# Capítulo 11
# Anillos

Ya introducimos anillos y cuerpos en el capítulo 3. Ahora vamos a estudiar otros conceptos relacionados y ver más detalles. Recordemos del capítulo 3 que un **anillo** $R$ es un conjunto dotado de dos operaciones $+$ (adición) y $\cdot$ (multiplicación) que satisfacen los siguientes axiomas.

R1) $R$ es un grupo abeliano respecto a $+$; es decir,

R1a) la adición es **asociativa**: para cualesquiera $x, y, z \in R$ tenemos

$$(x + y) + z = x + (y + z);$$

R1b) existe un elemento neutro aditivo $0 \in R$ (cero) tal que para todo $x \in R$ se cumple

$$0 + x = x = x + 0;$$

R1c) para todo $x \in R$ existe un elemento **opuesto** $-x \in R$ que satisface

$$(-x) + x = x + (-x) = 0;$$

R1d) la adición es **conmutativa**: para cualesquiera $x, y \in R$ se cumple

$$x + y = y + x;$$

R2) la multiplicación es **distributiva** respecto a la adición: para cualesquiera $x, y, z \in R$ se cumple

$$x \cdot (y + z) = xy + xz, \quad (x + y) \cdot z = xz + yz;$$

R3) la multiplicación es asociativa: para cualesquiera $x, y, z \in R$ tenemos

$$(x \cdot y) \cdot z = x \cdot (y \cdot z);$$

R4) existe un elemento neutro multiplicativo $1 \in R$ (identidad) tal que para todo $x \in R$ se cumple

$$1 \cdot x = x = x \cdot 1.$$

Además, si se cumple el axioma

R5) la multiplicación es conmutativa: para cualesquiera $x, y \in R$ se cumple

$$xy = yx.$$

se dice que $R$ es un **anillo conmutativo**. Al estudio de algunas propiedades especiales de anillos conmutativos estará dedicado el siguiente capítulo.

Advertencia para el lector: algunos libros de texto consideran anillos sin identidad (anillos que no satisfacen el axioma R4)), pero en este curso la palabra "anillo" siempre significa "anillo con identidad".

Recordemos algunos ejemplos de anillos que hemos visto.

1) Los números enteros $\mathbb{Z}$, racionales $\mathbb{Q}$, reales $\mathbb{R}$, complejos $\mathbb{C}$. Los últimos tres son **cuerpos**.

2) Para $n = 1, 2, 3, \ldots$ y para $p$ un número primo los conjuntos

$$\mathbb{Z}\Big[\frac{1}{n}\Big] := \Big\{ \frac{a}{n^k} \in \mathbb{Q} \;\Big|\; a \in \mathbb{Z},\ k = 0, 1, 2, \ldots \Big\}, \quad \mathbb{Z}_{(p)} := \Big\{ \frac{a}{b} \in \mathbb{Q} \;\Big|\; p \nmid b \Big\}$$

son anillos. Esto es un ejemplo de **localización** que vamos a estudiar más adelante en el curso.

3) El anillo $\mathbb{Z}/n\mathbb{Z}$ de los restos módulo $n$. Cuando $n = p$ es primo, $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ es un **cuerpo**.

4) Los anillos aritméticos como los **enteros de Gauss**

$$\mathbb{Z}[\sqrt{-1}] := \{a + b\sqrt{-1} \mid a, b \in \mathbb{Z}\}$$

los **enteros de Eisenstein**

$$\mathbb{Z}[\zeta_3] := \{a + b\,\zeta_3 \mid a, b \in \mathbb{Z}\}$$

(donde $\zeta_3 := e^{2\pi\sqrt{-1}/3}$) y el anillo

$$\mathbb{Z}[\sqrt{2}] := \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}.$$

5) El anillo de polinomios $R[X]$, donde $R$ es un anillo conmutativo.

Esta construcción puede ser generalizada al **anillo de polinomios en $n$ variables** $R[X_1, \ldots, X_n]$. En este caso los elementos son las expresiones formales de la forma

$$f = \sum_{i_1,\ldots,i_n \geq 0} a_{i_1,\ldots,i_n} X_1^{i_1} \cdots X_n^{i_n},$$

donde $a_{i_1,\ldots,i_n} = 0$, salvo un número finito de $(i_1, \ldots, i_n)$. Las sumas y productos están definidos por

$$\left( \sum_{i_1,\ldots,i_n \geq 0} a_{i_1,\ldots,i_n} X_1^{i_1} \cdots X_n^{i_n} \right) + \left( \sum_{i_1,\ldots,i_n \geq 0} b_{i_1,\ldots,i_n} X_1^{i_1} \cdots X_n^{i_n} \right) := \sum_{i_1,\ldots,i_n \geq 0} (a_{i_1,\ldots,i_n} + b_{i_1,\ldots,i_n})\, X_1^{i_1} \cdots X_n^{i_n}$$

y

$$\left( \sum_{i_1,\ldots,i_n \geq 0} a_{i_1,\ldots,i_n} X_1^{i_1} \cdots X_n^{i_n} \right) \cdot \left( \sum_{j_1,\ldots,j_n \geq 0} b_{j_1,\ldots,j_n} X_1^{j_1} \cdots X_n^{j_n} \right)$$

$$:= \sum_{k_1,\ldots,k_n \geq 0} \left( \sum_{\substack{(k_1,\ldots,k_n) = \\ (i_1,\ldots,i_n)+(j_1,\ldots,j_n)}} a_{i_1,\ldots,i_n}\, b_{j_1,\ldots,j_n} \right) X_1^{k_1} \cdots X_n^{k_n}.$$

6) Si quitamos la condición que $a_{i_1,\ldots,i_n} = 0$, salvo un número finito de $(i_1, \ldots, i_n)$, se obtiene el **anillo de las series formales de potencias en $n$ variables** $R[\![X_1, \ldots, X_n]\!]$.

7) Los anillos de matrices $M_n(R)$, donde $R$ es un anillo conmutativo.

Todos los anillos de arriba son conmutativos, salvo el anillo de matrices $M_n(R)$ para $n > 1$.

## 11.1 Subanillos

**11.1.1. Definición.** Sea $R$ un anillo. Se dice que un subconjunto $S \subseteq R$ es un **subanillo** de $R$ si

1) $S$ es un subgrupo abeliano de $R$ respecto a la adición,

2) $1 \in S$,

3) $S$ es cerrado respecto a la multiplicación: $xy \in S$ para cualesquiera $x, y \in S$.

El lector puede comprobar que en este caso $S$ es también un anillo respecto a las mismas operaciones que $R$.

**11.1.2. Ejemplo.** Sea $R$ un anillo conmutativo. Identificándolo con los polinomios constantes

$$\sum_{i_1,\dots,i_n \geq 0} a_{i_1,\dots,i_n} X_1^{i_1} \cdots X_n^{i_n}, \quad a_{i_1,\dots,i_n} = 0 \text{ para } (i_1,\dots,i_n) \neq (0,\dots,0),$$

podemos decir que $R$ es un subanillo de $R[X_1,\dots,X_n]$. De la misma manera, por la definición, los polinomios forman un subanillo de $R[\![X_1,\dots,X_n]\!]$.

$$R \subset R[X_1,\dots,X_n] \subset R[\![X_1,\dots,X_n]\!].$$

▲

**11.1.3. Ejemplo.** Tenemos una cadena de subanillos

$$\mathbb{Z} \subset \mathbb{Z}[\sqrt{5}] \subset \mathbb{Z}\Big[\frac{1+\sqrt{5}}{2}\Big] \subset \mathbb{R} \subset \mathbb{C},$$

donde

$$\mathbb{Z}[\sqrt{5}] := \{a + b\sqrt{5} \mid a, b \in \mathbb{Z}\}, \quad \mathbb{Z}\Big[\frac{1+\sqrt{5}}{2}\Big] := \Big\{a + b\,\frac{1+\sqrt{5}}{2} \;\Big|\; a, b \in \mathbb{Z}\Big\}.$$

▲

**11.1.4. Ejemplo.** Para $n = 1, 2, 3, \dots$ y para $p$ un número primo los conjuntos

$$\mathbb{Z}\Big[\frac{1}{n}\Big] := \Big\{\frac{a}{n^k} \in \mathbb{Q} \;\Big|\; a \in \mathbb{Z},\ k = 0, 1, 2, \dots\Big\}, \quad \mathbb{Z}_{(p)} := \Big\{\frac{a}{b} \in \mathbb{Q} \;\Big|\; a, b \in \mathbb{Z},\ p \nmid b\Big\}$$

son subanillos de $\mathbb{Q}$. ▲

**11.1.5. Ejemplo.** Consideremos el anillo de las aplicaciones $f\colon \mathbb{R} \to \mathbb{R}$ respecto a las operaciones **punto por punto**

$$(f+g)(x) := f(x) + g(x), \quad (f \cdot g)(x) := f(x) \cdot g(x).$$

Las aplicaciones continuas $\mathbb{R} \to \mathbb{R}$ forman un subanillo. ▲

**11.1.6. Ejemplo.** Para un anillo $R$ consideremos el subconjunto de los elementos que conmutan con todos los elementos:

$$Z(R) := \{x \in R \mid xy = yx \text{ para todo } y \in R\}.$$

Es un subanillo de $R$, llamado el **centro**. Notamos que $R$ es conmutativo si y solamente si $R = Z(R)$. ▲

**11.1.7. Ejemplo.** $\mathbb{Z}$ y $\mathbb{Z}/n\mathbb{Z}$ no tienen subanillos propios. En efecto, si $R \subseteq \mathbb{Z}$ es un subanillo, entonces $1 \in R$, y el mínimo subgrupo abeliano de $\mathbb{Z}$ que contiene a 1 es todo $\mathbb{Z}$. De la misma manera, para un subanillo $R \subseteq \mathbb{Z}/n\mathbb{Z}$ tenemos necesariamente $[1]_n \in R$, pero para todo $a = 1, 2, 3, 4, \dots$ se cumple

$$[a]_n = \underbrace{[1]_n + \cdots + [1]_n}_{n}.$$

▲

**11.1.8. Observación.** *Sea $R$ un anillo. Si $R_i \subseteq R$ son subanillos, entonces $\bigcap_i R_i$ es un subanillo.*

## 11.2 Homomorfismos de anillos

Un homomorfismo de anillos es una aplicación que preserva las operaciones de adición y multiplicación. Ya que no todos los elementos de $R$ son invertibles, de la identidad $f(xy) = f(x)\,f(y)$ en general no se puede deducir que $f(1_R) = 1_S$. La última condición hace parte de la definición de homomorfismo de anillos.

**11.2.1. Definición.** Sean $R$ y $S$ anillos. Se dice que una aplicación $f\colon R \to S$ es un **homomorfismo** si se cumplen las siguientes condiciones:

1) $f$ es un homomorfismo de grupos abelianos respecto a la adición; es decir, $f(x+y) = f(x) + f(y)$ para cualesquiera $x, y \in R$;

2) $f$ preserva la identidad: $f(1_R) = 1_S$;

3) $f$ preserva la multiplicación: $f(xy) = f(x)\,f(y)$ para cualesquiera $x, y \in R$.

Un homomorfismo $f\colon R \to R$ se llama un **endomorfismo** de $R$.

**11.2.2. Ejemplo.** La proyección canónica

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

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

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

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

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

El elemento $f(n) \in R$ por abuso de notación también se denota por $n$. ▲

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

$$\begin{aligned} \mathrm{ev}_{\underline{c}}\colon R[X_1, \ldots, X_n] &\to R, \\ f &\mapsto f(c_1, \ldots, c_n). \end{aligned}$$

Aquí si $f = \sum_{i_1,\ldots,i_n \geq 0} a_{i_1,\ldots,i_n}\, X_1^{i_1} \cdots X_n^{i_n}$, entonces

$$f(c_1, \ldots, c_n) := \sum_{i_1,\ldots,i_n \geq 0} a_{i_1,\ldots,i_n}\, c_1^{i_1} \cdots c_n^{i_n}.$$

▲

**11.2.6. Observación.** *Sea $f\colon R \to S$ un homomorfismo de anillos. Se cumplen las siguientes propiedades.*

1) $f(0_R) = 0_S$,

2) $f(-x) = -f(x)$ *para todo* $x \in R$,

3) *se cumple* $f(x^{-1}) = f(x)^{-1}$ *para todo* $x \in R^\times$, *y de este modo* $f$ *se restringe a un homomorfismo de grupos* $f^\times \colon R^\times \to S^\times$:

$$\begin{array}{ccc} R^\times & \overset{f^\times}{\dashrightarrow} & S^\times \\ \downarrow & & \downarrow \\ R & \xrightarrow{\ f\ } & S \end{array}$$

*Demostración.* Las partes 1) y 2) ya las probamos para homomorfismos de grupos. La parte 3) es un análogo multiplicativo de 2) y se demuestra de la misma manera:

$$f(x^{-1})\, f(x) = f(x^{-1}\, x) = f(1_R) = 1_S, \quad f(x)\, f(x^{-1}) = f(x\, x^{-1}) = f(1_R) = 1_S.$$

■

**11.2.7. Definición.** Se dice que un homomorfismo de anillos $f \colon R \to S$ es un **isomorfismo** si existe un homomorfismo de anillos $f^{-1} \colon S \to R$ tal que $f^{-1} \circ f = \mathrm{id}_R$ y $f \circ f^{-1} = \mathrm{id}_S$.

