0. \end{cases}$$ ▲

**4.1.12. Definición.** Se dice que un homomorfismo de anillos $\phi\colon A \to B$ es un **isomorfismo** si existe un homomorfismo $\phi^{-1}\colon B \to A$ tal que $\phi^{-1}\circ\phi = \mathrm{id}_A$ y $\phi\circ\phi^{-1} = \mathrm{id}_B$.

Cuando entre dos anillos $A$ y $B$ existe un isomorfismo, se dice que $A$ y $B$ son **isomorfos** y se escribe $A \cong B$.

Un isomorfismo $\phi\colon A \to A$ se llama un **automorfismo** de $A$.

Por supuesto, todo anillo $A$ es isomorfo a sí mismo: la aplicación identidad $\mathrm{id}\colon A \to A$ es un automorfismo. Sin embargo, en muchos casos hay automorfismos distintos de id y el estudio de automorfismos es muy importante en álgebra.

**4.1.13. Ejemplo.** La conjugación compleja $\sigma\colon \mathbb{C} \to \mathbb{C}$ es un automorfismo de $\mathbb{C}$: se tiene $\sigma\circ\sigma = \mathrm{id}$. ▲

**4.1.14. Observación.** *Todo homomorfismo de anillos $\phi\colon A \to B$ es un isomorfismo si y solamente si es biyectivo.*

*Demostración.* Si $\phi$ es un isomorfismo, entonces $\phi$ admite el homomorfismo inverso $\phi^{-1}\colon B \to A$, así que es una biyección.

Viceversa, supongamos que $\phi$ es un homomorfismo biyectivo. En este caso existe una aplicación inversa $\phi^{-1}\colon B \to A$ y hay que comprobar que es un homomorfismo de anillos. Dado que $\phi(1_A) = 1_B$, tenemos $\phi^{-1}(1_B) = 1_A$. Luego, para $x, y \in B$

$$\phi^{-1}(xy) = \phi^{-1}\Big(\phi\circ\phi^{-1}(x)\cdot\phi\circ\phi^{-1}(y)\Big) = \phi^{-1}\Big(\phi(\phi^{-1}(x)\cdot\phi^{-1}(y))\Big) = \phi^{-1}(x)\cdot\phi^{-1}(y).$$

Con el mismo truco se demuestra que $\phi^{-1}(x+y) = \phi^{-1}(x) + \phi^{-1}(y)$. ■

**4.1.15. Observación (Imagen y preimagen).** *Sea $\phi\colon A \to B$ un homomorfismo de anillos.*

1) *La **imagen** $\phi(A) := \{\phi(x) \mid x \in A\}$ es un subanillo de $B$.*
2) *Si $B' \subseteq B$ es un subanillo, entonces su preimagen*

$$\phi^{-1}(B') := \{x \in A \mid \phi(x) \in B'\}$$

*es un subanillo de $A$.* □

**4.1.16. Observación.** *Sea $\phi\colon A \to B$ un homomorfismo de anillos conmutativos.*

1) *Si $\mathfrak{b} \subseteq B$ es un ideal, entonces $\phi^{-1}(\mathfrak{b})$ es un ideal en $A$.*
2) *Si $\phi$ es sobreyectivo y $\mathfrak{a} \subseteq A$ es un ideal, entonces $\phi(\mathfrak{a})$ es un ideal en $B$.* □

**4.1.17. Comentario.** Si $\phi\colon A \to B$ es un homomorfismo que no es sobreyectivo, entonces $\phi(\mathfrak{a})$ no tiene por qué ser un ideal en $B$. Considere por ejemplo la inclusión $\iota\colon \mathbb{Z} \hookrightarrow \mathbb{Q}$. Note que $\mathbb{Z}$ no es un ideal en $\mathbb{Q}$, sino un subanillo. Cualquier otro ideal $(n) \subset \mathbb{Z}$ para $n = 2, 3, 4, 5, \ldots$ tampoco será un ideal en $\mathbb{Q}$

Un ejemplo importante de ideales es el núcleo de un homomorfismo de anillos.

**4.1.18. Observación.** *Sea $\phi\colon A \to B$ un homomorfismo de anillos conmutativos. Entonces, el conjunto*

$$\ker\phi := \{x \in A \mid \phi(x) = 0\}$$

*es un ideal en $A$, llamado el **núcleo** de $\phi$.* □

**4.1.19. Ejemplo.** Consideremos el homomorfismo

$$\phi\colon \mathbb{Q}[X] \to \mathbb{C}, \quad f \mapsto f(\zeta_3),$$

donde $\zeta_3 = e^{2\pi i/3} = -\frac{1}{2} + \frac{\sqrt{3}}{2}\,i$. El anillo $\mathbb{Q}[X]$ es un dominio de ideales principales, lo que implica que $\ker\phi = (g)$ para algún polinomio $g \in \mathbb{Q}[X]$. Notamos que $\zeta_3^2 + \zeta_3 + 1 = 0$, así que $X^2 + X + 1 \in \ker\phi$. Luego, $(X^2 + X + 1) \subseteq (g)$, lo que significa que $g \mid (X^2 + X + 1)$. Pero el polinomio $X^2 + X + 1$ es irreducible en $\mathbb{Q}[X]$: sus raíces son $\zeta_3$ y $\overline{\zeta_3}$. Podemos concluir que $g \sim X^2 + X + 1$ y $\ker\phi = (X^2 + X + 1)$. ▲

**4.1.20. Ejemplo.** Sea $k$ un cuerpo. Consideremos el homomorfismo

$$\phi\colon k[X_1,\dots,X_n] \to k, \quad f \mapsto f(0,\dots,0).$$

Su núcleo consiste en los polinomios con el término constante nulo. Se ve que

$$\ker\phi = (X_1,\dots,X_n) = \{f_1 X_1 + \cdots + f_n X_n \mid f_1,\dots,f_n \in k[X_1,\dots,X_n]\}.$$ ▲

**4.1.21. Observación.** *Un homomorfismo de anillos $\phi\colon A \to B$ es inyectivo si y solo si* $\ker\phi = 0$.

*Demostración.* Tenemos para cualesquiera $x, y \in A$

$$\phi(x) = \phi(y) \iff \phi(x) - \phi(y) = 0 \iff \phi(x-y) = 0.$$ ■

**4.1.22. Observación.** *Sea $k$ un cuerpo y $A$ un anillo no nulo. Entonces, todo homomorfismo $\phi\colon k \to A$ es inyectivo.*

*Primera demostración.* Todo elemento no nulo $x \in k$ es invertible, pero luego $\phi(x)$ es invertible en $A$, lo que implica $\phi(x) \neq 0$. Entonces, $\ker\phi = 0$. ■

*Segunda demostración.* En un cuerpo $k$ los únicos ideales son $0$ y $k$. Si $A \neq 0$, entonces $\phi(1) = 1 \neq 0$ y $1 \notin \ker\phi$. Podemos concluir que $\ker\phi = 0$. ■

(Ambos argumentos de arriba son esencialmente idénticos, pero el segundo suena más sofisticado.)

## 4.2 Anillos cociente

**4.2.1. Observación.** *Sea $A$ un anillo conmutativo y sea $\mathfrak{a} \subseteq A$ un ideal. Consideremos la relación*

$$x \equiv y \pmod{\mathfrak{a}} \iff x - y \in \mathfrak{a}.$$

*Esta es una relación de equivalencia sobre los elementos de $A$.* □

Denotemos el cociente de $A$ por la relación de equivalencia de arriba por $A/\mathfrak{a}$. La clase de equivalencia de $x \in A$ será denotada por

$$\overline{x} = \{b \mid x - b \in \mathfrak{a}\}.$$

Notamos que $\overline{x}$ consiste precisamente en los elementos de la forma $x + a$, donde $a \in \mathfrak{a}$, y por este motivo a veces en lugar de $\overline{x}$ se escribe "$x + \mathfrak{a}$", pero no vamos a usar esta notación cuando el ideal $\mathfrak{a}$ está claro desde el contexto.

**4.2.2. Definición.** Para un anillo conmutativo $A$ y un ideal $\mathfrak{a} \subseteq A$ el **anillo cociente** correspondiente es el conjunto de las clases de equivalencia $A/\mathfrak{a}$ con las operaciones

$$\overline{x} + \overline{y} := \overline{x+y}, \quad \overline{x} \cdot \overline{y} := \overline{xy}.$$

Hay que verificar que el producto y la suma están bien definidos y no dependen de la elección de representantes de clases de equivalencia. Supongamos que $y \equiv y' \pmod{a}$; es decir, que $y - y' \in \mathfrak{a}$. Luego, $(x+y) - (x+y') \in \mathfrak{a}$, lo que significa que $x + y \equiv x + y' \pmod{a}$. De la misma manera, para los productos $xy - xy' = x(y-y') \in \mathfrak{a}$, y por ende $xy \equiv xy' \pmod{a}$.

**4.2.3. Observación.** *El cociente $A/\mathfrak{a}$ con las operaciones de arriba es un anillo conmutativo. El cero es la clase de equivalencia $\overline{0}$, mientras que la identidad es la clase de equivalencia $\overline{1}$.* □

Notamos que $\overline{x} = 0$ en $A/\mathfrak{a}$ si y solo si $x \in \mathfrak{a}$.