Un isomorfismo $f \colon R \to R$ se llama un **automorfismo** de $R$.

**11.2.8. Ejemplo.** La conjugación compleja

$$z = x + y\sqrt{-1} \mapsto \overline{z} := x - y\sqrt{-1}$$

es un automorfismo de $\mathbb{C}$. ▲

**11.2.9. Observación.** *Todo homomorfismo de anillos* $f \colon R \to S$ *es un isomorfismo si y solamente si es biyectivo.*

*Demostración.* Si $f$ es un isomorfismo, entonces $f$ admite un homomorfismo inverso $f^{-1} \colon S \to R$, así que es una biyección.

Viceversa, supongamos que $f$ es un homomorfismo biyectivo. En este caso existe una aplicación inversa $f^{-1} \colon S \to R$ y hay que comprobar que es un homomorfismo de anillos. Dado que $f(1_R) = 1_S$, tenemos $f^{-1}(1_S) = 1_R$. Luego, para $x, y \in S$

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

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

**11.2.10. Observación (Imagen y preimagen).** *Sea* $f \colon R \to S$ *un homomorfismo de anillos.*

1) *La* ***imagen*** $\operatorname{im} f := \{f(x) \mid x \in R\}$ *es un subanillo de* $S$.

2) *Si* $S' \subseteq S$ *es un subanillo, entonces su preimagen*

$$f^{-1}(S') := \{x \in R \mid f(x) \in S'\}$$

*es un subanillo de* $R$.

*Demostración.* La parte 1) se sigue de las identidades

$$f(x + y) = f(x) + f(y), \quad f(1_R) = 1_S, \quad f(xy) = f(x)\, f(y).$$

En la parte 2), si $x \pm y \in f^{-1}(S')$, entonces $f(x), f(y) \in S'$. Luego, $x \pm y \in f^{-1}(S')$, dado que $f(x \pm y) = f(x) \pm f(y) \in S'$. De la misma manera, $xy \in f^{-1}(S')$, dado que $f(xy) = f(x)\, f(y) \in S'$. Tenemos $f(0_R) = 0_S \in S'$ y $f(1_R) = 1_S \in S'$, y por lo tanto $0_R, 1_R \in f^{-1}(S')$. ■

**11.2.11. Proposición.** *Sea $R$ un anillo. Consideremos el homomorfismo $f\colon \mathbb{Z} \to R$. Entonces,* $\operatorname{im} f$ *es el mínimo subanillo de $R$. Hay dos posibilidades.*

1) $\operatorname{im} f \cong \mathbb{Z}$. *En este caso se dice que $R$ es un anillo de* ***característica*** $0$.

2) $\operatorname{im} f \cong \mathbb{Z}/n\mathbb{Z}$ *para algún $n = 1, 2, 3, \ldots$ En este caso se dice que $R$ es un anillo de* ***característica*** $n$.

*Demostración.* Tenemos

$$\operatorname{im} f = \{\underbrace{1_R + \cdots + 1_R}_{m} \mid m = 0, 1, 2, 3, \ldots\}.$$

Notamos que todo subanillo $S \subseteq R$ necesariamente contiene $0_R$ y $1_R$, y siendo cerrado respecto a la suma, también contiene todos los elementos $\pm\underbrace{1 + \cdots + 1}_{m}$. Entonces, $\operatorname{im} f \subseteq S$ para cualquier subanillo $S \subseteq R$.

Hay dos posibilidades.

1) El orden de $1_R$ en el grupo aditivo de $R$ es infinito. En este caso $\operatorname{im} f \cong \mathbb{Z}$ y el isomorfismo viene dado por
$$\mathbb{Z} \to \operatorname{im} f, \quad 1 \mapsto 1_R.$$

2) El orden de $1_R$ en el grupo aditivo de $R$ es finito y es igual a algún número $n = 1, 2, 3, \ldots$ En este caso $\operatorname{im} f \cong \mathbb{Z}/n\mathbb{Z}$ y el isomorfismo viene dado por
$$\mathbb{Z}/n\mathbb{Z} \to \operatorname{im} f, \quad [1]_n \mapsto 1_R.$$

■

**11.2.12. Ejemplo.** Los anillos $\mathbb{Q}$, $\mathbb{Q}[X]$, $M_m(\mathbb{Z})$ y $\mathbb{Z}[X_1, \ldots, X_m]$ son de característica 0. Los anillos $M_m(\mathbb{Z}/n\mathbb{Z})$ y $\mathbb{Z}/n\mathbb{Z}[X_1, \ldots, X_m]$ son de característica $n$. El cuerpo finito $\mathbb{F}_p$ tiene característica $p$. ▲

**11.2.13. Observación.** *Si $R$ es un anillo no nulo sin divisores de cero ($xy = 0$ implica que $x = 0$ o $y = 0$), entonces la característica de $R$ es igual a $0$ o es un número primo $p$.*

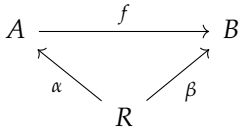
*Demostración.* El anillo $\mathbb{Z}/n\mathbb{Z}$ tiene divisores de cero si y solamente si $n$ es un número compuesto. ■

## 11.3 Álgebras sobre anillos

**11.3.1. Definición.** Sea $R$ un anillo. Una **$R$-álgebra** es un anillo $A$ junto con un homomorfismo de anillos $\alpha\colon R \to A$. En este caso por abuso de notación para $r \in R$ y $x \in A$

(11.1) en lugar de "$\alpha(r) \cdot x$" se escribe simplemente "$r \cdot x$".

Para dos $R$-álgebras $\alpha\colon R \to A$ y $\beta\colon R \to B$ un **homomorfismo** es un homomorfismo de anillos $f\colon R \to B$ que hace conmutar el diagrama



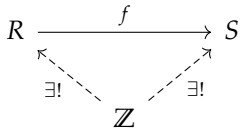

Notamos que la última condición $f \circ \alpha = \beta$ implica que para todo $r \in R$ y $x \in A$ se cumple

$$f \circ \alpha(r) \cdot f(x) = \beta(r) \cdot f(x).$$

Puesto que $f$ es un homomorfismo, esto es equivalente a $f(\alpha(r) \cdot x) = \beta(r) \cdot f(x)$ o, usando la notación (11.1),

$$f(r \cdot x) = r \cdot f(x).$$

**11.3.2. Ejemplo.** Todo anillo tiene una estructura única de $\mathbb{Z}$-álgebra: existe un homomorfismo único $\mathbb{Z} \to R$. Un homomorfismo de $\mathbb{Z}$-álgebras es la misma cosa que homomorfismo de anillos:




De nuevo, usando la notación (11.1), para $n \in \mathbb{Z}$ y $r \in R$ tenemos

$$n \cdot r = \begin{cases} \underbrace{r + \cdots + r}_{n}, & \text{si } n > 0, \\ -(\underbrace{r + \cdots + r}_{-n}), & \text{si } n < 0, \\ 0, & \text{si } n = 0. \end{cases}$$

▲

**11.3.3. Ejemplo.** Los números complejos forman una $\mathbb{R}$-álgebra: tenemos un homomorfismo

$$\begin{aligned} \alpha \colon \mathbb{R} &\rightarrowtail \mathbb{C}, \\ x &\mapsto x + 0\sqrt{-1}. \end{aligned}$$

Notamos que para $x \in \mathbb{R}$ se tiene

$$x \cdot (u + v\sqrt{-1}) = xu + xv\sqrt{-1}.$$

▲

**11.3.4. Ejemplo.** Sea $R$ un anillo conmutativo. Los anillos de polinomios $R[X_1, \ldots, X_n]$ y series formales de potencias $R[\![X_1, \ldots, X_n]\!]$ son $R$-álgebras. En el caso de polinomios, el homomorfismo

$$\alpha \colon R \to R[X_1, \ldots, X_n]$$

asocia a los elementos de $R$ los polinomios constantes correspondientes. En este caso

$$r \cdot \sum_{i_1,\ldots,i_n} a_{i_1,\ldots,i_n} X_1^{i_1} \cdots X_n^{i_n} = \sum_{i_1,\ldots,i_n} (r \cdot a_{i_1,\ldots,i_n}) X_1^{i_1} \cdots X_n^{i_n}.$$

De modo similar, tenemos para las series de potencias

$$\alpha \colon R \to R[\![X_1, \ldots, X_n]\!].$$

▲

**11.3.5. Ejemplo.** Sea $R$ un anillo conmutativo. El homomorfismo

$$\alpha \colon R \to M_n(R), \quad r \mapsto \begin{pmatrix} r & & & \\ & r & & \\ & & \ddots & \\ & & & r \end{pmatrix}$$

que asocia a los elementos de $R$ las matrices escalares correspondientes define estructura de $R$-álgebra sobre $M_n(R)$. En este caso

$$r \cdot (x_{ij}) = (rx_{ij}).$$

▲

Ahora podemos finalmente aclarar qué es el anillo de polinomios $R[X_1, \ldots, X_n]$.

**11.3.6. Proposición (Propiedad universal del álgebra de polinomios).** *Sea $R$ un anillo conmutativo y sea $A$ una $R$-álgebra conmutativa. Consideremos elementos $x_1, \ldots, x_n \in A$. Existe un homomorfismo único de $R$-álgebras $f\colon R[X_1, \ldots, X_n] \to A$ tal que $f(X_i) = x_i$ para $i = 1, \ldots, n$.*

$$\begin{array}{ccc} X_i & \longmapsto & x_i \\ R[X_1, \ldots, X_n] & \overset{\exists!}{\dashrightarrow} & A \\ & \nwarrow \quad \nearrow_{\alpha} & \\ & R & \end{array}$$

*Demostración.* Si $f\colon R[X_1, \ldots, X_n] \to A$ es un homomorfismo de $R$-álgebras, entonces para todo polinomio tenemos

$$\begin{aligned} f\left(\sum_{i_1,\ldots,i_n \geq 0} a_{i_1,\ldots,i_n} X_1^{i_1} \cdots X_n^{i_n}\right) &= \sum_{i_1,\ldots,i_n \geq 0} f\left(a_{i_1,\ldots,i_n} X_1^{i_1} \cdots X_n^{i_n}\right) \\ &= \sum_{i_1,\ldots,i_n \geq 0} a_{i_1,\ldots,i_n} \cdot f(X_1^{i_1} \cdots X_n^{i_n}) = \sum_{i_1,\ldots,i_n \geq 0} a_{i_1,\ldots,i_n} \cdot f(X_1)^{i_1} \cdots f(X_n)^{i_n}. \end{aligned}$$

Esto significa que $f$ está definido de modo único por las imágenes $f(X_i) \in A$. Además, se ve que especificando $f(X_i) = x_i$ para elementos arbitrarios $x_1, \ldots, x_n \in A$ se obtiene un homomorfismo de $R$-álgebras $f\colon R[X_1, \ldots, X_n] \to A$. ∎

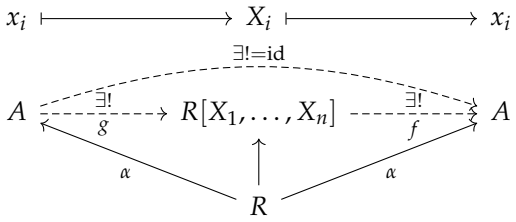
**11.3.7. Corolario.** *Sea $R$ un anillo conmutativo. Consideremos elementos $x_1, \ldots, x_n \in R$. Existe un homomorfismo único de anillos $f\colon \mathbb{Z}[X_1, \ldots, X_n] \to R$ tal que $f(X_i) = x_i$ para $i = 1, \ldots, n$.*

$$\begin{array}{ccc} X_i & \longmapsto & x_i \\ \mathbb{Z}[X_1, \ldots, X_n] & \overset{\exists!}{\dashrightarrow} & R \end{array}$$

*Demostración.* Recordemos que anillos son $\mathbb{Z}$-álgebras. ∎

Como siempre, las palabras "propiedad universal" significan que $R[X_1, \ldots, X_n]$ está definido de modo único salvo isomorfismo único por esta propiedad. En efecto, supongamos que $A$ es una $R$-álgebra con algunos elementos $x_1, \ldots, x_n$ que satisface la misma propiedad universal. Entonces, existe un único homomorfismo de $R$-álgebras $f\colon R[X_1, \ldots, X_n] \to A$ tal que $X_i \mapsto x_i$ y un único homomorfismo de $R$-álgebras $g\colon A \to R[X_1, \ldots, X_n]$ tal que $x_i \mapsto X_i$. Luego, necesariamente $g \circ f = \mathrm{id}_{R[X_1,\ldots,X_n]}$ y $f \circ g = \mathrm{id}_A$:

$$\begin{array}{ccccc} X_i & \longmapsto & x_i & \longmapsto & X_i \\ & & \overset{\exists!=\mathrm{id}}{\frown} & & \\ R[X_1, \ldots, X_n] & \overset{\exists!}{\underset{f}{\dashrightarrow}} & A & \overset{\exists!}{\underset{g}{\dashrightarrow}} & R[X_1, \ldots, X_n] \\ & \nwarrow & \uparrow{\scriptstyle \alpha} & \nearrow & \\ & & R & & \end{array}$$




**11.3.8. Comentario.** Es importante que $A$ sea conmutativa. En el caso contrario, los elementos $f(X_i)$ no necesariamente conmutan entre sí, mientras que $X_i$ conmutan en $R[X_1,\ldots,X_n]$. La propiedad universal similar respecto a álgebras no conmutativas caracteriza a los "polinomios en variables no conmutativas" (aunque suena exótico, es un objeto natural e importante).