**4.2.4. Observación.** *Si $A$ es un anillo conmutativo y $\mathfrak{a} \subseteq A$ es un ideal, entonces la proyección sobre el cociente*

$$\pi\colon A \twoheadrightarrow A/\mathfrak{a}, \quad x \mapsto \overline{x}$$

*es un homomorfismo de anillos.* □

**4.2.5. Ejemplo.** En todo anillo $A$ hay dos ideales evidentes: $\mathfrak{a} = 0$ e $\mathfrak{a} = A$. Para el ideal nulo, la relación de equivalencia es trivial: $x \equiv y$ significa que $x = y$. Por este motivo el cociente $A/0$ puede ser identificado con el mismo $A$; es decir, $A/0 \cong A$. Para el ideal $A$, se tiene $x \equiv y$ para cualesquiera $x, y \in A$, así que el cociente $A/A$ consiste en un elemento y es el anillo nulo: $A/A = 0$. ▲

**4.2.6. Ejemplo.** El cociente del anillo $\mathbb{Z}$ por el ideal $(n) =: n\mathbb{Z}$ generado por $n$ es el anillo $\mathbb{Z}/n\mathbb{Z}$ de los restos módulo $n$. ▲

**4.2.7. Ejemplo.** Sean $k$ un cuerpo y $f \in k[x]$ un polinomio con coeficientes en $k$. Usando la división con resto, cualesquiera $g_1, g_2 \in k[x]$ se pueden escribir como

$$g_1 = q_1 f + r_1, \quad g_2 = q_2 f + r_2, \quad \text{donde } \deg r_1, \deg r_2 < \deg f.$$

De aquí se ve que $g_1 \equiv g_2 \pmod{f}$ si y solamente si $r_1 = r_2$. Entonces, los distintos elementos en el cociente $k[x]/(f)$ se representan por los polinomios de grado $< \deg f$:

$$a_{n-1} X^{n-1} + a_{n-2} X^{n-2} + \cdots + a_1 X + a_0, \quad a_i \in k, \quad n = \deg f.$$ ▲

**4.2.8. Ejemplo.** Tenemos $\mathbb{R}[X]/(X^2+1) \cong \mathbb{C}$. En efecto, los elementos de $\mathbb{R}[X]/(X^2+1)$ pueden ser representados por los polinomios de la forma $bX + a$, donde $a, b \in \mathbb{R}$. Luego,

$$(bX + a)(dX + c) = bd X^2 + (bc + ad) X + ac \equiv (ac - bd) + (bc + ad) X \pmod{X^2+1}.$$

Esta fórmula corresponde a la multiplicación compleja, y se verifica que se tiene un isomorfismo

$$\begin{aligned} \mathbb{R}[X]/(X^2+1) &\xrightarrow{\cong} \mathbb{C} \\ bX + a &\mapsto a + bi. \end{aligned}$$ ▲

**4.2.9. Ejemplo (El cuerpo de cuatro elementos).** Calculemos $\mathbb{F}_2[X]/(X^2+X+1)$. Los elementos del cociente pueden ser representados por los polinomios de grado $\leq 1$ en $\mathbb{F}_2[X]$:

$$\overline{0}, \quad \overline{1}, \quad \overline{X}, \quad \overline{X+1}.$$

La tabla de adición y multiplicación correspondiente viene dada por

| $+$ | $\overline{0}$ | $\overline{1}$ | $\overline{X}$ | $\overline{X+1}$ |
|---|---|---|---|---|
| $\overline{0}$ | $\overline{0}$ | $\overline{1}$ | $\overline{X}$ | $\overline{X+1}$ |
| $\overline{1}$ | $\overline{1}$ | $\overline{0}$ | $\overline{X+1}$ | $\overline{X}$ |
| $\overline{X}$ | $\overline{X}$ | $\overline{X+1}$ | $\overline{0}$ | $\overline{1}$ |
| $\overline{X+1}$ | $\overline{X+1}$ | $\overline{X}$ | $\overline{1}$ | $\overline{0}$ |

| $\cdot$ | $\overline{0}$ | $\overline{1}$ | $\overline{X}$ | $\overline{X+1}$ |
|---|---|---|---|---|
| $\overline{0}$ | $\overline{0}$ | $\overline{0}$ | $\overline{0}$ | $\overline{0}$ |
| $\overline{1}$ | $\overline{0}$ | $\overline{1}$ | $\overline{X}$ | $\overline{X+1}$ |
| $\overline{X}$ | $\overline{0}$ | $\overline{X}$ | $\overline{X+1}$ | $\overline{1}$ |
| $\overline{X+1}$ | $\overline{0}$ | $\overline{X+1}$ | $\overline{1}$ | $\overline{X}$ |

Notamos que $\overline{X}^{-1} = \overline{X+1}$ y $\mathbb{F}_2[X]/(X^2+X+1)$ es un cuerpo de cuatro elementos. Todos los cuerpos finitos pueden ser construidos de esta manera. Por ejemplo, el lector puede verificar que $\mathbb{F}_3[X]/(X^2+1)$ es un cuerpo de 9 elementos. ▲

Los últimos dos ejemplos tienen algo en común: $\mathbb{R}[X]$ y $\mathbb{F}_2[X]$ son dominios de ideales principales y los polinomios $X^2+1$ y $X^2+X+1$ son irreducibles en $\mathbb{R}[X]$ y $\mathbb{F}_2[X]$ respectivamente.

**4.2.10. Proposición.** *Sea $A$ un anillo conmutativo y $p \in A$ un elemento primo.*

1) *El anillo cociente $A/(p)$ es un dominio.*

2) *Si $A$ es un dominio de ideales principales, entonces $A/(p)$ es un cuerpo.*

*Demostración.* En la parte 1), tenemos $p \notin A^\times$, y por ende $A/(p) \neq 0$. Luego, para cualesquiera $x, y \in A$ se tiene

$$p \mid xy \Longrightarrow p \mid x \text{ o } p \mid y,$$

pero esto implica que para cualesquiera $\overline{x}, \overline{y} \in A/(p)$ se tiene

$$\overline{x}\,\overline{y} = 0 \Longrightarrow \overline{x} = 0 \text{ o } \overline{y} = 0.$$

En la parte 2), sea $\overline{x} \in A/(p)$ un elemento no nulo; es decir, un elemento representado por $x \in A$ tal que $p \nmid x$. Consideremos el ideal $(p, x) \subseteq A$. Por nuestra hipótesis sobre $A$, este tiene que ser generado por un elemento: existe $u \in A$ tal que $(p, x) = (u)$. Pero en este caso $u \mid p$ y $u \mid x$. Siendo primo, $p$ es irreducible, así que $u \sim p$ o $u \in A^\times$. El caso de $u \sim p$ puede ser excluido: esto implicaría que $p \mid x$. Entonces, $u \in A^\times$ y $(p, x) = A$. En particular, existen $a, y \in A$ tales que

$$ap + yx = 1.$$

Módulo $p$ esta identidad nos da

$$\overline{y} \cdot \overline{x} = \overline{1},$$

y entonces $\overline{x}^{-1} = \overline{y}$ en $A/(p)$. ■

El resultado de arriba nos permite construir cuerpos de la siguiente manera: si $k$ es un cuerpo, entonces el anillo de polinomios $k[X]$ es un dominio de ideales principales. Luego, si $f \in k[X]$ es un polinomio irreducible, entonces $k[X]/(f)$ es un cuerpo. Notamos que el homomorfismo

$$k \hookrightarrow k[X] \twoheadrightarrow k[X]/(f)$$

es inyectivo gracias a 4.1.22, así que $k$ puede ser identificado con un subcuerpo de $k[X]/(f)$.

**4.2.11. Ejemplo.** En el anillo de los enteros de Gauss $\mathbb{Z}[i]$ consideremos el elemento primo $1+i$. Calculemos el cociente $\mathbb{Z}[i]/(1+i)$. Primero notamos que cualquier elemento $\alpha \in \mathbb{Z}[i]$ es congruente a 0 o 1 módulo el ideal $(1+i)$. En efecto, si $\alpha = a + bi$, donde $a$ y $b$ tienen la misma paridad, entonces

$$\frac{a+bi}{1+i} = \frac{(a+bi)(1-i)}{2} = \frac{(a+b)+(b-a)\,i}{2},$$

donde $a+b$ y $b-a$ son números pares, así que $(1+i) \mid \alpha$ y por ende

$$\alpha \equiv 0 \pmod{1+i}.$$

Ahora si $a$ y $b$ tienen diferente paridad, entonces $a-1$ y $b$ tienen la misma paridad y

$$a + bi - 1 \equiv 0 \pmod{1+i},$$

y por lo tanto $\alpha \equiv 1 \pmod{1+i}$. Por otro lado, $(1+i) \nmid 1$, así que $1 \not\equiv 0 \pmod{1+i}$. Esto nos permite concluir que

$$\mathbb{Z}[i]/(1+i) = \{\overline{0}, \overline{1}\}.$$

Entonces, tenemos un cuerpo de dos elementos. ▲

El lector puede tratar de hacer cálculos parecidos y verificar que, por ejemplo, $\mathbb{Z}[i]/(1+2i)$ es un cuerpo de 5 elementos.

## 4.3 Teoremas de isomorfía

**4.3.1. Primer teorema de isomorfía.** *Sea $\phi\colon A \to B$ un homomorfismo de anillos. Entonces, existe un isomorfismo canónico*

$$\overline{\phi}\colon A/\ker\phi \xrightarrow{\cong} \phi(A), \quad \overline{x} \mapsto \phi(x).$$

*Demostración.* Primero notamos que la aplicación $\overline{\phi}$ está bien definida. Tenemos para cualesquiera $x, x' \in A$

$$\overline{x} = \overline{x'} \iff x - x' \in \ker\phi \iff \phi(x - x') = 0 \iff \phi(x) = \phi(x').$$

Esto también demuestra que $\overline{\phi}$ es una aplicación inyectiva. La sobreyectividad es evidente: el conjunto de llegada de $\overline{\phi}$ es precisamente la imagen de $\phi$. En fin, $\overline{\phi}$ es un homomorfismo, puesto que $\phi$ lo es:

$$\overline{\phi}(\overline{x}\cdot\overline{y}) = \overline{\phi}(\overline{xy}) = \phi(xy) = \phi(x)\,\phi(y) = \overline{\phi}(\overline{x})\,\overline{\phi}(\overline{y}).$$ ■

**4.3.2. Ejemplo.** Para la proyección sobre el anillo cociente $\pi\colon A \to A/\mathfrak{a}$ se tiene $\ker\pi = \mathfrak{a}$. ▲

**4.3.3. Ejemplo.** Consideremos el homomorfismo de evaluación

$$\begin{aligned}\phi\colon \mathbb{R}[X] &\to \mathbb{C},\\ \phi &\mapsto \phi(i).\end{aligned}$$

Es visiblemente sobreyectivo. Su núcleo consiste en los polinomios en $\mathbb{R}[X]$ que tienen $i$ como su raíz, y se verifica fácilmente que $\ker\phi = (X^2+1)$. Podemos concluir que

$$\mathbb{R}[X]/(X^2+1) \cong \mathbb{C}.$$ ▲

**4.3.4. Ejemplo.** El homomorfismo de evaluación

$$\begin{aligned}\phi\colon k[X_1,\dots,X_n] &\to k,\\ f &\mapsto f(0,\dots,0)\end{aligned}$$

es sobreyectivo y tiene como su núcleo el ideal $(X_1,\dots,X_n)$ que consiste en polinomios con término constante nulo. Luego,

$$k[X_1,\dots,X_n]/(X_1,\dots,X_n) \cong k.$$ ▲

**4.3.5. Ejemplo.** Sea $A$ un anillo conmutativo y $\mathfrak{a} \subseteq A$ un ideal. Consideremos la aplicación

$$\begin{aligned}\phi\colon A[X] &\to (A/\mathfrak{a})[X],\\ \sum_{i\geq 0} c_i X^i &\mapsto \sum_{i\geq 0} \overline{c_i} X^i\end{aligned}$$

que reduce los coeficientes de un polinomio módulo $\mathfrak{a}$. Se ve que este es un homomorfismo sobreyectivo. Su núcleo consiste en los polinomios con coeficientes en $\mathfrak{a}$:

$$\mathfrak{a}[X] := \Big\{ \sum_{i\geq 0} c_i X^i \;\Big|\; c_i \in \mathfrak{a} \Big\}.$$

Luego, el primer teorema de isomorfía nos permite concluir que

$$A[X]/\mathfrak{a}[X] \cong (A/\mathfrak{a})[X].$$

En particular, si $\mathbb{Z}[X]$ es el anillo de polinomios con coeficientes enteros, entonces los polinomios con coeficientes divisibles por $n$ forman un ideal $n\mathbb{Z}[X] \subset \mathbb{Z}[X]$ y se tiene

$$\mathbb{Z}[X]/n\mathbb{Z}[X] \cong \mathbb{Z}/n\mathbb{Z}[X].$$ ▲

Ahora vamos a formular el segundo y el tercer teorema de isomorfía, pero las pruebas se dejan al lector (véanse los ejercicios 4.7 y 4.7 para las indicaciones).

**4.3.6. Segundo teorema de isomorfía**. *Sean $A$ un anillo conmutativo, $B \subseteq A$ un subanillo y $\mathfrak{a} \subseteq A$ un ideal. Entonces,*

$$B + \mathfrak{a} := \{x + y \mid x \in B, y \in \mathfrak{a}\}$$

*es un subanillo de $A$ y $\mathfrak{a}$ es un ideal en $B + \mathfrak{a}$ y hay un isomorfismo canónico*

$$B/(B \cap \mathfrak{a}) \cong (B + \mathfrak{a})/\mathfrak{a}.$$

**4.3.7. Tercer teorema de isomorfía**. *Sean $A$ un anillo conmutativo y $\mathfrak{a} \subseteq \mathfrak{b} \subseteq A$ ideales. Entonces,*

$$\mathfrak{b}/\mathfrak{a} := \{x + \mathfrak{a} \mid x \in \mathfrak{b}\}$$

*es un ideal en el anillo cociente $A/\mathfrak{a}$ y hay un isomorfismo canónico*

$$(A/\mathfrak{a})/(\mathfrak{b}/\mathfrak{a}) \cong A/\mathfrak{b}.$$

## 4.4 Ideales en el anillo cociente

**4.4.1. Teorema.** *Sean $A$ un anillo conmutativo y $\mathfrak{a} \subseteq A$ un ideal. Denotemos por $\pi\colon A \twoheadrightarrow A/\mathfrak{a}$ la proyección sobre el anillo cociente dada por $x \mapsto \overline{x} := x + \mathfrak{a}$. Hay una biyección*

$$\begin{aligned} \{\textit{ideales } \mathfrak{b} \subseteq A \textit{ tales que } \mathfrak{a} \subseteq \mathfrak{b}\} &\leftrightarrow \{\textit{ideales } \overline{\mathfrak{b}} \subseteq A/\mathfrak{a}\}, \\ \mathfrak{b} &\mapsto \mathfrak{b}/\mathfrak{a} := \pi(\mathfrak{b}) = \{x + \mathfrak{a} \mid x \in \mathfrak{b}\}, \\ \pi^{-1}(\overline{\mathfrak{b}}) &\mapsfrom \overline{\mathfrak{b}}. \end{aligned}$$

*Esta biyección preserva las inclusiones:*

1) *si $\mathfrak{a} \subseteq \mathfrak{b}_1 \subseteq \mathfrak{b}_2 \subseteq A$, entonces $\pi(\mathfrak{b}_1) \subseteq \pi(\mathfrak{b}_2) \subseteq A/\mathfrak{a}$;*

2) *si $\overline{\mathfrak{b}_1} \subseteq \overline{\mathfrak{b}_2} \subseteq A/\mathfrak{a}$, entonces $\mathfrak{a} \subseteq \pi^{-1}(\overline{\mathfrak{b}_1}) \subseteq \pi^{-1}(\overline{\mathfrak{b}_2}) \subseteq A$.*

*Demostración.* El hecho de que las aplicaciones estén bien definidas se sigue de 4.1.16: la imagen $\pi(\mathfrak{b}) \subseteq A/\mathfrak{a}$ de un ideal $\mathfrak{b} \subseteq A$ respecto al homomorfismo sobreyectivo $\pi$ es un ideal y la preimagen $\pi^{-1}(\overline{\mathfrak{b}}) \subseteq A$ de un ideal $\overline{\mathfrak{b}} \subseteq A/\mathfrak{a}$ es también un ideal. Además, tenemos $\overline{0} \in \overline{\mathfrak{b}}$ para todo ideal $\overline{\mathfrak{b}} \subseteq A/\mathfrak{a}$ y $\pi^{-1}(\overline{0}) = \mathfrak{a}$, así que $\mathfrak{a} \subseteq \pi^{-1}(\overline{\mathfrak{b}})$.

Hay que ver que las aplicaciones $\mathfrak{b} \mapsto \pi(\mathfrak{b})$ y $\overline{\mathfrak{b}} \mapsto \pi^{-1}(\overline{\mathfrak{b}})$ son mutualmente inversas. Tenemos

$$\pi(\pi^{-1}(\overline{\mathfrak{b}})) = \overline{\mathfrak{b}}$$

gracias a la sobreyectividad de $\pi$. Además,

$$\begin{aligned} \pi^{-1}(\pi(\mathfrak{b})) = \{x \in A \mid \pi(x) \in \pi(\mathfrak{b})\} = \{x \in A \mid \pi(x) = \pi(x') \text{ para algún } x' \in \mathfrak{b}\} \\ = \{x \in A \mid x - x' \in \ker \pi = \mathfrak{a} \text{ para algún } x' \in \mathfrak{b}\} = \mathfrak{b} \end{aligned}$$

(usando que $\mathfrak{a} \subseteq \mathfrak{b}$). Está claro que las dos aplicaciones preservan las inclusiones. ∎