Sin embargo, para polinomios *en una variable* tenemos la siguiente propiedad universal: si $A$ es una $R$-álgebra, *no necesariamente conmutativa* y $x \in A$, entonces existe un homomorfismo único de $R$-álgebras $f\colon R[X] \to A$ tal que $f(X) = x$:

$$f\Big(\sum_{i\geq 0} a_i\, X^i\Big) = \sum_{i\geq 0} a_i \cdot f(X)^i.$$

**11.3.9. Comentario.** El anillo de series formales $R[\![X_1,\ldots,X_n]\!]$ también se caracteriza por cierta propiedad universal, pero es un poco más complicada y por esto la omitimos.

**11.3.10. Proposición.** *Sea $R$ un anillo conmutativo y sea $n = 2,3,4,\ldots$ Tenemos isomorfismos*

$$R[X_1,\ldots,X_{n-1}][X_n] \cong R[X_1,\ldots,X_n],$$
$$R[\![X_1,\ldots,X_{n-1}]\!][\![X_n]\!] \cong R[\![X_1,\ldots,X_n]\!].$$

*Idea de la demostración.* Todo elemento $\sum_{i_1,\ldots,i_n\geq 0} a_{i_1,\ldots,i_n}\, X_1^{i_1}\cdots X_n^{i_n}$ puede ser escrito como $\sum_{i\geq 0} f_i\, X_n^i$, donde en $f_i$ aparecen las variables $X_1,\ldots,X_{n-1}$. Dejo los detalles al lector. ■

## 11.4 El álgebra de grupo

**11.4.1. Definición.** Sea $G$ un grupo y sea $R$ un anillo conmutativo. Definamos

$$R[G] := \Big\{\text{sumas formales } \sum_{g\in G} a_g\, g \;\Big|\; a_g \in R,\ a_g = 0 \text{ salvo un número finito de } g \in G\Big\}.$$

Definamos la suma mediante

$$\Big(\sum_{g\in G} a_g\, g\Big) + \Big(\sum_{g\in G} b_g\, g\Big) := \sum_{g\in G} (a_g + b_g)\, g$$

y el producto mediante la multiplicación en $G$ y la distributividad formal:

$$\Big(\sum_{h\in G} a_h\, h\Big)\cdot\Big(\sum_{k\in G} b_k\, k\Big) := \sum_{h\in G} a_h\Big(\sum_{k\in G} b_k\, hk\Big) = \sum_{h\in G} a_h\,\Big(\sum_{g\in G} b_{h^{-1}g}\, h(h^{-1}g)\Big)$$
$$= \sum_{h\in G}\Big(\sum_{h\in G} a_h\, b_{h^{-1}g}\Big)\, g = \sum_{g\in G}\Big(\sum_{hk=g} a_h b_k\Big)\, g.$$

Aquí la segunda igualdad sigue del hecho de que el conjunto $\{h^{-1}g \mid g \in G\}$ está en biyección con los elementos de $G$. Entonces, podemos tomar como la definición la identidad[*]

$$\Big(\sum_{h\in G} a_h\, h\Big)\cdot\Big(\sum_{k\in G} b_k\, k\Big) := \sum_{g\in G}\Big(\sum_{hk=g} a_h b_k\Big)\, g.$$

Se puede comprobar que $R[G]$ es un anillo. El cero es la suma $\sum_{g\in G} a_g\, g$ donde $a_g = 0$ para todo $g \in G$ y la identidad es la suma donde $a_e = 1$ (donde $e \in G$ es el elemento neutro de $G$) y $a_g = 0$ para $g \neq e$. Notamos que el anillo $R[G]$ es conmutativo si y solamente si $G$ es un grupo abeliano. El homomorfismo

$$\begin{aligned} &R \to R[G],\\ &r \mapsto \sum_{g\in G} a_g\, g, \quad a_g := \begin{cases} r, & g = e,\\ 0, & g \neq e \end{cases} \end{aligned}$$

define una estructura de $R$-álgebra sobre $R[G]$. Tenemos

$$r\cdot\sum_{g\in G} a_g\, g = \sum_{g\in G}(r\, a_g)\, g.$$

El álgebra $R[G]$ se llama el **álgebra de grupo** asociada a $G$.

Notamos que cada elemento $g \in G$ corresponde a un elemento

$$\sum_{h\in G} a_h\, g \in R[G], \quad a_h := \begin{cases} 1, & h = g,\\ 0, & h \neq g, \end{cases}$$

y esto nos da una aplicación inyectiva $G \hookrightarrow R[G]$. Respecto a esta inclusión, $G \subseteq R[G]^\times$.

Tenemos

$$h\sum_{g\in G} a_g\, g = \sum_{g\in G} a_g\, hg = \sum_{g\in G} a_{h^{-1}g}\, g, \quad \Big(\sum_{g\in G} a_g\, g\Big)\, h = \sum_{g\in G} a_g\, gh = \sum_{g\in G} a_{gh^{-1}}\, g.$$

Comparando estas dos expresiones, se puede calcular el centro de $R[G]$ (haga el ejercicio 11.10).

**11.4.2. Ejemplo.** En el álgebra $\mathbb{Z}[S_3]$ calculamos

$$\begin{aligned}(1\cdot(1\ 2)+2\cdot(2\ 3))^2 &= 1\cdot\underbrace{(1\ 2)^2}_{=\mathrm{id}} + 2\cdot\underbrace{(1\ 2)\,(2\ 3)}_{=(1\ 2\ 3)} + 2\cdot\underbrace{(2\ 3)\,(1\ 2)}_{=(1\ 3\ 2)} + 4\cdot\underbrace{(2\ 3)^2}_{=\mathrm{id}}\\ &= 5\cdot\mathrm{id} + 2\cdot(1\ 2\ 3) + 2\cdot(1\ 3\ 2).\end{aligned}$$

Si $C_3 = \{e, g, g^2\}$ es el grupo cíclico de orden 3, entonces tenemos en $\mathbb{Z}[C_3]$

$$(e+g+g^2)^2 = e+g+g^2+g+g^2+\underbrace{g^3}_{=e}+g^2+\underbrace{g^3}_{=e}+\underbrace{g^4}_{=g} = 3\cdot(e+g+g^2).$$

(Para una generalización, de este cálculo, haga el ejercicio 11.9.) ▲

[*]Note que es parecida a la fórmula

$$\Big(\sum_{i\geq 0} a_i\, X^i\Big)\cdot\Big(\sum_{j\geq 0} b_j\, X^j\Big) := \sum_{k\geq 0}\Big(\sum_{i+j=k} a_i b_j\Big)\, X^k.$$

(No es una coincidencia.)

**11.4.3. Proposición (Propiedad universal del álgebra de grupo o adjunción con $A \rightsquigarrow A^\times$).** *Sea $R$ un anillo conmutativo, $G$ un grupo y $A$ una $R$-álgebra. Todo homomorfismo de grupos $f\colon G \to A^\times$ se extiende de modo único a un homomorfismo de $R$-álgebras $\widetilde{f}\colon R[G] \to A$:*

$$\begin{array}{ccc} G & \hookrightarrow & R[G] \\ {\scriptstyle f}\downarrow & & \vdots\,{\scriptstyle \exists!\widetilde{f}} \\ A^\times & \hookrightarrow & A \end{array}$$

*En otras palabras, hay una biyección natural*

$$\{\text{homomorfismos de } R\text{-álgebras } R[G] \to A\} \cong \{\text{homomorfismos de grupos } G \to A^\times\}.$$

*En particular, para todo anillo $R$ hay una biyección natural*

$$\{\text{homomorfismos de anillos } \mathbb{Z}[G] \to R\} \cong \{\text{homomorfismos de grupos } G \to R^\times\}.$$

*Demostración.* Sea $\alpha\colon R \to A$ el homomorfismo que define la estructura de $R$-álgebra. Sea $\widetilde{f}\colon R[G] \to A$ un homomorfismo de $R$-álgebras. Puesto que $G \subseteq R[G]^\times$, este homomorfismo se restinge a un homomorfismo de grupos $f\colon G \to A^\times$. Luego,

$$\widetilde{f}\Big(\sum_{g\in G} a_g\, g\Big) = \sum_{g\in G} \widetilde{f}(a_g\, g) = \sum_{g\in G} \alpha(a_g)\, f(g).$$

■

**11.4.4. Corolario.** *Sea $R$ un anillo conmutativo. Todo homomorfismo de grupos $f\colon G \to H$ se extiende de manera canónica a un homomorfismo de $R$-álgebras $\widetilde{f}\colon R[G] \to R[H]$.*

*Demostración.* El homomorfismo de $R$-álgebras en cuestión viene dado por

$$\widetilde{f}\Big(\sum_{g\in G} a_g\, g\Big) = \sum_{g\in G} a_g\, f(g),$$

y es un caso particular del resultado anterior:

$$\begin{array}{ccc} G & \hookrightarrow & R[G] \\ {\scriptstyle f}\downarrow & & \\ H & & \vdots\,{\scriptstyle \exists!\widetilde{f}} \\ \downarrow & & \\ R[H]^\times & \hookrightarrow & R[H] \end{array}$$

■

El álgebra $R[G]$ juega papel importante en la teoría de representación de grupos finitos.

## 11.5 Monomorfismos y epimorfismos de anillos

**11.5.1. Proposición.** *Sea $f\colon R \to S$ un homomorfismo de anillos. Las siguientes condiciones son equivalentes.*

*1) $f$ es inyectivo.*

2) *Si $S'$ es otro anillo y hay homomorfismos $g, g' \colon R' \to R$ tales que $f \circ g = f \circ g'$, entonces $g = g'$.*

*En este caso se dice que $f$ es un* ***monomorfismo****.*

*Demostración.* La implicación 1) $\Rightarrow$ 2) se cumple para cualquier aplicación inyectiva $f$. Para ver que 2) $\Rightarrow$ 1), supongamos que $f$ no es inyectiva y existen diferentes $x, x' \in R$ tales que $f(x) = f(x')$. Primero recordemos que para todo anillo $R$ un homomorfismo $f \colon \mathbb{Z}[X] \to R$ está definido de modo único por $f(X) \in R$ (véase el comentario 11.3.9). Consideremos los homomorfismos

$$g \colon \mathbb{Z}[X] \to R, \quad X \mapsto x$$

y

$$g \colon \mathbb{Z}[X] \to R, \quad X \mapsto x'.$$

Ahora $f \circ g = f \circ g'$, aunque $g \neq g'$. ■

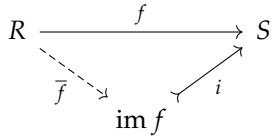
**11.5.2. Ejemplo.** Consideremos la propiedad dual para un homomorfismo $f \colon R \to S$: *si $S'$ es otro anillo y hay homomorfismos $g, g' \colon S \to S'$ tales que $g \circ f = g' \circ f$, entonces $g = g'$.* Esto se cumple si $f$ es sobreyectivo. Sin embargo, esta propiedad no necesariamente implica que $f$ es sobreyectivo. Por ejemplo, consideremos la inclusión $i \colon \mathbb{Z} \to \mathbb{Q}$. Supongamos que $g \circ i = g' \circ i$. Luego, para todo $\frac{a}{b} \in \mathbb{Q}$ se tiene

$$\begin{aligned} g\left(\frac{a}{b}\right) = g(a) \cdot g\left(\frac{1}{b}\right) = g'(a) \cdot g\left(\frac{1}{b}\right) = g'\left(\frac{a}{b} \cdot b\right) \cdot g\left(\frac{1}{b}\right) = g'\left(\frac{a}{b}\right) \cdot g'(b) \cdot g\left(\frac{1}{b}\right) \\ = g'\left(\frac{a}{b}\right) \cdot g(b) \cdot g\left(\frac{1}{b}\right) = g'\left(\frac{a}{b}\right) \cdot g\left(b \cdot \frac{1}{b}\right) = g'\left(\frac{a}{b}\right) \cdot g(1) = g'\left(\frac{a}{b}\right). \end{aligned}$$

Entonces, $g = g'$. ▲

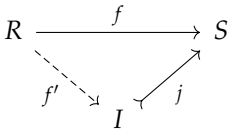
**11.5.3. Proposición (Propiedad universal de la imagen).** *Sea $f \colon R \to S$ un homomorfismo de anillos.*

1) *Existe una factorización de $f$ por el monomorfismo canónico $i \colon \operatorname{im} f \rightarrowtail S$ (inclusión de subanillo):*



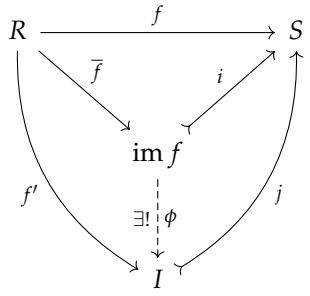

$$f = i \circ \overline{f}.$$

2) *Supongamos que hay otro anillo $I$ junto con un monomorfismo $j \colon I \rightarrowtail S$ y una factorización de $f$ por $I$:*




$$f = j \circ f'.$$

*Luego existe un único homomorfismo $\phi \colon \operatorname{im} f \to I$ que hace conmutar el siguiente diagrama:*




$$\phi \circ \overline{f} = f', \quad j \circ \phi = i.$$

*($\phi$ es mono, puesto que $i = j \circ \phi$ lo es).*

*Demostración.* La parte 1) está clara de la definición de la imagen: ya que $f$ toma sus valores en $\operatorname{im} f \subset S$, en realidad $f$ puede ser vista como una aplicación $\overline{f}\colon R \to \operatorname{im} f$. Es un homomorfismo, puesto que $f$ es un homomorfismo. Su composición con la inclusión del subanillo $i\colon \operatorname{im} f \rightarrowtail S$ coincide con $f$.