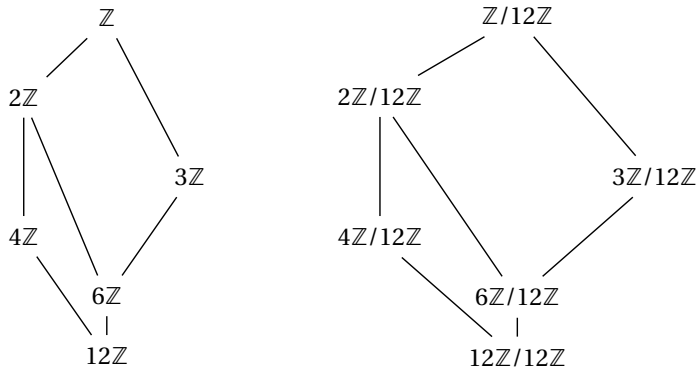
**4.4.2. Ejemplo.** Describamos los ideales en el anillo cociente $\mathbb{Z}/12\mathbb{Z}$. Según el teorema, estos corresponden a los ideales en $\mathbb{Z}$ que contienen a $12\mathbb{Z}$:

$$12\mathbb{Z} \subseteq n\mathbb{Z} \subseteq \mathbb{Z}.$$

Dado que $12\mathbb{Z} \subseteq n\mathbb{Z}$ significa que $n \mid 12$, tenemos $n = 1, 2, 3, 4, 6, 12$. Entonces, los ideales en el cociente son

$$\begin{aligned}
\mathbb{Z}/12\mathbb{Z} &= \{[0],[1],[2],[3],[4],[5],[6],[7],[8],[9],[10],[11]\},\\
2\mathbb{Z}/12\mathbb{Z} &= \{[0],[2],[4],[6],[8],[10]\},\\
3\mathbb{Z}/12\mathbb{Z} &= \{[0],[3],[6],[9]\},\\
4\mathbb{Z}/12\mathbb{Z} &= \{[0],[4],[8]\},\\
6\mathbb{Z}/12\mathbb{Z} &= \{[0],[6]\},\\
12\mathbb{Z}/12\mathbb{Z} &= 0.
\end{aligned}$$

Tenemos las siguientes inclusiones de ideales:




▲

## 4.5 Suma y producto de ideales

**4.5.1. Observación (Suma y producto de ideales).** *Sean $A$ un anillo conmutativo y $\mathfrak{a}_1, \ldots, \mathfrak{a}_n \subseteq A$ ideales.*

1) *El ideal generado por los elementos de $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ coincide con el conjunto*

$$\mathfrak{a}_1 + \cdots + \mathfrak{a}_n := \{x_1 + \cdots + x_n \mid x_i \in \mathfrak{a}_i\}$$

*y se llama la **suma** de los ideales $\mathfrak{a}_i$. Es el mínimo ideal en $A$ que contiene a $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$.*

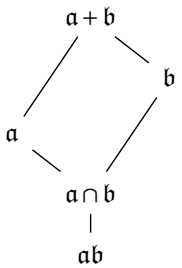
2) *El ideal generado por los productos $x_1 \cdots x_n$ donde $x_i \in \mathfrak{a}_i$ coincide con el conjunto*

$$\mathfrak{a}_1 \cdots \mathfrak{a}_n := \{\textit{sumas finitas } \sum_i x_{i_1} \cdots x_{i_n} \mid x_{i_k} \in \mathfrak{a}_k\}$$

*y se llama el **producto** de los ideales $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$. Además, se tiene*

$$\mathfrak{a}_1 \cdots \mathfrak{a}_n \subseteq \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n.$$

□



**4.5.2. Observación.** *Sean $A$ un anillo conmutativo y $\mathfrak{a}, \mathfrak{b}, \mathfrak{c} \subseteq A$ ideales. Tenemos las siguientes propiedades.*

*1)* $\mathfrak{a} + \mathfrak{b} = \mathfrak{b} + \mathfrak{a}$;

*2)* $\mathfrak{a}\mathfrak{b} = \mathfrak{b}\mathfrak{a}$;

*3)* $(\mathfrak{a} + \mathfrak{b}) + \mathfrak{c} = \mathfrak{a} + (\mathfrak{b} + \mathfrak{c}) = \mathfrak{a} + \mathfrak{b} + \mathfrak{c}$;

*4)* $(\mathfrak{a}\mathfrak{b})\mathfrak{c} = \mathfrak{a}(\mathfrak{b}\mathfrak{c}) = \mathfrak{a}\mathfrak{b}\mathfrak{c}$;

*5)* $(\mathfrak{a} + \mathfrak{b})\mathfrak{c} = \mathfrak{a}\mathfrak{c} + \mathfrak{b}\mathfrak{c}$;

*6)* $\mathfrak{a} + 0 = \mathfrak{a}$;

*7)* $\mathfrak{a} + A = A$;

*8)* $\mathfrak{a} \cdot 0 = 0$;

*9)* $\mathfrak{a} \cdot A = \mathfrak{a}$. □

Algunas de estas propiedades se ven como los axiomas de anillo conmutativo. Lo que falta son los elementos opuestos "$-\mathfrak{a}$" tales que $\mathfrak{a} + (-\mathfrak{a}) = 0$. En efecto, si tuvieramos los opuestos, entonces la identidad $A + A = A$ implicaría $A = 0$.

Ya que tenemos productos de ideales, podemos definir potencias $\mathfrak{a}^n$.

**4.5.3. Definición.** Sea $A$ un anillo conmutativo y sea $\mathfrak{a} \subseteq A$ un ideal. Para $n = 1, 2, 3, \ldots$ la $n$-ésima potencia de $\mathfrak{a}$ se define mediante

$$\mathfrak{a}^n := \underbrace{\mathfrak{a} \cdots \mathfrak{a}}_{n} = \{\text{sumas finitas } \sum_i x_{i_1} \cdots x_{i_n} \mid x_{i_k} \in \mathfrak{a}\}$$

que es equivalente a la definición inductiva

$$\mathfrak{a}^1 := \mathfrak{a}, \quad \mathfrak{a}^n := \mathfrak{a} \cdot \mathfrak{a}^{n-1}.$$

**4.5.4. Ejemplo.** Para los ideales principales se tiene para cualesquiera $x_1, \ldots, x_n \in A$

$$(x_1) + \cdots + (x_n) = (x_1, \ldots, x_n),$$
$$(x_1) \cdots (x_n) = (x_1 \cdots x_n).$$

Recordemos que en un dominio de ideales principales se tiene

$$(x_1) + \cdots + (x_n) = (\text{mcd}(x_1, \ldots, x_n)),$$
$$(x_1) \cap \cdots \cap (x_n) = (\text{mcm}(x_1, \ldots x_n)).$$ ▲

**4.5.5. Ejemplo.** Sea $k$ un cuerpo y sea $k[X]$ el anillo de polinomios correspondiente. El ideal generado por $X$ en $k[X]$ viene dado por

$$\mathfrak{a} := (X) = \{f \in k[X] \mid \deg f \geq 1\} \cup \{0\}.$$

Luego,

$$\mathfrak{a}^n = (X^n) = \{f \in k[X] \mid \deg f \geq n\} \cup \{0\}.$$ ▲

**4.5.6. Ejemplo.** Para un número primo $p$, en el anillo $\mathbb{Z}[X]$ consideremos el ideal $\mathfrak{a} := (p, X)$ generado por los elementos $p$ y $X$. Es el ideal de los polinomios con el término constante divisible por $p$:

$$(p, X) = \{f \cdot p + g \cdot X \mid f, g \in \mathbb{Z}[X]\} = \{a_n X^n + a_{n-1} X + \cdots + a_1 X + a_0 \mid a_i \in \mathbb{Z},\ p \mid a_0\}.$$

Luego,

$$\mathfrak{a}^2 = \left\{\text{sumas finitas } \sum_i f_i g_i \;\middle|\; f_i, g_i \in \mathfrak{a}\right\}.$$

En particular, dado que $p \in \mathfrak{a}$ y $X \in \mathfrak{a}$, tenemos $p^2, X^2 \in \mathfrak{a}^2$, y por lo tanto $X^2 + p^2 \in \mathfrak{a}^2$. Notamos que el polinomio $X^2 + p^2$ no puede ser escrito como un producto $fg$ donde $f, g \in \mathfrak{a}$. ▲

## 4.6 Teorema chino del resto

Recordemos que en el capítulo 1 hemos definido los productos de anillos $A_1 \times \cdots \times A_n$ como productos cartesianos con operaciones término por término. El teorema chino del resto en la teoría de números elemental dice que si $a$ y $b$ son números coprimos, entonces para todo entero $x$ su resto módulo $ab$ está definido de modo único por sus restos módulo $a$ y $b$. Precisamente, hay un isomorfismo de anillos

$$\mathbb{Z}/ab\mathbb{Z} \xrightarrow{\cong} \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}, \quad [x]_{ab} \mapsto ([x]_a, [x]_b).$$

En esta sección vamos a generalizar este resultado a anillos conmutativos.

**4.6.1. Lema.** *Sea $A$ un anillo conmutativo y sean $\mathfrak{a}_1, \ldots, \mathfrak{a}_n \subseteq A$ ideales tales que $\mathfrak{a}_i + \mathfrak{a}_j = A$ para $i \neq j$. Luego,*

*1)* $\mathfrak{a}_1 + \mathfrak{a}_2\mathfrak{a}_3\cdots\mathfrak{a}_n = A$;

*2)* $\mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n = \mathfrak{a}_1 \cdots \mathfrak{a}_n$.