En 2), la única opción para $\phi$ para que se cumpla $\phi \circ \overline{f} = f'$ es definir

$$\begin{aligned} \phi\colon \operatorname{im} f &\to I, \\ f(x) &\mapsto f'(x). \end{aligned}$$

Esta aplicación está bien definida: si tenemos $f(x_1) = f(x_2)$, entonces

$$j(f'(x_1)) = f(x_1) = f(x_2) = j(f'(x_2)) \Rightarrow f'(x_1) = f'(x_2).$$

También se cumple $i = j \circ \phi$. En efecto, para $h = f(x) \in \operatorname{im} f$ tenemos

$$j(\phi(h)) = j(f'(x)) = f(x).$$

■

## 11.6 Ideales

El la teoría de grupos, el grupo cociente se construye a partir de un subgrupo *normal*. Para anillos, los cocientes se definen a partir de un *ideal*.

**11.6.1. Definición.** Sea $R$ un anillo y sea $I \subseteq R$ un subgrupo abeliano de $R$ respecto a la adición.

1) Si $rx \in I$ para cualesquiera $r \in R$ y $x \in I$, se dice que $I$ es un **ideal izquierdo** en $R$.

2) Si $xr \in I$ para cualesquiera $r \in R$ y $x \in I$, se dice que $I$ es un **ideal derecho** en $R$.

3) Si se cumplen las condiciones 2) y 3), entonces se dice que $I$ es un **ideal bilateral** en $R$. Esto es equivalente a asumir que $rxr' \in I$ para cualesquiera $r, r' \in R$ y $x \in I$.

**11.6.2. Comentario.** Tenemos $-x = (-1) \cdot x = x \cdot (-1)$, así que para comprobar que un subconjunto $I \subseteq R$ es un ideal, es suficiente comprobar que $I$ no es vacío, cerrado respecto a la adición, y cumple una de las propiedades 1)–3) de la definición de arriba.

**11.6.3. Comentario.** Si $R$ es un anillo *conmutativo*, entonces las condiciones 1)–3) son equivalentes. En este caso se dice simplemente que $I$ es un **ideal** en $R$.

**11.6.4. Observación.** *Sea $R$ un anillo.*

1) *Si $I_k \subseteq R$ es una familia de ideales izquierdos (resp. derechos, bilaterales), entonces $\bigcap_k I_k$ es un ideal izquierdo (resp. derecho, resp. bilateral).*

2) *Si*

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots \subseteq R$$

*es una cadena de ideales izquierdos (resp. derechos, bilaterales), entonces $\bigcup_k I_k$ es un ideal izquierdo (resp. derecho, resp. bilateral).*

*Demostración.* Ejercicio para el lector. ■

**11.6.5. Ejemplo.** 0 y $R$ son ideales bilaterales para cualquier anillo $R$. ▲

**11.6.6. Ejemplo.** Consideremos el anillo de los números enteros $\mathbb{Z}$. Como sabemos, sus subgrupos abelianos son de la forma

$$n\mathbb{Z} := \{na \mid a \in \mathbb{Z}\}$$

para $n = 0, 1, 2, 3, \ldots$ Se puede comprobar que $n\mathbb{Z}$ son ideales (al multiplicar un múltiplo de $n$ por cualquier número entero se obtiene un múltiplo de $n$). ▲

**11.6.7. Observación.** *Sea $R$ un anillo.*

1) *Para un ideal izquierdo (resp. derecho, resp. bilateral) $I \subseteq R$ se tiene $I = R$ si y solo si $u \in I$ para algún elemento invertible $u \in R^\times$.*

2) *Si $R$ es un anillo conmutativo, entonces $R$ es un cuerpo si y solo si 0 y $R$ son los únicos ideales en $R$.*

*Demostración.* En 1), notamos que si $I = R$, entonces $1 \in I$ y $1 \in R^\times$. Viceversa, si $u \in R^\times$ es un elemento tal que $u \in I$, entonces para todo $r \in R$

$$r = r \cdot 1 = r\,(u^{-1}\,u) = (r\,u^{-1})\,u \in I.$$

Este argumento funciona si $I$ es un ideal izquierdo. Para un ideal derecho, tenemos

$$r = 1 \cdot r = (u\,u^{-1})\,r = u\,(u^{-1}\,r) \in I.$$

En 2), si $R$ es un cuerpo, entonces para todo ideal no nulo $I$ si $x \in I$ y $x \neq 0$, entonces $x \in R^\times$ y por ende $I = R$ según la parte 1). Viceversa, si 0 y $R$ son los únicos ideales en $R$, para $x \neq 0$ podemos considerar el ideal

$$Rx := \{rx \mid r \in R\}.$$

Tenemos $Rx \neq 0$, así que $Rx = R$. En particular, $rx = 1$ para algún $r \in R$, y este elemento $r$ es el inverso de $x$. ■

**11.6.8. Ejemplo.** Sea $X$ un conjunto no vacío y sea $R$ un anillo. Entonces, las aplicaciones $f\colon X \to R$ forman un anillo $Fun(X, R)$ respecto a las operaciones punto por punto. Para un punto $x \in X$ sea $I_x$ el conjunto de las aplicaciones tales que $f(x) = 0$:

$$I_x := \{f\colon X \to R \mid f(x) = 0\}.$$

Esto es un ideal en $Fun(X, R)$. En general, para un subconjunto $Y \subseteq X$, tenemos un ideal

$$I(Y) = \bigcap_{x \in Y} I_x = \{f\colon X \to R \mid f(x) = 0 \text{ para todo } x \in Y\} \subseteq Fun(X, R).$$

▲

El último ejemplo tiene muchas variaciones. Por ejemplo, se puede tomar $R = \mathbb{R}$ y $X$ un subconjunto de $\mathbb{R}$ y considerar las funciones continuas $f\colon X \to \mathbb{R}$. También se puede tomar un cuerpo $k$ y el **espacio afín**

$$\mathbb{A}^n(k) := \{(x_1, \ldots, x_n) \mid x_i \in k\}$$

y en lugar de todas las funciones $f\colon \mathbb{A}^n(k) \to k$ considerar los polinomios $f \in k[X_1, \ldots, X_n]$ que también pueden ser evaluados en los puntos de $\mathbb{A}^n(k)$.

**11.6.9. Ejemplo.** Sea $k$ un cuerpo. Para todo subconjunto $X \subseteq \mathbb{A}^n(k)$ consideremos el conjunto de los polinomios en $n$ variables con coeficientes en $k$ que se anulan en todos los puntos de $X$:

$$I(X) := \{f \in k[X_1, \ldots, X_n] \mid f(x) = 0 \text{ para todo } x \in X\} = \bigcap_{x \in X} I(\{x\}).$$

Esto es un ideal en el anillo de polinomios $k[X_1, \ldots, X_n]$. En efecto, si $f_i(x) = 0$ para todo $x \in X$, entonces todas las sumas finitas $\sum_i g_i f_i$ se anulan sobre $X$. ▲

En este curso no vamos a ver muchos resultados sobre anillos no conmutativos, pero es bueno conocer algunas definiciones básicas. El lector interesado puede consultar el libro [Lam2001].

**11.6.10. Ejemplo.** Las matrices de la forma $\begin{pmatrix} * & 0 \\ * & 0 \end{pmatrix}$ forman un ideal izquierdo en $M_2(R)$ que no es un ideal derecho. Viceversa, las matrices $\begin{pmatrix} * & * \\ 0 & 0 \end{pmatrix}$ forman un ideal derecho que no es izquierdo. ▲

**11.6.11. Observación.** *Sea $k$ un cuerpo. Entonces, los únicos ideales bilaterales en el anillo de matrices $R = M_n(k)$ son $0$ y $R$.*

*Demostración.* Denotemos por $e_{ij}$ la matriz que tiene ceros en todas las entradas y 1 en la entrada $(i, j)$. Notamos que

$$e_{ij}\, A\, e_{k\ell} = a_{jk}\, e_{i\ell}.$$

Supongamos que $I \subseteq R$ es un ideal bilateral no nulo. Sea $A \in I$ donde $A$ es una matriz tal que $a_{jk} \neq 0$ para algunos $1 \leq j, k \leq n$. Luego, la fórmula de arriba nos dice que para todo $1 \leq i, \ell \leq n$ se tiene

$$e_{i\ell} = a_{jk}^{-1}\, e_{ij}\, A\, e_{k\ell}.$$

Puesto que $I$ es un ideal bilateral, podemos concluir que todas las matrices $e_{i\ell}$ pertenecen a $I$. Luego, para cualquier matriz $B = (b_{i\ell}) \in M_n(k)$ tenemos

$$B = \sum_{1 \leq i, \ell \leq n} b_{i\ell}\, e_{i\ell},$$

y esta matriz pertenece a $I$, siendo una suma de $b_{i\ell}\, e_{i\ell} \in I$. Entonces, acabamos de probar que un ideal bilateral no nulo en $M_n(k)$ necesariamente coincide con todo $M_n(k)$. ■

Para una generalización del último resultado, haga el ejercicio 11.15.

**11.6.12. Observación.** *Sea $f\colon R \to S$ un homomorfismo de anillos.*

1) *Si $I \subseteq S$ es un ideal izquierdo (resp. ideal derecho, resp. ideal bilateral), entonces $f^{-1}(I)$ es un ideal izquierdo (resp. ideal derecho, resp. ideal bilateral) en $R$.*

2) *Si $f$ es sobreyectivo e $I \subseteq R$ es un ideal izquierdo (resp. ideal derecho, resp. ideal bilateral), entonces $f(I)$ es un ideal izquierdo (resp. ideal derecho, resp. ideal bilateral) en $S$.*

*Demostración.* Veamos el caso de ideales izquierdos; el caso de ideales derechos y bilaterales es similar.

Tenemos $f(0_R) = 0_S \in I$, así que $0_R \in f^{-1}(I)$. Si $x, y \in f^{-1}(I)$, esto significa que $f(x), f(y) \in I$. Luego, $f(x+y) = f(x) + f(y) \in I$, así que $x + y \in f^{-1}(I)$. Ahora si $x \in f^{-1}(I)$, entonces $f(x) \in I$, y luego $f(rx) = f(r)f(x) \in I$ para cualesquiera $r \in R$, así que $rx \in f^{-1}(I)$.

En la parte 2), tenemos $0_S = f(0_R)$ donde $0_R \in I$, así que $0_S \in f(I)$. Para $x, y \in I$ tenemos $x + y \in I$, así que $f(x), f(y) \in f(I)$ implica que $f(x) + f(y) = f(x+y) \in f(I)$. Para $x \in I$ y $s \in S$, dado que $f$ es una aplicación sobretectiva, se tiene $s = f(r)$ para algún $r \in R$. Luego, $sf(x) = f(r)f(x) = f(rx) \in f(I)$. ■

**11.6.13. Comentario.** Si $f\colon R \to S$ es un homomorfismo que no es sobreyectivo e $I \subseteq R$ es un ideal, entonces $f(I)$ no tiene por qué ser un ideal en $S$. Considere por ejemplo la inclusión $f\colon \mathbb{Z} \hookrightarrow \mathbb{Q}$.