*Demostración.* Tenemos

$$A = \underbrace{A \cdots A}_{n-1} = (\mathfrak{a}_1 + \mathfrak{a}_2)(\mathfrak{a}_1 + \mathfrak{a}_3)\cdots(\mathfrak{a}_1 + \mathfrak{a}_n) = \mathfrak{a} + \mathfrak{a}_2\mathfrak{a}_3\cdots\mathfrak{a}_n,$$

donde $\mathfrak{a} \subseteq \mathfrak{a}_1$. De hecho, al desarrollar el producto de sumas de ideales, se ve que todos los términos pertenecen a $\mathfrak{a}_1$, salvo el último término $\mathfrak{a}_2\mathfrak{a}_3\cdots\mathfrak{a}_n$. Esto nos permite concluir que

$$\mathfrak{a}_1 + \mathfrak{a}_2\mathfrak{a}_3\cdots\mathfrak{a}_n = A.$$

En la parte 2), la inclusión que se cumple en cualquier caso es $\mathfrak{a}_1 \cdots \mathfrak{a}_n \subseteq \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n$, y hay que probar la inclusión inversa. Procedamos por inducción sobre $n$. Supongamos que $n = 2$ e $\mathfrak{a}_1 + \mathfrak{a}_2 = A$. Luego, existen $y \in \mathfrak{a}_1$ y $z \in \mathfrak{a}_2$ tales que $y + z = 1$. Para todo $x \in \mathfrak{a}_1 \cap \mathfrak{a}_2$ se tiene

$$x = x(y + z) = xy + xz \in \mathfrak{a}_1\mathfrak{a}_2,$$

así que $\mathfrak{a}_1 \cap \mathfrak{a}_2 \subseteq \mathfrak{a}_1\mathfrak{a}_2$. Para $n > 2$, supongamos que el resultado se cumple para $n - 1$ ideales. Entonces,

$$\mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n = \mathfrak{a}_1 \cap (\mathfrak{a}_2 \cap \mathfrak{a}_3 \cap \cdots \cap \mathfrak{a}_n) = \mathfrak{a}_1 \cap \mathfrak{a}_2\mathfrak{a}_3\cdots\mathfrak{a}_n.$$

Sin embargo, $\mathfrak{a}_1 + \mathfrak{a}_2\mathfrak{a}_3\cdots\mathfrak{a}_n = A$ según la parte 1), así que $\mathfrak{a}_1 \cap \mathfrak{a}_2\mathfrak{a}_3\cdots\mathfrak{a}_n = \mathfrak{a}_1\mathfrak{a}_2\mathfrak{a}_3\cdots\mathfrak{a}_n$ por el caso de dos ideales. ■

**4.6.2. Teorema chino del resto**. *Sea $A$ un anillo conmutativo y sean $\mathfrak{a}_1, \ldots, \mathfrak{a}_n \subseteq A$ ideales tales que $\mathfrak{a}_i + \mathfrak{a}_j = A$ para $i \neq j$. Luego, hay un isomorfismo natural*

$$A/(\mathfrak{a}_1 \cdots \mathfrak{a}_n) \xrightarrow{\cong} A/\mathfrak{a}_1 \times \cdots \times A/\mathfrak{a}_n,$$
$$x + \mathfrak{a}_1 \cdots \mathfrak{a}_n \mapsto (x + \mathfrak{a}_1, \ldots, x + \mathfrak{a}_n).$$

*Demostración.* Consideremos el homomorfismo de anillos

$$\phi\colon A \to A/\mathfrak{a}_1 \times \cdots \times A/\mathfrak{a}_n,$$
$$x \mapsto (x + \mathfrak{a}_1, \ldots, x + \mathfrak{a}_n).$$

Vamos a probar que es sobreyectivo y su núcleo es igual al producto de ideales $\mathfrak{a}_1 \cdots \mathfrak{a}_n$.

Para ver la sobreyectividad, necesitamos probar que para cualesquiera $x_1, \ldots, x_n \in A$ existe $x \in \mathfrak{a}$ tal que $x \equiv x_i \pmod{\mathfrak{a}_i}$ para todo $i = 1, \ldots, n$. Según la parte 1) del lema de arriba,

$$\mathfrak{a}_1 + \mathfrak{a}_2\mathfrak{a}_3\cdots\mathfrak{a}_n = A,$$

y en particular, existen $z_1 \in \mathfrak{a}_1$ e $y_1 \in \mathfrak{a}_2\mathfrak{a}_3\cdots\mathfrak{a}_n$ tales que $z_1 + y_1 = 1$. Tenemos entonces $y_1 \equiv 1 \pmod{\mathfrak{a}_1}$ e $y_1 \equiv 0 \pmod{\mathfrak{a}_i}$ para $i \neq 1$. Usando el mismo argumento, podemos ver que existen $y_2, \ldots, y_n$ que satisfacen

$$y_i \equiv 1 \pmod{\mathfrak{a}_i}, \quad y_i \equiv 0 \pmod{\mathfrak{a}_j} \text{ si } j \neq i.$$

El elemento

$$x := x_1 y_1 + \cdots + x_n y_n$$

cumple la condición deseada $x \equiv x_i \pmod{\mathfrak{a}_i}$ para todo $i = 1, \ldots, n$.

Ahora está claro que

$$\ker \phi = \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n,$$

y luego por la parte 2) del lema anterior,

$$\mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n = \mathfrak{a}_1 \cdots \mathfrak{a}_n. \qquad \blacksquare$$

Notamos que en un dominio de ideales principales $A$ se tiene $(a) + (b) = (a, b) = (\mathrm{mcd}(a, b))$, así que la condición $(a) + (b) = A$ es equivalente a $\mathrm{mcd}(a, b) = 1$.

**4.6.3. Corolario.** *Si $a_1, \ldots, a_n$ son números coprimos dos a dos, entonces hay un isomorfismo de anillos*

$$\mathbb{Z}/(a_1 \cdots a_n)\mathbb{Z} \xrightarrow{\cong} \mathbb{Z}/a_1\mathbb{Z} \times \cdots \times \mathbb{Z}/a_n\mathbb{Z},$$
$$[x]_{a_1 \cdots a_n} \mapsto ([x]_{a_1}, \ldots, [x]_{a_n}).$$

**4.6.4. Ejemplo.** En el anillo de los enteros de Gauss $\mathbb{Z}[i]$ se tiene $5 = (1+2i)(1-2i)$, donde $1+2i$ y $1-2i$ son dos primos no asociados entre sí. En particular, $(1+2i) + (1-2i) = \mathbb{Z}[i]$. Entonces, gracias al teorema chino del resto,

$$\mathbb{Z}[i]/(5) \cong \mathbb{Z}[i]/(1+2i) \times \mathbb{Z}[i]/(1-2i) \cong \mathbb{F}_5 \times \mathbb{F}_5.$$

Notamos que $\mathbb{Z}[i]/(5) \cong \mathbb{F}_5[X]/(X^2+1)$ (haga el ejercicio 4.11). El polinomio $X^2+1$ es reducible en $\mathbb{F}_5[X]$: se tiene

$$X^2 + 1 = (X-2)(X-3).$$

Luego,

$$\mathbb{F}_5[X]/(X^2+1) \cong \mathbb{F}_5[X]/(X-2) \times \mathbb{F}_5[X]/(X-3) \cong \mathbb{F}_5 \times \mathbb{F}_5. \qquad \blacktriangle$$

## 4.7 Propiedades universales (♣)

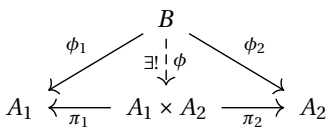
Todas las construcciones en álgebra se caracterizan por sus propiedades universales. En esta sección vamos a formular las propiedades universales del producto de anillos, cuerpo de fracciones, anillo de polinomios y anillo cociente. Las ideas subyacentes son conceptualmente nuevas y representan otro nivel más de abstracción, así que uno necesita paciencia para acostumbrarse a ellas. En este punto el lector puede regresar a la breve discusión de propiedades universales en el capítulo 0.

**4.7.1. Proposición (Propiedad universal del producto).** *Sean $A_1$ y $A_2$ anillos y $B$ cualquier otro anillo. Para todo par de homomorfismos $\phi_1 \colon B \to A_1$ y $\phi_2 \colon B \to A_2$ existe un único homomorfismo $\phi \colon B \to A_1 \times A_2$ tal que*

$$\pi_1 \circ \phi = \phi_1, \quad \pi_2 \circ \phi = \phi_2.$$

*donde $\pi_1$ y $\pi_2$ denotan los homomorfismos de proyección*

$$\begin{array}{ccccc} A_1 & \xleftarrow{\pi_1} & A_1 \times A_2 & \xrightarrow{\pi_2} & A_2 \\ a_1 & \longleftarrow & (a_1, a_2) & \longmapsto & a_2 \end{array}$$



*Demostración.* Las condiciones $\pi_1 \circ \phi = \phi_1$ y $\pi_2 \circ \phi = \phi_2$ implican que la aplicación $\phi$ necesariamente viene dada por

$$\phi(b) = (\phi_1(b), \phi_2(b)).$$

Puesto que $\phi_1$ y $\phi_2$ son homomorfismos, esta fórmula también define un homomorfismo. ■

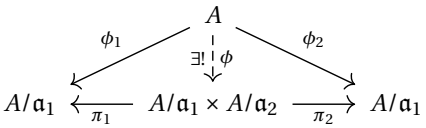
Dejo al lector formular la propiedad similar para los productos arbitrarios $\prod_i A_i$, y también verificar que la propiedad universal define el producto de modo único salvo isomorfismo. Para esto véase la discusión de propiedades universales en el capítulo 0.