## 11.7 Ideales generados

**11.7.1. Definición.** Sea $R$ un anillo y $A \subset R$ un subconjunto.

1) El **ideal izquierdo generado por** $A$ es el mínimo ideal izquierdo que contiene a $A$:

$$RA := \bigcap_{\substack{I \subseteq R \\ \text{izquierdo} \\ A \subseteq I}} I.$$

2) El **ideal derecho generado por** $A$ es el mínimo ideal derecho que contiene a $A$:

$$AR := \bigcap_{\substack{I \subseteq R \\ \text{derecho} \\ A \subseteq I}} I.$$

3) El **ideal bilateral generado por** $A$ es el mínimo ideal bilateral que contiene a $A$:

$$RAR := \bigcap_{\substack{I \subseteq R \\ \text{bilateral} \\ A \subseteq I}} I.$$

**11.7.2. Comentario.** Si $A = \{x_1, \ldots, x_n\}$ es un conjunto finito, se usa la notación

$$RA = Rx_1 + \cdots + Rx_n, \quad AR = x_1R + \cdots + x_nR, \quad RAR = Rx_1R + \cdots + Rx_nR.$$

**11.7.3. Comentario.** Notamos que cuando $R$ es un anillo conmutativo, se tiene $RA = AR = RAR$, y normalmente este ideal se denota por $(A)$, o por $(x_1, \ldots, x_n)$ cuando $A = \{x_1, \ldots, x_n\}$ es un conjunto finito.

**11.7.4. Definición.** Si $I \subseteq R$ es un ideal (izquierdo, derecho, bilateral) que puede ser generado por un número finito de elementos, se dice que $I$ es **finitamente generado**. Si $I$ puede ser generado por un elemento (es decir, $I = Rx$, $xR$, $RxR$ respectivamente), se dice que $I$ es un **ideal principal**.

**11.7.5. Ejemplo.** Todo ideal en $\mathbb{Z}$ es de la forma $n\mathbb{Z}$ para algún $n = 0, 1, 2, 3, \ldots$ El ideal $n\mathbb{Z}$ es el mínimo ideal que contiene a $n$, así que es exactamente el ideal generado por $n$. Entonces, todos los ideales en $\mathbb{Z}$ son principales. ▲

Más adelante vamos a estudiar los anillos conmutativos donde todos los ideales son finitamente generados o donde todos los ideales son principales.

**11.7.6. Observación.** *Sea $R$ un anillo y $A \subset R$ un subconjunto.*

1) *El ideal $RA$ consiste en todas las sumas finitas $\sum_i r_i\, a_i$ donde $r_i \in R$ y $a_i \in A$.*
2) *El ideal $AR$ consiste en todas las sumas finitas $\sum_i a_i\, r_i$ donde $r_i \in R$ y $a_i \in A$.*
3) *El ideal $RAR$ consiste en todas las sumas finitas $\sum_i r_i\, a_i\, r_i'$ donde $r_i, r_i' \in R$ y $a_i \in A$.*

*Demostración.* Verifiquemos, por ejemplo, la parte 1). Si $I$ es un ideal izquierdo tal que $A \subseteq I$, entonces $\sum_i r_i a_i \in I$ para cualesquiera $r_i \in R$, $a_i \in A$. Además, se ve que

$$\left\{ \sum_i r_i\, a_i \;\middle|\; r_i \in R,\ a_i \in A \right\}$$

es un ideal izquierdo: es cerrado respecto a las sumas: si $\sum_i r_i\, a_i$ y $\sum_j r_j'\, a_j'$ son sumas finitas con $r_i, r_j' \in R$ y $a_i, a_j' \in A$, entonces $\sum_i r_i\, a_i + \sum_j r_j'\, a_j'$ es una suma finita de la misma forma. Además, para todo $r \in R$

$$r \sum_i r_i\, a_i = \sum_i (r\, r_i)\, a_i,$$

así que el conjunto es cerrado respecto a la multiplicación por los elementos de $R$ por la izquierda.

Las partes 2) y 3) se verifican de la misma manera. ■

**11.7.7. Corolario (Sumas de ideales).** *Sea $R$ un anillo y sea $I_k \subseteq R$ una familia de ideales izquierdos (resp. derechos, resp. bilaterales). Entonces, el ideal izquierdo (resp. derecho, resp. bilateral) generado por los elementos de $I_k$ coincide con el conjunto*

$$\sum_k I_k := \{\text{sumas finitas } \sum_k x_k \mid x_k \in I_k\}$$

*y se llama la **suma** de los ideales $I_k$. Es el mínimo ideal izquierdo (resp. derecho, resp. bilateral) en $R$ tal que $I_k \subseteq \sum_k I_k$ para todo $k$.*

*Demostración.* Por ejemplo, en el caso de ideales izquierdos, la observación anterior nos dice que hay que tomar las sumas finitas $\sum_i r_i a_i$ donde $r_i \in R$ y $a_i \in I_k$ para algún $k$. Puesto que cada $I_k$ es un ideal izquierdo, en este caso se tiene $r_i a_i \in I_k$. Las sumas de elementos del mismo ideal $I_k$ también pertenecen a $I_k$. Entonces, el conjunto de las sumas finitas $\sum_i r_i a_i$ coincide con el conjunto de las sumas finitas $\sum_k x_k$ donde $x_k \in I_k$. ■

**11.7.8. Observación (Productos de ideales).** *Sea $R$ un anillo y sean $I_1, \ldots, I_n \subseteq R$ ideales izquierdos (resp. derechos, bilaterales).*

1) *El ideal izquierdo (resp. derecho, bilateral) generado por los productos $x_1 \cdots x_n$ donde $x_k \in I_k$ coincide con el conjunto*

$$I_1 \cdots I_n := \{\text{sumas finitas } \sum_i x_{i_1} \cdots x_{i_n} \mid x_{i_k} \in I_k\}$$

   *y se llama el **producto** de los ideales $I_1, \ldots, I_n$.*

2) *Si $I_1, \ldots, I_n$ son ideales bilaterales, entonces*

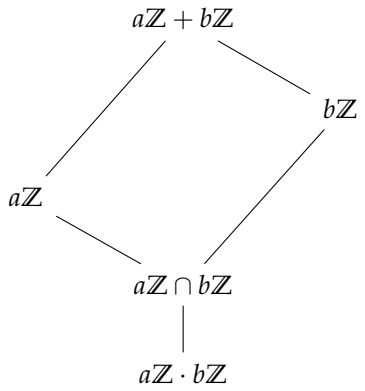
$$I_1 \cdots I_n \subseteq I_1 \cap \cdots \cap I_n.$$

*Demostración.* Por ejemplo, en el caso de ideales izquierdos, hay que considerar las sumas $\sum_i r_i\, x_{i_1} \cdots x_{i_n}$ donde $r_i \in R$, pero $I_1$ es un ideal, así que $r_i\, x_{i_1} \in I_1$.

Si todo $I_k$ es un ideal bilateral, tenemos $x_{i_1} \cdots x_{i_k} \cdots x_{i_n} \in I_k$ para todo $k = 1, \ldots, n$, así que $I_1 \cdots I_n \subseteq I_k$ para todo $k$. ■

**11.7.9. Ejemplo.** Para dos ideales $a\mathbb{Z}, b\mathbb{Z} \subseteq \mathbb{Z}$ tenemos

$$\begin{aligned} a\mathbb{Z} + b\mathbb{Z} &= d\mathbb{Z}, \quad d = \operatorname{mcd}(a,b), \\ a\mathbb{Z} \cdot b\mathbb{Z} &= ab\mathbb{Z}, \\ a\mathbb{Z} \cap b\mathbb{Z} &= m\mathbb{Z}, \quad m = \operatorname{mcm}(a,b). \end{aligned}$$




▲

**11.7.10. Definición.** Sea $R$ un anillo y sea $I \subseteq R$ un ideal bilateral. Para $n = 1, 2, 3, \ldots$ la $n$-ésima potencia de $I$ se define mediante

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

que es equivalente a la definición inductiva

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

**11.7.11. 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

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

Luego, se ve que

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

▲

**11.7.12. Ejemplo.** En el anillo $\mathbb{Z}[X]$ consideremos el ideal $I := (2, X)$ generado por los elementos 2 y $X$. Es el ideal de los polinomios con el término constante par:

$$(2, X) = \{2f + Xg \mid f, g \in \mathbb{Z}[X]\} = \{a_n X^n + a_{n-1} X + \cdots + a_1 X + a_0 \mid n \geq 0,\ a_i \in \mathbb{Z},\ a_0 \text{ es par}\}.$$

Luego,

$$I^2 = \Big\{\text{sumas finitas } \sum_i f_i g_i \;\Big|\; f_i, g_i \in I\Big\}.$$

En particular, dado que $2 \in I$ y $X \in I$, tenemos $4, X^2 \in I^2$, y por lo tanto $X^2 + 4 \in I^2$. Notamos que el polinomio $X^2 + 4$ no puede ser escrito como un producto $fg$ donde $f, g \in I$. ▲

**11.7.13. Ejemplo.** Sea $k$ un cuerpo. Para una colección de polinomios $f_i \in k[X_1, \ldots, X_n]$ consideremos el conjunto de sus ceros comunes en $\mathbb{A}^n(k)$:

$$V(\{f_i\}_{i\in I}) := \{x \in \mathbb{A}^n(k) \mid f_i(x) = 0 \text{ para todo } i \in I\}.$$

Diferentes colecciones $\{f_i\}_{i\in I}$ pueden dar el mismo conjunto de los ceros. Para resolver este problema, podemos definir para todo ideal $J \subseteq k[X_1, \ldots, X_n]$

$$V(J) := \{x \in \mathbb{A}^n(k) \mid f(x) = 0 \text{ para todo } f \in J\}.$$

Ahora

$$V(\{f_i\}_{i\in I}) = V((f_i)_{i\in I})$$

donde $(f_i)_{i\in I}$ denota el ideal en $k[X_1, \ldots, X_n]$ generado por los polinomios $f_i$. En efecto, en general, la inclusión $\{f_i\}_{i\in I} \subseteq (f_i)_{i\in I}$ implica que $V(\{f_i\}_{i\in I}) \supseteq V((f_i)_{i\in I})$. Viceversa, si $x \in V(\{f_i\}_{i\in I})$, entonces $f_i(x) = 0$ para todo $i$, y por ende todas las sumas finitas $\sum_i g_i f_i$ se anulan en $x$. ▲

Los ejemplos 11.6.9 y 11.7.13 nos dan dos operaciones $I$ y $V$:

$$\{\text{ideales } J \subseteq k[X_1, \ldots, X_n]\} \underset{I}{\overset{V}{\rightleftarrows}} \{\text{subconjuntos } X \subseteq \mathbb{A}^n(k)\}$$

Vamos a ver algunas relaciones entre ellas en los ejercicios 11.19 y 11.20. Su estudio pertenece al terreno de la geometría algebraica. Para una introducción, el lector puede consultar el libro [Ful2008].

## 11.8 El núcleo de un homomorfismo de anillos

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

**11.8.1. Observación.** *Sea $f\colon R \to S$ un homomorfismo de anillos. Entonces, el conjunto*

$$\ker f := \{x \in R \mid f(x) = 0\}$$

*es un ideal bilateral en $R$, llamado el **núcleo** de $f$.*

Note que en la teoría de grupos, si $f\colon G \to H$ es un homomorfismo, entonces $\ker f$ es un *subgrupo normal* de $G$. Para un homomorfismo de anillos $f\colon R \to S$, el núcleo $\ker f$ no es un *subanillo* de $R$, sino un *ideal*.

*Demostración.* Un homomorfismo de anillos es en particular de los grupos abelianos correspondientes, y ya sabemos que el núcleo es un subgrupo abeliano. Falta comprobar que para cualesquiera $x \in \ker f$ y $r \cdot R$ se cumple $rx, xr \in \ker f$. En efecto, si $f(x) = 0$, entonces

$$f(rx) = f(r)\,f(x) = f(r) \cdot 0 = 0, \quad f(xr) = f(x)\,f(r) = 0 \cdot f(r) = 0.$$

■

**11.8.2. Observación.** *Un homomorfismo de anillos $f\colon R \to S$ es inyectivo (es decir, un monomorfismo) si y solo si* $\ker f = 0$.

*Demostración.* Ya lo verificamos para homomorfismos de grupos abelianos. ■

**11.8.3. Observación.** *Sea $k$ un cuerpo y $R$ un anillo no nulo. Entonces, todo homomorfismo $f\colon k \to R$ es inyectivo.*

*Demostración.* Si $R \neq 0$, entonces $f(1_k) = 1_R \neq 0$ y $1_k \notin \ker f$. Pero las únicas opciones son $\ker f = 0$ y $\ker f = k$. Entonces, $\ker f = 0$. ■

## 11.9 Anillos cociente

**11.9.1. Definición.** Sea $R$ un anillo y sea $I \subseteq R$ un ideal bilateral. El **anillo cociente** correspondiente $R/I$ es el grupo abeliano cociente $R/I$ con la multiplicación definida por

$$(x+I)\cdot(y+I) := (xy+I).$$

Hay que verificar que el producto está bien definido. Supongamos que $x+I = x'+I$; es decir, $x-x' \in I$. Luego, $xy - x'y = (x-x')\,y \in I$, dado que $I$ es un ideal derecho, y esto implica que $xy+I = x'y+I$. De la misma manera, si $y+I = y'+I$, esto significa que $y-y' \in I$. Esto implica que $xy - xy' = x\,(y-y') \in I$, puesto que $I$ es un ideal izquierdo. De aquí se sigue que $xy+I = xy'+I$. Notamos que en este argumento es importante que $I$ sea un ideal *bilateral*[*].