**4.7.2. Ejemplo.** Para un anillo conmutativo $A$ y dos ideales $\mathfrak{a}_1, \mathfrak{a}_2 \subseteq A$ la propiedad universal nos dice que los homomorfismos

$$\begin{array}{ccccc} A/\mathfrak{a}_1 & \xleftarrow{\phi_1} & A & \xrightarrow{\phi_2} & A/\mathfrak{a}_2 \\ x+\mathfrak{a}_1 & \longleftarrow\!\shortmid & x & \longmapsto & x+\mathfrak{a}_2 \end{array}$$

inducen un homomorfismo

$$\phi\colon A \to A/\mathfrak{a}_1 \times A/\mathfrak{a}_2.$$




Este homomorfismo apareció en la prueba del teorema chino del resto. ▲

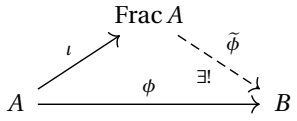
**4.7.3. Proposición (Propiedad universal del cuerpo de fracciones).** *Sean $A$ un dominio,* $\operatorname{Frac} A$ *su cuerpo de fracciones y*

$$\iota\colon A \to \operatorname{Frac} A, \quad a \mapsto \frac{a}{1}$$

*el homomorfismo inyectivo correspondiente.*

1) *Se cumple $\iota(a) \in (\operatorname{Frac} A)^\times$ para todo $a \neq 0$.*

2) *Si $B$ es otro anillo conmutativo y $\phi\colon A \to B$ un homomorfismo tal que $\phi(a) \in B^\times$ para todo $a \neq 0$, entonces existe un único homomorfismo $\tilde{\phi}\colon \operatorname{Frac} A \to B$ tal que $\iota \circ \tilde{\phi} = \phi$.*




*Demostración.* Tenemos necesariamente

$$\tilde{\phi}\left(\frac{a}{b}\right) = \tilde{\phi}\left(\frac{a}{1}\right)\tilde{\phi}\left(\left(\frac{b}{1}\right)^{-1}\right) = \tilde{\phi}\left(\frac{a}{1}\right)\tilde{\phi}\left(\frac{b}{1}\right)^{-1} = \phi(a)\,\phi(b)^{-1}.$$

Por otra parte, se comprueba fácilmente que esta fórmula define un homomorfismo. ■

Intuitivamente, la propiedad de arriba significa que $\operatorname{Frac} A$ es el anillo más pequeño donde todos los elementos no nulos de $A$ se vuelven invertibles. Aquí "más pequeño" significa que todo homomorfismo $\phi\colon A \to B$ que invierte todos los elementos no nulos de $A$ se factoriza de manera única por $\operatorname{Frac} A$.

**4.7.4. Ejemplo.** Consideremos el anillo de los enteros de Gauss $\mathbb{Z}[i]$ y el cuerpo

$$\mathbb{Q}(i) := \{x + iy \mid x, y \in \mathbb{Q}\} \subset \mathbb{C}.$$

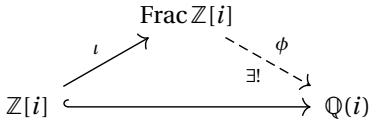
Tenemos la inclusión natural $\mathbb{Z}[i] \hookrightarrow \mathbb{Q}(i)$. Ahora todo homomorfismo $\phi\colon \mathbb{Z}[i] \to B$ que cumple la propiedad de que $\phi(\alpha) \in B^\times$ para $\alpha \neq 0$, se extiende de modo único a $\mathbb{Q}(i)$:

$$\widetilde{\phi}\Big(\frac{a}{b} + \frac{c}{d}\,i\Big) = \widetilde{\phi}((ad + bci)\,(bd)^{-1}) = \widetilde{\phi}(ad + bci)\,\widetilde{\phi}(bd)^{-1} = \phi(ad + bci)\,\phi(bd)^{-1}$$

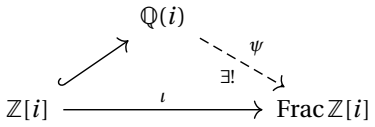
(y una verificación tediosa nos diría que esta fórmula define un homomorfismo). Entonces, la inclusión $\mathbb{Z}[i] \hookrightarrow \mathbb{Q}(i)$ cumple la misma propiedad universal que $\iota\colon \mathbb{Z}[i] \to \operatorname{Frac}\mathbb{Z}[i]$, y se puede deducir que esto nos da un isomorfismo

$$\mathbb{Q}(i) \cong \operatorname{Frac}\mathbb{Z}[i].$$

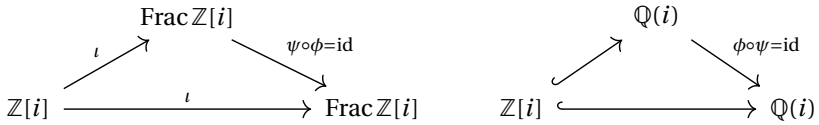
En efecto, aplicando la propiedad universal de $\operatorname{Frac}\mathbb{Z}[i]$ a $\mathbb{Z}[i] \hookrightarrow \mathbb{Q}(i)$, se obtiene




y viceversa, aplicando la propiedad universal de $\mathbb{Q}(i)$ a $\iota\colon \mathbb{Z}[i] \to \operatorname{Frac}\mathbb{Z}[i]$, se obtiene




Ahora las propiedades universales de $\operatorname{Frac}\mathbb{Z}[i]$ y $\mathbb{Q}(i)$ implican que $\phi$ y $\psi$ son mutualmente inversos.




Por supuesto, el isomorfismo en cuestión esta claro desde el principio:

$$\mathbb{Q}(i) \xrightarrow{\cong} \operatorname{Frac}\mathbb{Z}[i],$$
$$\frac{a}{b} + \frac{c}{d}\,i \mapsto \frac{ad + bci}{bd}.$$

▲

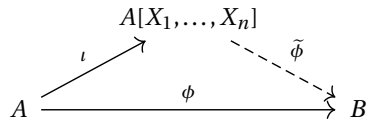
**4.7.5. Proposición (Propiedad universal del anillo de polinomios).** *Para un anillo conmutativo $A$ sean $A[X_1, \ldots, X_n]$ el anillo de polinomios en $n$ variables y*

$$\iota\colon A \to A[X_1, \ldots, X_n]$$

*la inclusión de los polinomios constantes. Dado otro anillo conmutativo $B$, un homomorfismo $\phi\colon A \to B$ y elementos $b_1, \ldots, b_n \in B$, existe un único homomorfismo*

$$\widetilde{\phi}\colon A[X_1, \ldots, X_n] \to B$$

*tal que $\widetilde{\phi} \circ \iota = \phi$ y $\phi(X_i) = b_i$ para todo $i = 1, \ldots, n$.*



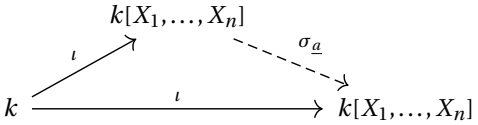
*Demostración.* Puesto que $\widetilde{\phi}$ tiene que ser un homomorfismo, tenemos necesariamente

$$\widetilde{\phi}\Big(\sum_{i_1,\dots,i_n\geq 0} a_{i_1,\dots,i_n} X_1^{i_1}\cdots X_n^{i_n}\Big) = \sum_{i_1,\dots,i_n\geq 0} \widetilde{\phi}(\iota(a_{i_1,\dots,i_n}))\,\widetilde{\phi}(X_1^{i_1})\cdots\widetilde{\phi}(X_n^{i_n})$$
$$= \sum_{i_1,\dots,i_n\geq 0} \phi(a_{i_1,\dots,i_n})\, b_1^{i_1}\cdots b_n^{i_n}.$$

Es fácil verificar que esta fórmula define un homomorfismo, puesto que $\phi$ lo es. ■

**4.7.6. Ejemplo.** Hemos usado esta propiedad de manera implícita cuando estábamos hablando de los homomorfismos de evaluación de polinomios. Para dar un ejemplo práctico, sean $k$ un cuerpo y $k[X_1,\dots,X_n]$ el anillo de polinomios en $n$ variables. Notamos que para $a_1,\dots,a_n \in k$ existe un único homomorfismo que envía las constantes a las mismas constantes y $X_i$ a $X_i - a_i$:

$$\sigma_{\underline{a}}\colon k[X_1,\dots,X_n] \to k[X_1,\dots,X_n],$$
$$X_i \mapsto X_i - a_i.$$




Este es un *automorfismo*: el homomorfismo inverso viene dado por

$$\sigma_{\underline{a}}^{-1}\colon k[X_1,\dots,X_n] \to k[X_1,\dots,X_n],$$
$$X_i \mapsto X_i + a_i.$$

La misma propiedad universal define el homomorfismo $ev_{\underline{0}}\colon k[X_1,\dots,X_n] \to k$ que envía un polinomio $f$ a su término constante $f(0,\dots,0)$:

$$ev_{\underline{0}}\colon k[X_1,\dots,X_n] \to k,$$
$$X_i \mapsto 0.$$

Está claro que el núcleo de $ev_{\underline{0}}$ consiste en los polinomios sin término constante, que es precisamente el ideal generado por las variables $X_1,\dots,X_n$:

$$\ker ev_{\underline{0}} = \{f \mid f(0)=0\} = \{f_1X_1+\cdots+f_nX_n \mid f_i \in k[X_1,\dots,X_n]\} = (X_1,\dots,X_n).$$