Dejo al lector verificar que los axiomas de anillo para el cociente $R/I$ se siguen de los axiomas correspondientes para $R$.

**11.9.2. Ejemplo.** En todo anillo $R$ hay dos ideales evidentes: $I = 0$ e $I = R$. Al desarrollar las definiciones, se ve que $R/0 \cong R$ y $R/R = 0$. ▲

**11.9.3. Ejemplo.** El cociente del anillo $\mathbb{Z}$ por el ideal $n\mathbb{Z}$ es el anillo $\mathbb{Z}/n\mathbb{Z}$ de los restos módulo $n$. ▲

**11.9.4. Ejemplo.** Tenemos $\mathbb{R}[X]/(X^2+1) \cong \mathbb{C}$. En efecto, puesto que $X^2 \equiv -1 \pmod{X^2+1}$ en el cociente, se ve que los elementos de $\mathbb{R}[X]/(X^2+1)$ pueden ser representados por los polinomios $b\,X+a$, donde $a, b \in \mathbb{R}$. Luego,

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

Esta fórmula corresponde a la multiplicación compleja, y por ende se tiene un isomorfismo

$$\begin{aligned} \mathbb{R}[X]/(X^2+1) &\xrightarrow{\cong} \mathbb{C} \\ b\,X+a &\mapsto a + b\sqrt{-1}. \end{aligned}$$

▲

**11.9.5. Ejemplo (El cuerpo de cuatro elementos).** Calculemos $\mathbb{F}_2[X]/(X^2+X+1)$. Puesto que $X^2 \equiv X+1 \pmod{X^2+X+1}$, todos 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 correspondiente viene dada por

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

Notamos que este grupo es isomorfo al grupo de Klein $V \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. La tabla de multiplicación viene dada por

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

[*] De la misma manera, el producto sobre el grupo cociente $G/H$ está bien definido solo cuando $H$ es un subgrupo normal (véase el capítulo 7).

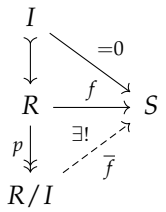
Se ve que todo elemento no nulo es invertible, así que $\mathbb{F}_2[X]/(X^2+X+1)$ es un cuerpo de cuatro elementos. Su grupo de elementos no nulos es de orden 3 y en particular es cíclico. Esto coincide con el resultado del capítulo 7 que dice que si $k$ es un cuerpo, entonces todo subgrupo finito de $k^\times$ es necesariamente cíclico. ▲

Más adelante en el curso vamos a construir todos los cuerpos finitos.

**11.9.6. Proposición (Propiedad universal del anillo cociente).** *Sea $I \subseteq R$ un ideal bilateral. Sea*

$$\begin{aligned} p\colon R &\twoheadrightarrow R/I, \\ x &\mapsto x+I \end{aligned}$$

*la proyección canónica sobre el anillo cociente. Si $f\colon R \to S$ es un homomorfismo de anillos tal que $I \subseteq \ker f$, entonces $f$ se factoriza de modo único por $R/I$: existe un homomorfismo único $\overline{f}\colon R/I \to S$ tal que $f = \overline{f} \circ p$.*




*Demostración.* La flecha punteada $\overline{f}$ es necesariamente

$$x+I \mapsto f(x).$$

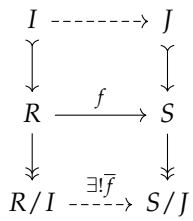
Es una aplicación bien definida: si $x+I = x'+I$ para algunos $x, x' \in R$, entonces $x-x' \in I$, luego $x-x' \in \ker f$ y

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

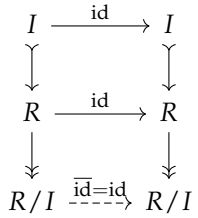
La aplicación $\overline{f}$ es un homomorfismo de anillos, puesto que $f$ lo es. ■

**11.9.7. Corolario (Funtorialidad del cociente).**

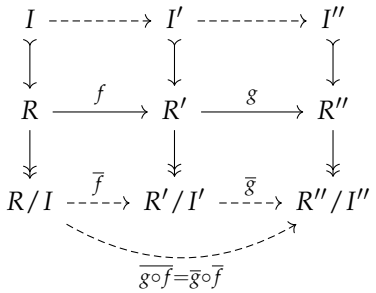
1) *Sea $f\colon R \to S$ un homomorfismo de anillos. Sean $I \subseteq R$ y $J \subseteq S$ ideales bilaterales. Supongamos que $f(I) \subseteq J$. Entonces $f$ induce un homomorfismo canónico $\overline{f}\colon R/I \to S/J$ que conmuta con las proyecciones canónicas:*




2) *La aplicación identidad* $\mathrm{id}\colon R \to R$ *induce la aplicación identidad* $\mathrm{id}\colon R/I \to R/I$*:*




3) *Sean $f\colon R \to R'$ y $g\colon R' \to R''$ dos homomorfismos de anillos y sean $I \subseteq R$, $I' \subseteq R'$, $I'' \subseteq R''$ ideales bilaterales tales que $f(I) \subseteq I'$ y $g(I') \subseteq I''$. Entonces, $\overline{g \circ f} = \overline{g} \circ \overline{f}$:*

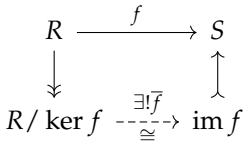



*Demostración.* En 1) la flecha $\overline{f}$ existe y es única gracias a la propiedad universal de $R/I$ aplicada a la composición $R \xrightarrow{f} S \twoheadrightarrow S/J$. Los resultados de 2) y 3) siguen de la unicidad del homomorfismo inducido sobre los grupos cociente. ■

**11.9.8. Proposición (Primer teorema de isomorfía).** *Sea $f\colon R \to S$ un homomorfismo de anillos. Entonces, existe un isomorfismo canónico*

$$\overline{f}\colon R/\ker f \xrightarrow{\cong} \operatorname{im} f$$

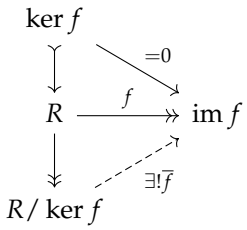
*que hace parte del diagrama conmutativo*




Descifremos el diagrama: la flecha $R \twoheadrightarrow R/\ker f$ es la proyección canónica $x \mapsto x + \ker f$ y la flecha $\operatorname{im} f \rightarrowtail S$ es la inclusión de subanillo, así que el isomorfismo $\overline{f}$ necesariamente viene dado por

$$\overline{f}\colon g + \ker f \mapsto f(g).$$

*Demostración.* La flecha $\overline{f}$ viene dada por la propiedad universal de $R/\ker f$:



Luego, el homomorfismo $\overline{f}$ es evidentemente sobreyectivo. Para ver que es inyectivo, notamos que

$$f(x) = f(y) \iff x - y \in \ker f \iff x + \ker f = y + \ker f.$$

■

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

$$\begin{aligned} f\colon \mathbb{R}[X] &\hookrightarrow \mathbb{C}[X] \to \mathbb{C}, \\ f &\mapsto f(\sqrt{-1}). \end{aligned}$$

Es visiblemente sobreyectivo. Su núcleo consiste en los polinomios en $\mathbb{R}[X]$ que tienen $\sqrt{-1}$ como su raíz; es decir, los polinomios divisibles por $X^2+1$. Entonces, $\ker f = (X^2+1)$. Podemos concluir que $\mathbb{R}[X]/(X^2+1) \cong \mathbb{C}$. ▲

**11.9.10. Ejemplo.** Sea $p$ un número primo. Consideremos el anillo

$$\mathbb{Z}_{(p)} := \left\{ \frac{a}{b} \in \mathbb{Q} \;\middle|\; p \nmid b \right\}.$$

Este es un subanillo de $\mathbb{Q}$. Consideremos la aplicación

$$\begin{aligned} f\colon \mathbb{Z}_{(p)} &\to \mathbb{Z}/p^k\mathbb{Z}, \\ \frac{a}{b} &\mapsto [a]_{p^k} [b]_{p^k}^{-1} \end{aligned}$$

que a una fracción $\frac{a}{b} \in \mathbb{Z}_{(p)}$ asocia el producto del resto $[a]_{p^k}$ por el inverso multiplicativo $[b]_{p^k}^{-1}$ (que existe, dado que $p \nmid b$). Notamos que la aplicación está bien definida: si $\frac{a}{b} = \frac{a'}{b'}$, entonces $[a]_{p^k} [b]_{p^k}^{-1} = [a']_{p^k} [b']_{p^k}^{-1}$. Esto es un homomorfismo de anillos: tenemos

$$f\left(\frac{1}{1}\right) = [1]_{p^k} [1]_{p^k}^{-1} = [1]_{p^k},$$

$$\begin{aligned} f\left(\frac{a_1}{b_1} + \frac{a_2}{b_2}\right) = f\left(\frac{a_1 b_2 + a_2 b_1}{b_1 b_2}\right) &= [a_1 b_2 + a_2 b_1]_{p^k} [b_1 b_2]_{p^k}^{-1} = ([a_1]_{p^k} [b_2]_{p^k} + [a_2]_{p^k} [b_1]_{p^k}) [b_1]_{p^k}^{-1} [b_2]_{p^k}^{-1} \\ &= [a_1]_{p^k} [b_1]_{p^k}^{-1} + [a_2]_{p^k} [b_2]_{p^k}^{-1} = f\left(\frac{a_1}{b_1}\right) + f\left(\frac{a_2}{b_2}\right), \end{aligned}$$

$$f\left(\frac{a_1}{b_1} \cdot \frac{a_2}{b_2}\right) = f\left(\frac{a_1\, a_2}{b_1\, b_2}\right) = [a_1\, a_2]_{p^k} [b_1\, b_2]_{p^k}^{-1} = [a_1]_{p^k} [b_1]_{p^k}^{-1} [a_2]_{p^k} [b_2]_{p^k}^{-1} = f\left(\frac{a_1}{b_1}\right) \cdot f\left(\frac{a_2}{b_2}\right).$$

Este homomorfismo es sobreyectivo: para $[a]_{p^k} \in \mathbb{Z}/p^k\mathbb{Z}$ tenemos $f\left(\frac{a}{1}\right) = [a]_{p^k} [1]_{p^k}^{-1} = [a]_{p^k}$. El núcleo viene dado por

$$\ker f = \left\{ \frac{a}{b} \in \mathbb{Z}_{(p)} \;\middle|\; [a]_{p^k} [b]_{p^k}^{-1} = 0 \right\} = \left\{ \frac{a}{b} \in \mathbb{Z}_{(p)} \;\middle|\; [a]_{p^k} = 0 \right\} = \left\{ \frac{a}{b} \in \mathbb{Z}_{(p)} \;\middle|\; p^k \mid a \right\}.$$

Este es precisamente el ideal $p^k\mathbb{Z}_{(p)}$ generado por $p^k$. El primer teorema de isomorfía nos dice que

$$\mathbb{Z}_{(p)}/p^k\mathbb{Z}_{(p)} \cong \mathbb{Z}/p^k\mathbb{Z}.$$

▲

Ahora vamos a formular el segundo y el tercer teorema de isomorfía, pero los dejo como un ejercicio.

**11.9.11. Teorema (Segundo teorema de isomorfía).** *Sean $R$ un anillo, $S \subseteq R$ un subanillo y $I \subseteq R$ un ideal bilateral. Entonces,*

1) *$S + I := \{x + y \mid x \in S, y \in I\}$ es un subanillo de $R$;*

2) *$I$ es un ideal bilateral en $S + I$;*

3) *la aplicación*

$$\begin{aligned} S &\to (S + I)/I, \\ x &\mapsto x + I \end{aligned}$$

*es un homomorfismo de anillos sobreyectivo que tiene como núcleo a $S \cap I$.*

*Luego, gracias al primer teorema de isomorfía,*

$$S/(S \cap I) \cong (S + I)/I.$$

**11.9.12. Teorema (Tercer teorema de isomorfía).** *Sea $R$ un anillo y sean $I \subseteq J \subseteq R$ ideales bilaterales. Entonces, la aplicación*

$$\begin{aligned} R/I &\to R/J, \\ x + I &\mapsto x + J \end{aligned}$$

*está bien definida y es un homomorfismo sobreyectivo que tiene como núcleo a*

$$J/I := \{x + I \mid x \in J\} \subseteq R/I.$$

*Luego, gracias al primer teorema de isomorfía,*

$$(R/I)/(J/I) \cong R/J.$$

En fin, vamos a describir los ideales en el anillo cociente.

**11.9.13. Teorema.** *Sea $R$ un anillo y sea $I \subseteq R$ un ideal bilateral. Denotemos por $p\colon R \to R/I$ la proyección sobre el anillo cociente dada por $x \mapsto x + I$. Hay una biyección*

$$\begin{aligned} \{\text{ideales bilaterales } J \subseteq R \text{ tales que } I \subseteq J\} &\leftrightarrow \{\text{ideales bilaterales } \overline{J} \subseteq R/I\}, \\ J &\mapsto p(J) = J/I, \\ p^{-1}(\overline{J}) &\hookleftarrow \overline{J}. \end{aligned}$$

*Esta biyección preserva las inclusiones:*

1) *si $I \subseteq J_1 \subseteq J_2$, entonces $J_1/I \subseteq J_2/I$;*

2) *si $\overline{J_1} \subseteq \overline{J_2} \subseteq R/I$, entonces $p^{-1}(\overline{I_1}) \subseteq p^{-1}(\overline{J_2})$.*

*Demostración.* El hecho de que las aplicaciones estén bien definidas sigue de 11.6.12. El homomorfismo $p\colon R \to R/I$ es sobreyectivo, así que para todo ideal $J \subseteq R$ su imagen $p(J)$ es un ideal en $R/I$. Para todo ideal $\overline{J} \subseteq R/I$ la preimagen $p^{-1}(\overline{J})$ es un ideal en $R$. Además, tenemos $0_{R/I} \in \overline{J}$ para todo ideal $\overline{J} \subseteq R/I$ y $p^{-1}(0_{R/I}) = I$, así que $I \subseteq p^{-1}(\overline{J})$.

Hay que ver que las aplicaciones $J \mapsto J/I$ y $\overline{J} \mapsto p^{-1}(\overline{J})$ son mutualmente inversas. Tenemos

$$p^{-1}(\overline{J})/I = \{x + I \mid x \in p^{-1}(\overline{J})\} = \{p(x) \mid p(x) \in \overline{J}\} = \overline{J}$$

y

$$p^{-1}(J/I) = \{x \in R \mid p(x) \in J/I\} = \{x \in R \mid x + I \in J/I\} = J.$$

Está claro que las dos aplicaciones preservan las inclusiones (esto es teoría de conjuntos elemental). ■

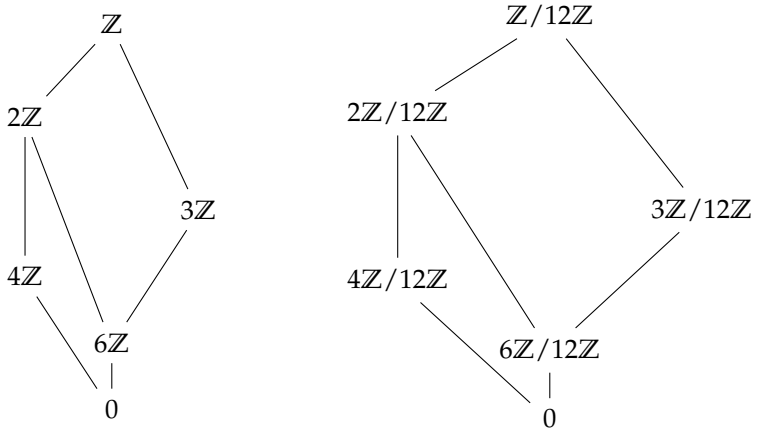
**11.9.14. Ejemplo.** Describamos los ideales en el anillo cociente $\mathbb{Z}/12\mathbb{Z}$. Según el teorema, estos corresponden a los ideales en $\mathbb{Z}$ que contienen a $12\mathbb{Z}$:

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

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:




▲

## 11.10 Productos de anillos

**11.10.1. Definición.** Sea $R_i$, $i \in I$ una familia anillos. El **producto** $\prod_{i\in I} R_i$ es el conjunto

$$\prod_{i\in I} R_i := \{(x_i)_{i\in I} \mid x_i \in R_i\}$$

con la suma y producto definidos término por término:

$$\begin{aligned}
(x_i)_{i\in I} + (y_i)_{i\in I} &:= (x_i + y_i)_{i\in I},\\
(x_i)_{i\in I} \cdot (y_i)_{i\in I} &:= (x_i\, y_i)_{i\in I}.
\end{aligned}$$

Ya que las operaciones se definen término por término, los axiomas de anillos para los $R_i$ implican los axiomas correspondientes para el producto $\prod_{i\in I} R_i$. El cero es el elemento donde $x_i = 0$ para todo $i \in I$ y la identidad es el elemento donde $x_i = 1$ para todo $i \in I$. Notamos que las proyecciones naturales sobre cada uno de los $R_i$:

$$\begin{aligned} p_i \colon \prod_{i\in I} R_i &\twoheadrightarrow R_i, \\ (x_i)_{i\in I} &\mapsto x_i \end{aligned}$$

son homomorfismos de anillos[*].

Cuando $I = \{1, \dots, n\}$ es un conjunto finito, se usa la notación $R_1 \times \cdots \times R_n$.

**11.10.2. Observación (Propiedad universal del producto).** *Sea $R_i$, $i \in I$ una familia de anillos y $S$ cualquier otro anillo. Para toda familia de homomorfismos de anillos $\{f_i \colon S \to R_i\}_{i\in I}$ existe un único homomorfismo de anillos $f \colon S \to \prod_{i\in I} R_i$ tal que $p_i \circ f = f_i$ para todo $i \in I$.*

$$\begin{array}{ccc} S & & \\ {\scriptstyle \exists!}\,\vdots\, {\scriptstyle f}\downarrow & \searrow^{f_i} & \\ \prod_{i\in I} R_i & \xrightarrow[p_i]{} & R_i \end{array}$$

*En otras palabras, hay una biyección natural entre conjuntos*

$$\begin{aligned} \left\{ \textit{homomorfismos } S \to \prod_{i\in I} R_i \right\} &\xrightarrow{\cong} \prod_{i\in I} \{\textit{homomorfismos } S \to R_i\}, \\ f &\mapsto p_i \circ f. \end{aligned}$$

*Demostración.* La condición $p_i \circ f = f_i$ implica que $f$ viene dado por

$$s \mapsto (f_i(s))_{i\in I}.$$

Puesto que cada uno de los $f_i$ es un homomorfismo de anillos, esta fórmula define un homomorfismo de anillos. ■

**11.10.3. Observación.** *Sean $R_1, R_2, R_3$ anillos.*

1) *Hay un isomorfismo natural de anillos $R_1 \times R_2 \cong R_2 \times R_1$.*
2) *Hay isomorfismos naturales $(R_1 \times R_2) \times R_3 \cong R_1 \times (R_2 \times R_3) \cong R_1 \times R_2 \times R_3$.*

*Demostración.* Ejercicio para el lector. Esto se puede deducir de la propiedad universal del producto (véase las pruebas correspondientes para los productos de grupos en el capítulo 10). ■

**11.10.4. Observación ($R \rightsquigarrow R^\times$ preserva productos).** *Sea $R_i$, $i \in I$ una familia de anillos. Hay un isomorfismo natural de grupos*

$$\left(\prod_{i\in I} R_i\right)^\times \cong \prod_{i\in I} R_i^\times.$$

*Demostración.* Dado que el producto en el anillo $\prod_{i\in I} R_i$ está definido término por término, un elemento $(x_i)_{i\in I}$ es invertible en $\prod_{i\in I} R_i$ si y solo si cada $x_i$ es invertible en $R_i$. ■

[*] Note que las inclusiones $R_i \rightarrowtail \prod_{i\in I} R_i$ no son homomorfismos de anillos: la identidad no se preserva.

**11.10.5. Digresión (*).** Otra prueba más general y abstracta puede ser obtenida de 11.4.3. Para cualquier grupo $G$ y anillo $R$ hay una biyección natural

$$\{\text{homomorfismos de anillos } \mathbb{Z}[G] \to R\} \cong \{\text{homomorfismos de grupos } G \to R^\times\}.$$

Junto con la propiedad universal del producto de grupos y de anillos, esto nos da biyecciones *naturales* para cualquier grupo $G$

$$\begin{aligned}\left\{\text{homom. de grupos } G \to \prod_{i\in I} R_i^\times\right\} &\cong \prod_{i\in I}\{\text{homom. de grupos } G \to R_i^\times\}\\ &\cong \prod_{i\in I}\{\text{homom. de anillos } \mathbb{Z}[G] \to R_i\} \cong \left\{\text{homom. de anillos } \mathbb{Z}[G] \to \prod_{i\in I} R_i\right\}\\ &\cong \left\{\text{homom. de grupos } G \to \left(\prod_{i\in I} R_i\right)^\times\right\}.\end{aligned}$$

Esto es suficiente para concluir que $\prod_{i\in I} R_i^\times \cong \left(\prod_{i\in I} R_i\right)^\times$, pero omitiré los detalles. El punto es que el isomorfismo de 11.10.4 puede ser obtenido como una consecuencia formal de 11.4.3.

En el capítulo 10 hemos probado que si $m$ y $n$ son coprimos, entonces hay un isomorfismo de *grupos abelianos* $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. En realidad, esto es un isomorfismo de *anillos*, y ahora estamos listos para probar una generalización.

**11.10.6. Teorema chino del resto**. *Sea $R$ un anillo conmutativo y sean $I_1, \ldots, I_n \subseteq R$ ideales tales que $I_k + I_\ell = R$ para $k \neq \ell$. Luego, hay un isomorfismo natural*

$$R/(I_1 \cdots I_n) \cong R/I_1 \times \cdots \times R/I_n.$$

*Demostración.* Denotemos por $p_k \colon R \to R/I_k$ las proyecciones canónicas $x \mapsto x + I_k$. Estas inducen un homomorfismo de anillos

$$\begin{aligned}R &\to R/I_1 \times \cdots \times R/I_n,\\ x &\mapsto (x + I_1, \ldots, x + I_n).\end{aligned}$$

Vamos a probar que es sobreyectivo y su núcleo es igual al producto de ideales $I_1 \cdots I_n$.

Escribamos $x \equiv y \pmod{I}$ para $x + I = y + I$. Para ver la sobreyectividad, necesitamos probar que para cualesquiera $x_1, \ldots, x_n \in R$ existe $x \in I$ tal que $x \equiv x_k \pmod{I_k}$ para todo $k = 1, \ldots, n$. Tenemos

$$R = R \cdots R = (I_1 + I_2)\,(I_1 + I_3) \cdots (I_1 + I_n) = I + I_2\, I_3 \cdots I_n,$$

donde $I \subseteq I_1$. De hecho, al desarrollar el producto de sumas de ideales (vése el ejercicio 11.13), se ve que todos los términos pertenecen a $I_1$, salvo el último término $I_2\, I_3 \cdots I_n$. Podemos concluir que

$$I_1 + I_2\, I_3 \cdots I_n = R \tag{11.2}$$

En particular, existen $z_1 \in I_1$ e $y_1 \in I_2\, I_3 \cdots I_n$ tales que $z_1 + y_1 = 1$. Tenemos entonces $y_1 \equiv 1 \pmod{I_1}$ e $y_1 \equiv 0 \pmod{I_k}$ para $k \neq 1$. Usando el mismo argumento, podemos ver que existen $y_2, \ldots, y_n$ que satisfacen

$$y_k \equiv 1 \pmod{I_k}, \quad y_k \equiv 0 \pmod{I_\ell} \text{ si } \ell \neq k.$$

El elemento

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

cumple la condición deseada $x \equiv x_k \pmod{I_k}$ para todo $k = 1, \ldots, n$.

Ahora necesitamos calcular el núcleo del homomorfismo $x \mapsto (x + I_1, \ldots, x + I_n)$. Está claro que

$$\ker(x \mapsto (x + I_1, \ldots, x + I_n)) = I_1 \cap \cdots \cap I_n.$$

Vamos a probar que la hipótesis de que $I_k + I_\ell = R$ para $k \neq \ell$ implica que

$$I_1 \cap \cdots \cap I_n = I_1 \cdots I_n.$$

La inclusión que se cumple en cualquier caso es $I_1 \cdots I_n \subseteq I_1 \cap \cdots \cap I_n$, y hay que probar la inclusión inversa.

Procedamos por inducción sobre $n$. Supongamos que $n = 2$ e $I_1 + I_2 = R$. Luego, existen $y \in I_1$ y $z \in I_2$ tales que $y + z = 1$. Para todo $x \in I_1 \cap I_2$ se tiene

$$x = x\,(y + z) = xy + xz \in I_1\, I_2,$$

así que $I_1 \cap I_2 \subseteq I_1\, I_2$.