De la misma manera, podemos evaluar un polinomio en $a_1,\dots,a_n$:

$$ev_{\underline{a}}\colon k[X_1,\dots,X_n] \to k,$$
$$X_i \mapsto a_i.$$

En este caso tal vez no está tan claro cuál es el núcleo de este homomorfismo. Sin embargo, podemos notar que $ev_{\underline{0}} = ev_{\underline{a}} \circ \sigma_{\underline{a}}$, y luego

$$\ker ev_{\underline{a}} = \{f \mid ev_{\underline{a}}(f)=0\} = \{f \mid ev_{\underline{0}}(\sigma_{\underline{a}}^{-1}(f))=0\} = \{f \mid \sigma_{\underline{a}}^{-1}(f) \in \ker ev_{\underline{0}}\}$$
$$= \{f \mid f \in \sigma_{\underline{a}}(\ker ev_{\underline{0}})\} = \sigma_{\underline{a}}(\ker ev_{\underline{0}}).$$

Entonces,

$$\ker ev_{\underline{a}} = \sigma_{\underline{a}}((X_1,\dots,X_n)) = \{\sigma_{\underline{a}}(f_1)\,\sigma_{\underline{a}}(X_1)+\cdots+\sigma_{\underline{a}}(f_n)\,\sigma_{\underline{a}}(X_n) \mid f_i \in k[X_1,\dots,X_n]\}$$
$$= \{g_1(X_1-a_1)+\cdots+g_n(X_n-a_n) \mid g_i \in k[X_1,\dots,X_n]\} = (X_1-a_1,\dots,X_n-a_n).$$

En fin, notamos que el primer teorema de isomorfia implica que

$$k[X_1,\dots,X_n]/(X_1-a_1,\dots,X_n-a_n) \cong k.$$ ▲

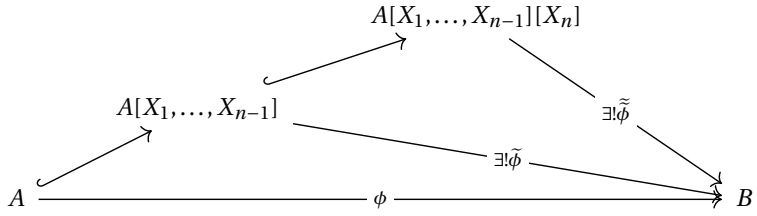
**4.7.7. Ejemplo.** Consideremos el anillo

$$A[X_1,\dots,X_{n-1}][X_n]$$

que consiste en los polinomios $\sum_{i\geq 0} f_i X_n^i$, donde $f_i \in A[X_1,\dots,X_{n-1}]$. Tenemos las inclusiones de los polinomios constantes

$$A \hookrightarrow A[X_1,\dots,X_{n-1}] \hookrightarrow A[X_1,\dots,X_{n-1}][X_n].$$

Ahora dado un homomorfismo $\phi\colon A \to B$ y $b_1,\dots,b_n \in B$, primero $\phi$ se levanta de manera única a un homomorfismo $\widetilde{\phi}\colon A[X_1,\dots,X_{n-1}] \to B$ tal que $\widetilde{\phi}(X_i) = b_i$ para $i = 1,\dots,n-1$, y luego $\widetilde{\phi}$ se levanta a un homomorfismo $\widetilde{\widetilde{\phi}}\colon A[X_1,\dots,X_{n-1}][X_n] \to B$ tal que $\widetilde{\widetilde{\phi}}(X_n) = b_n$.




Esto significa que $A[X_1,\dots,X_{n-1}][X_n]$ tiene la misma propiedad universal que $A[X_1,\dots,X_n]$, de donde de manera formal se deduce un isomorfismo canónico

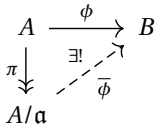
$$A[X_1,\dots,X_{n-1}][X_n] \cong A[X_1,\dots,X_n].$$

Sin embargo, este isomorfismo nada más significa que un polinomio en las variables $X_1,\dots,X_n$ puede ser escrito como $\sum_{i\geq 0} f_i X_n^i$, donde $f_i \in A[X_1,\dots,X_{n-1}]$. ▲

**4.7.8. Proposición (Propiedad universal del anillo cociente).** *Sean $\mathfrak{a} \subseteq A$ un ideal y*

$$\pi\colon A \to A/\mathfrak{a}, \quad x \mapsto \overline{x}$$

*el homomorfismo de proyección sobre el anillo cociente. Si $\phi\colon A \to B$ es un homomorfismo de anillos tal que $\mathfrak{a} \subseteq \ker\phi$, entonces $\phi$ se factoriza de modo único por $A/\mathfrak{a}$: existe un único homomorfismo $\overline{\phi}\colon A/\mathfrak{a} \to B$ tal que $\phi = \overline{\phi}\circ\pi$.*




*Demostración.* La flecha punteada $\overline{\phi}$ es necesariamente $\overline{x} \mapsto \phi(x)$. Es una aplicación bien definida: si $x \equiv x' \pmod{\mathfrak{a}}$ para algunos $x, x' \in A$, entonces $x - x' \in \mathfrak{a}$, luego $x - x' \in \ker f$ y

$$\phi(x - x') = 0 \iff \phi(x) = \phi(x').$$

La aplicación $\overline{\phi}$ es un homomorfismo de anillos, puesto que $\phi$ lo es. ■

Notamos que la propiedad universal del anillo cociente está detrás del primer teorema de isomorfía.

**4.7.9. Ejemplo.** Para $n = 1,2,3,\dots$ consideremos el homomorfismo

$$\pi_n\colon \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, \quad a \mapsto [a]_n.$$

Su núcleo consiste en los múltiplos de $n$. En particular, si $n \mid m$, entonces $m\mathbb{Z} \subseteq \ker\pi$, así que $\pi$ induce un homomorfismo

$$\pi_{m,n}\colon \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, \quad [a]_m \to [a]_n.$$ ▲

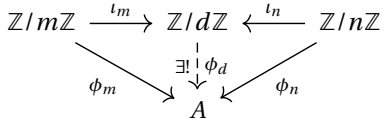
**4.7.10. Ejemplo.** Para dos números naturales $m$ y $n$, sea $d = \mathrm{mcd}(m, n)$. Tenemos entonces homomorfismos de anillos

$$\iota_m \colon \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/d\mathbb{Z}, \quad \iota_n \colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/d\mathbb{Z}.$$

Ahora para cualquier otro anillo conmutativo $A$ existen homomorfismos únicos

$$\phi_m \colon \mathbb{Z}/m\mathbb{Z} \to A, \quad \phi_n \colon \mathbb{Z}/m\mathbb{Z} \to A$$

si y solo si $m \cdot 1_A = n \cdot 1_A = 0$. En este caso $d \cdot 1_A = 0$, lo que nos da un único homomorfismo $\phi_d \colon \mathbb{Z}/d\mathbb{Z} \to A$. Notamos que este homomorfismo hace parte del diagrama conmutativo




Entonces, el anillo $\mathbb{Z}/d\mathbb{Z}$ tiene la propiedad universal parecida a la propiedad universal del producto $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, *solo con todas las flechas al revés*. El objeto caracterizado por tal propiedad se llama el **producto tensorial** de anillos y se denota por $\otimes$. Entonces,

$$\mathbb{Z}/m\mathbb{Z} \otimes \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/d\mathbb{Z}.$$

En el segundo semestre vamos a dar la definición y construcción general de productos tensoriales. Por el momento es bueno saber que existe una construcción con la propiedad *dual* a la del producto. ▲

**4.7.11. Ejemplo.** Sea $k$ un cuerpo. La propiedad universal del anillo de polinomios $k[X, Y, Z]$ nos da un homomorfismo

$$\phi \colon k[X, Y, Z] \to k[T], \quad X \mapsto T,\ Y \mapsto T^2,\ Z \mapsto T^3.$$

Notamos que los polinomios $X^2 - Y$ e $X^3 - Z$ están en el núcleo de $\phi$. Esto implica que el ideal generado por estos polinomios pertenece al núcleo:

$$(X^2 - Y, X^3 - Z) \subseteq \ker \phi.$$

En realidad, se cumple la igualdad, pero ¿cómo justificarlo? Gracias a la propiedad universal del anillo cociente, $\phi$ induce un homomorfismo desde el anillo cociente

$$\overline{\phi} \colon k[X, Y, Z]/(X^2 - Y, X^3 - Z) \to k[T], \quad \overline{X} \mapsto T,\ \overline{Y} \mapsto T^2,\ \overline{Z} \mapsto T^3.$$

Viceversa, la propiedad universal del anillo de polinomios $k[T]$ nos da un homomorfismo

$$\psi \colon k[T] \to k[X, Y, Z]/(X^2 - Y, X^3 - Z), \quad T \mapsto \overline{X}.$$

Notamos que

$$\psi(\overline{\phi}(\overline{X})) = \overline{X}, \quad \psi(\overline{\phi}(\overline{Y})) = \overline{Y}, \quad \psi(\overline{\phi}(\overline{Z})) = \overline{Z}$$

y también

$$\overline{\phi}(\psi(T)) = T.$$

Entonces, $\overline{\phi}$ y $\psi$ son mutualmente inversos y nos dan un isomorfismo

$$k[X, Y, Z]/(X^2 - Y, X^3 - Z) \cong k[T].$$

La curva en el espacio tridimensional definida por las ecuaciones $y = x^2$, $z = x^3$ se llama la **cúbica torcida**. El lector puede tratar de visualizarla. ▲

## 4.8 Ejercicios

**Ejercicio 4.1.** Sea $\phi\colon A \to B$ un homomorfismo de anillos. Determine cuáles de las siguientes afirmaciones son ciertas. Justifique sus respuestas (encuentre una prueba o contraejemplo).

a) Si $a \in A$ es un nilpotente, entonces $\phi(a) \in B$ es también un nilpotente.

b) Si $a \in A$ es un idempotente, entonces $\phi(a) \in B$ es también un idempotente.

c) Si $a \in A$ es un divisor de cero, entonces $\phi(a) \in B$ es también un divisor de cero.

**Ejercicio 4.2.** Demuestre que el conjunto

$$A := \left\{ \begin{pmatrix} x & -y \\ y & x \end{pmatrix} \middle| x, y \in \mathbb{R} \right\}$$

es un subanillo del anillo de matrices $M_2(\mathbb{R})$. Encuentre un isomorfismo $A \cong \mathbb{C}$.

**Ejercicio 4.3.** Para un anillo no conmutativo $A$ definamos su **centro** como

$$Z(A) := \{x \in A \mid ax = xa \text{ para todo } a \in A\}.$$

1) Demuestre que $Z(A)$ es un subanillo de $A$.

2) Demuestre que si $\phi\colon A \to B$ es un homomorfismo sobreyectivo, entonces $\phi(Z(A)) \subseteq Z(B)$.

**Ejercicio 4.4.** Demuestre que los anillos de polinomios $\mathbb{Z}[X]$ y $\mathbb{Q}[X]$ no son isomorfos.
*Sugerencia: demuestre que un isomorfismo de anillos $\phi\colon A \xrightarrow{\cong} B$ induce una biyección $A^\times \xrightarrow{\cong} B^\times$.*

**Ejercicio 4.5.** Escriba la tabla de adición y multiplicación en el anillo cociente $\mathbb{F}_3[X]/(X^2+1)$. Demuestre que este es un cuerpo de 9 elementos.

**Ejercicio 4.6.** Demuestre que el anillo cociente $\mathbb{Z}[i]/(1+2i)$ es isomorfo al cuerpo de 5 elementos $\mathbb{F}_5$. (Describa los elementos y encuentre un isomorfismo explícito con $\mathbb{F}_5$.)

**Ejercicio 4.7 (Segundo teorema de isomorfía).** Sean $A$ un anillo conmutativo, $B \subseteq A$ un subanillo y $\mathfrak{a} \subseteq A$ un ideal.

1) Demuestre que $B + \mathfrak{a} := \{x + y \mid x \in B, y \in \mathfrak{a}\}$ es un subanillo de $A$ y que $\mathfrak{a}$ es un ideal en $B + \mathfrak{a}$.

2) Demuestre que la aplicación
$$\phi\colon B \to (B+\mathfrak{a})/\mathfrak{a}, \quad x \mapsto \overline{x}$$
es un homomorfismo sobreyectivo.

3) Demuestre que $\ker\phi = B \cap \mathfrak{a}$.

4) Deduzca que $B/(B \cap \mathfrak{a}) \cong (B+\mathfrak{a})/\mathfrak{a}$.

**Ejercicio 4.8 (Tercer teorema de isomorfía).** Sean $A$ un anillo y $\mathfrak{a} \subseteq \mathfrak{b} \subseteq A$ ideales.

1) Demuestre que la aplicación
$$\phi\colon A/\mathfrak{a} \to A/\mathfrak{b}, \quad x + \mathfrak{a} \mapsto x + \mathfrak{b}$$
está bien definida y es un homomorfismo sobreyectivo.

2) Demuestre que $\ker\phi = \mathfrak{b}/\mathfrak{a} := \{x + \mathfrak{a} \mid x \in \mathfrak{b}\} \subseteq A/\mathfrak{a}$.

3) Deduzca que $(A/\mathfrak{a})/(\mathfrak{b}/\mathfrak{a}) \cong A/\mathfrak{b}$.

**Ejercicio 4.9.** Para $n \neq 1$ un entero libre de cuadrados encuentre un isomorfismo

$$\mathbb{Q}[X]/(X^2 - n) \cong \mathbb{Q}(\sqrt{n}) := \{x + y\sqrt{n} \mid x, y \in \mathbb{Q}\}.$$

**Ejercicio 4.10.** Encuentre un isomorfismo $\mathbb{Z}[X]/(X^2+1) \cong \mathbb{Z}[i]$.

**Ejercicio 4.11.** Para un número primo $p$ encuentre un isomorfismo $\mathbb{F}_p[X]/(X^2+1) \cong \mathbb{Z}[i]/(p)$.

**Ejercicio 4.12.** Encuentre isomorfismos de anillos cociente

a) $\mathbb{F}_2[X]/(X^3 + X^2 + 1) \cong \mathbb{F}_2[X]/(X^3 + X + 1)$;

b) $\mathbb{F}_3[X]/(X^2 + 1) \cong \mathbb{F}_3[X]/(X^2 + X + 2)$.

**Ejercicio 4.13.** Encuentre los ideales en el anillo cociente $\mathbb{Z}[i]/(10)$ y las inclusiones entre ellos.

**Ejercicio 4.14 (Ideales maximales).** Sean $A$ un anillo conmutativo y $\mathfrak{m} \subsetneq A$ un ideal propio. Demuestre que las siguientes dos condiciones son equivalentes:

1) para cualquier otro ideal $\mathfrak{a}$ tal que $\mathfrak{m} \subseteq \mathfrak{a} \subseteq A$ se tiene $\mathfrak{a} = \mathfrak{m}$ o $\mathfrak{a} = A$;

2) el cociente $A/\mathfrak{m}$ es un cuerpo.

**Ejercicio 4.15 (Suma de ideales).** Sean $A$ un anillo conmutativo y $\mathfrak{a}_1, \ldots, \mathfrak{a}_n \subseteq A$ ideales. Demuestre que el ideal generado por los elementos de $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ coincide con el conjunto

$$\mathfrak{a}_1 + \cdots + \mathfrak{a}_n := \{x_1 + \cdots + x_n \mid x_i \in \mathfrak{a}_i\}.$$

**Ejercicio 4.16 (Producto de ideales).** Sean $A$ un anillo conmutativo y $\mathfrak{a}_1, \ldots, \mathfrak{a}_n \subseteq A$ ideales. Demuestre que el ideal generado por los productos $x_1 \cdots x_n$ donde $x_i \in \mathfrak{a}_i$ coincide con el conjunto

$$\mathfrak{a}_1 \cdots \mathfrak{a}_n := \{\text{sumas finitas } \sum_i x_{i_1} \cdots x_{i_n} \mid x_{i_k} \in \mathfrak{a}_k\}.$$

**Ejercicio 4.17.** Demuestre que $\mathfrak{a}_1 \cdots \mathfrak{a}_n \subseteq \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n$.

**Ejercicio 4.18.** Demuestre que para los ideales principales se tiene para cualesquiera $x_1, \ldots, x_n \in A$

$$(x_1) + \cdots + (x_n) = (x_1, \ldots, x_n),$$
$$(x_1) \cdots (x_n) = (x_1 \cdots x_n).$$

**Ejercicio 4.19.** Sean $A$ un anillo conmutativo y $\mathfrak{a}, \mathfrak{b}, \mathfrak{c} \subseteq A$ ideales. Demuestre que el producto de ideales es distributivo respecto a la suma:

$$(\mathfrak{a} + \mathfrak{b})\mathfrak{c} = \mathfrak{a}\mathfrak{c} + \mathfrak{b}\mathfrak{c}.$$

**Ejercicio 4.20.** Demuestre que si

$$\mathfrak{a} = (x_1, \ldots, x_m), \quad \mathfrak{b} = (y_1, \ldots, y_n),$$

entonces

$$\mathfrak{a}\mathfrak{b} = (x_i y_j \mid i = 1, \ldots, m,\ j = 1, \ldots, n).$$

**Ejercicio 4.21.** Usando el teorema chino del resto, demuestre que el anillo cociente

$$\mathbb{F}_3[X]/(X^3 + X^2 + X + 1)$$

es isomorfo al producto $\mathbb{F}_9 \times \mathbb{F}_3$, donde $\mathbb{F}_9$ es un cuerpo de 9 elementos y $\mathbb{F}_3$ es un cuerpo de 3 elementos.

**Ejercicio 4.22.** Sea $p$ un primo impar. Demuestre que el anillo cociente $\mathbb{F}_p[X]/(X^2+1) \cong \mathbb{Z}[i]/(p)$ es isomorfo a

a) un cuerpo de $p^2$ elementos, o

b) el producto de cuerpos $\mathbb{F}_p \times \mathbb{F}_p$.

¿Para cuáles primos $p$ ocurre a) y para cuáles ocurre b)? ¿Qué sucede si $p = 2$?