Para $n > 2$, supongamos que el resultado se cumple para $n - 1$ ideales. Entonces,

$$I_1 \cap \cdots \cap I_n = I_1 \cap (I_2 \cap I_3 \cap \cdots \cap I_n) = I_1 \cap I_2\, I_3 \cdots I_n.$$

Sin embargo, $I_1 + I_2\, I_3 \cdots I_n = R$ (véase (11.2)), así que $I_1 \cap I_2\, I_3 \cdots I_n = I_1\, I_2\, I_3 \cdots I_n$ por el caso de dos ideales. ■

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

$$\mathbb{Z}/a_1 \cdots a_n\mathbb{Z} \cong \mathbb{Z}/a_1\mathbb{Z} \times \cdots \times \mathbb{Z}/a_n\mathbb{Z}.$$

*Demostración.* Para dos ideales $m\mathbb{Z}$ y $n\mathbb{Z}$ en $\mathbb{Z}$ tenemos $m\mathbb{Z} \cdot n\mathbb{Z} = mn\mathbb{Z}$ y $m\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z}$, donde $d = \operatorname{mcd}(m, n)$. En particular, si $m$ y $n$ son coprimos, $m\mathbb{Z} + n\mathbb{Z} = \mathbb{Z}$. Se cumplen las condiciones del teorema anterior y se obtiene un isomorfismo

$$\mathbb{Z}/a_1 \cdots a_n\mathbb{Z} \cong \mathbb{Z}/a_1\mathbb{Z} \times \cdots \times \mathbb{Z}/a_n\mathbb{Z}.$$

■

**11.10.8. Corolario.**

1) *La función de Euler $\phi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$ es multiplicativa: si $m$ y $n$ son coprimos, entonces*

$$\phi(mn) = \phi(m)\,\phi(n).$$

2) *Si $n$ se factoriza en números primos como $p_1^{k_1} \cdots p_\ell^{k_\ell}$, entonces*

$$\phi(n) = \phi(p_1^{k_1}) \cdots \phi(p_\ell^{k_\ell}) = n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_\ell}\right).$$

*Demostración.* Si $m$ y $n$ son coprimos, el isomorfismo de anillos

$$\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

induce un isomorfismo de grupos

$$(\mathbb{Z}/mn\mathbb{Z})^\times \cong (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times,$$

como notamos en 11.10.4. De aquí sigue 1). La parte 2) se demuestra de la misma manera o por inducción usando la parte 1). La fórmula

$$\phi(p^k) = p^k\left(1 - \frac{1}{p}\right)$$

fue obtenida en el capítulo 4. ■

En el capítulo 10 hemos probado la multiplicatividad de la función $\phi$ de Euler usando que los elementos de $(\mathbb{Z}/n\mathbb{Z})^\times$ son los generadores del grupo cíclico $\mathbb{Z}/n\mathbb{Z}$. La prueba de arriba es más natural.

## 11.11 Ejercicios

### Subanillos

Corto 1
23.08.18

**Ejercicio 11.1.** *Verifique que hay una cadena de subanillos*

$$\mathbb{Z}[\sqrt{5}] \subset \mathbb{Z}\Big[\frac{1+\sqrt{5}}{2}\Big] \subset \mathbb{R}$$

*donde*

$$\mathbb{Z}[\sqrt{5}] := \{a + b\sqrt{5} \mid a, b \in \mathbb{Z}\}, \quad \mathbb{Z}\Big[\frac{1+\sqrt{5}}{2}\Big] := \Big\{a + b\,\frac{1+\sqrt{5}}{2} \;\Big|\; a, b \in \mathbb{Z}\Big\}.$$

**Ejercicio 11.2.** *Consideremos el anillo de las funciones $f\colon \mathbb{R} \to \mathbb{R}$ respecto a las operaciones* ***punto por punto***

$$(f+g)(x) := f(x) + g(x), \quad (f \cdot g)(x) := f(x) \cdot g(x).$$

*Demuestre que hay una cadena de subanillos*

$$\{\textit{funciones constantes } \mathbb{R} \to \mathbb{R}\} \subset \{\textit{funciones polinomiales } \mathbb{R} \to \mathbb{R}\}$$
$$\subset \{\textit{funciones continuas } \mathbb{R} \to \mathbb{R}\} \subset \{\textit{funciones } \mathbb{R} \to \mathbb{R}\}.$$

### Homomorfismos de anillos

**Ejercicio 11.3.** *Sea $R$ un anillo conmutativo y $M_n(R)$ el anillo de las matrices de $n \times n$ con coeficientes en $R$. ¿Cuáles aplicaciones de abajo son homomorfismos?*

1) *La proyección*
$$\begin{pmatrix} x_{11} & x_{12} & \cdots & x_{1n} \\ x_{21} & x_{22} & \cdots & x_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ x_{n1} & x_{n2} & \cdots & x_{nn} \end{pmatrix} \mapsto x_{11}.$$

2) *La traza*
$$\begin{pmatrix} x_{11} & x_{12} & \cdots & x_{1n} \\ x_{21} & x_{22} & \cdots & x_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ x_{n1} & x_{n2} & \cdots & x_{nn} \end{pmatrix} \mapsto x_{11} + x_{22} + \cdots + x_{nn}.$$

3) *El determinante $A \mapsto \det A$.*

**Ejercicio 11.4.** *Sea $f\colon R \to S$ un homomorfismo de anillos conmutativos y sea $n = 1, 2, 3, \ldots$*

1) *Demuestre que $f$ induce un homomorfismo de los anillos de matrices correspondientes $f_*\colon M_n(R) \to M_n(S)$ dado por*
$$\begin{pmatrix} x_{11} & x_{12} & \cdots & x_{1n} \\ x_{21} & x_{22} & \cdots & x_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ x_{n1} & x_{n2} & \cdots & x_{nn} \end{pmatrix} \mapsto \begin{pmatrix} f(x_{11}) & f(x_{12}) & \cdots & f(x_{1n}) \\ f(x_{21}) & f(x_{22}) & \cdots & f(x_{2n}) \\ \vdots & \vdots & \ddots & \vdots \\ f(x_{n1}) & f(x_{n2}) & \cdots & f(x_{nn}) \end{pmatrix}.$$

2) *Demuestre que $f$ induce un homomorfismo de grupos $\mathrm{GL}_n(f)\colon \mathrm{GL}_n(R) \to \mathrm{GL}_n(S)$.*

3) *Demuestre que el diagrama de homomorfismos de grupos*

$$\begin{array}{ccc} \mathrm{GL}_n(R) & \xrightarrow{\det} & R^\times \\ {\scriptstyle \mathrm{GL}_n(f)}\downarrow & & \downarrow{\scriptstyle f^\times} \\ \mathrm{GL}_n(S) & \xrightarrow[\det]{} & S^\times \end{array}$$

*conmuta.*

*(Sugerencia: use la fórmula* $\det(x_{ij}) = \sum_{\sigma\in S_n} \operatorname{sgn}\sigma \cdot x_{1\sigma(1)}\cdots x_{n\sigma(n)}$*.)*

**Ejercicio 11.5.** *Sea $R$ un anillo conmutativo. Calcule $Z(M_n(R))$, el centro del anillo de las matrices de $n \times n$ con coeficientes en $R$.*
*(Véanse los ejercicios donde calculamos el centro del grupo lineal general* $\mathrm{GL}_n(R)$*.)*

**Ejercicio 11.6.**

1) *Demuestre que un isomorfismo de anillos $R \to S$ se restringe a un isomorfismo de grupos $R^\times \to S^\times$.*

2) *Demuestre que los anillos de polinomios $\mathbb{Z}[X]$ y $\mathbb{Q}[X]$ no son isomorfos.*

**Ejercicio 11.7.** *Sea $f\colon R \to S$ un homomorfismo sobreyectivo de anillos. Demuestre que $f(Z(R)) \subseteq Z(S)$.*

## Álgebra de grupo

**Ejercicio 11.8.** *Sea $R$ un anillo conmutativo y $G$ un grupo. Demuestre que*

$$\epsilon\colon R[G] \twoheadrightarrow R, \quad \sum_{g\in G} a_g\, g \mapsto \sum_{g\in G} a_g$$

*es un homomorfismo sobreyectivo de anillos.*

**Ejercicio 11.9.** *Sea $R$ un anillo conmutativo y $G$ un grupo finito. Consideremos $t := \sum_{g\in G} 1\cdot g \in R[G]$. Demuestre que $t^2 = |G|\, t$.*

**Ejercicio 11.10.** *En este ejercicio vamos a calcular el centro del álgebra de grupo $R[G]$. Consideremos*

$$x = \sum_{g\in G} a_g\, g \in R[G].$$

1) *Demuestre que $x \in Z(R[G])$ si y solamente si $h\,x = x\,h$ para todo $h \in G$.*

2) *Deduzca que $x \in Z(R[G])$ si y solamente si $a_g = a_{hgh^{-1}}$ para cualesquiera $g, h \in G$.*

*Entonces, el centro de $R[G]$ consiste en los elementos $\sum_{g\in G} a_g\, g$ cuyos coeficientes $a_g$ son constantes sobre las clases de conjugación de $G$.*

Corto 2
30.08.18

**Ejercicio 11.11.** *Sea $R$ un anillo conmutativo y $G$ un grupo. Consideremos el homomorfismo*

$$\epsilon\colon R[G] \twoheadrightarrow R, \quad \sum_{g\in G} a_g\, g \mapsto \sum_{g\in G} a_g.$$

1) *Demuestre que el ideal $I_G := \ker\epsilon$ está generado por los elementos $g - e$ para $g \in G$. Este se llama el* ***ideal de aumento****.*

2) *En particular, si $G = C_n = \{e, g, \ldots, g^{n-1}\}$ es el grupo cíclico de orden $n$ generado por $g$, demuestre que $\ker\epsilon$ está generado por el elemento $g - e$.*

## Ideales

**Ejercicio 11.12.** *Sea $R$ un anillo y $S \subseteq R$ un subanillo.*

1) *Demuestre que para todo ideal $I \subseteq R$ (izquierdo, derecho, bilateral) la intersección $I \cap S$ es un ideal en $S$ (izquierdo, derecho, bilateral).*

2) *Encuentre un ejemplo de $S \subseteq R$ donde no todos los ideales de $S$ son de la forma $I \cap S$.*

**Ejercicio 11.13.** *Sea $R$ un anillo y sean $I, J, K$ ideales bilaterales. Demuestre que $I(J+K) = IJ + IK$ y $(I+J)K = IK + JK$.*

**Ejercicio 11.14.** *Sea $R$ un anillo. Para un ideal izquierdo $I \subseteq R$ definamos el **aniquilador** por*

$$\operatorname{Ann} I := \{r \in R \mid rx = 0 \text{ para todo } x \in I\}.$$

*Demuestre que esto es un ideal bilateral en $R$.*

**Ejercicio 11.15.** *Sea $R$ un anillo conmutativo y $M_n(R)$ el anillo de matrices correspondiente.*

1) *Sea $I \subseteq R$ un ideal. Denotemos por $M_n(I)$ el conjunto de las matrices que tienen como sus entradas elementos de $I$. Verifique que $M_n(I)$ es un ideal bilateral en $M_n(R)$.*

2) *Sea $J \subseteq M_n(R)$ un ideal bilateral. Sea $I$ el conjunto de los coeficientes que aparecen en la entrada $(1,1)$ de las matrices que pertenecen a $J$. Demuestre que $I$ es un ideal en $R$.*

3) *Demuestre que $J = M_n(I)$. (Use las mismas ideas de 11.6.11.)*

*Entonces, todo ideal en el anillo de matrices $M_n(R)$ es de la forma $M_n(I)$ para algún ideal $I \subseteq R$. Esto generaliza el resultado de 11.6.11.*

## Nilradical y radical

**Ejercicio 11.16.** *Sea $R$ un anillo conmutativo.*

1) *Demuestre que el conjunto de nilpotentes*

$$N(R) := \{x \in R \mid x^n = 0 \text{ para algún } n = 1, 2, 3, \ldots\}$$

*es un ideal en $R$. Este se llama el **nilradical** de $R$.*

2) *Demuestre que en el anillo no conmutativo $M_n(R)$ los nilpotentes no forman un ideal.*

**Ejercicio 11.17.** *Sea $R$ un anillo conmutativo. Supongamos que el nilradical de $R$ es finitamente generado; es decir, $N(R) = (x_1, \ldots, x_n)$ donde $x_i$ son algunos nilpotentes. Demuestre que en este caso $N(R)$ es un **ideal nilpotente**:*

$$N(R)^m := \underbrace{N(R) \cdots N(R)}_{m} = 0$$

*para algún $m = 1, 2, 3, \ldots$*

**Ejercicio 11.18.** *Sea $R$ un anillo conmutativo y sea $I \subseteq R$ un ideal. Demuestre que*

$$\sqrt{I} := \{x \in R \mid x^n \in I \text{ para algún } n = 1, 2, 3, \ldots\}$$

*es también un ideal en $R$, llamado el **radical** de $I$. (Note que el nilradical $N(R) = \sqrt{(0)}$ es un caso particular.)*

## Operaciones I y V

**Ejercicio 11.19 (*).** *Sea $k$ un cuerpo. Sean $J, J_1, J_2$ ideales en $k[X_1, \ldots, X_n]$ y sean $X, Y$ subconjuntos de $\mathbb{A}^n(k)$. Demuestre las siguientes relaciones.*

*0) $I(\emptyset) = k[X_1, \ldots, X_n]$, $V(0) = \mathbb{A}^n(k)$, $V(1) = V(k[X_1, \ldots, X_n]) = \emptyset$.*

*1) Si $J_1 \subseteq J_2$, entonces $V(J_2) \subseteq V(J_1)$.*

*2) Si $X \subseteq Y$, entonces $I(Y) \subseteq I(X)$.*

*3) $V(J) = V(\sqrt{J})$.*

*4) $J \subseteq \sqrt{J} \subseteq IV(J)$. Demuestre que la inclusión es estricta para $J = (X^2 + 1) \subset \mathbb{R}[X]$.*

*5) $X \subseteq VI(X)$.*

*6) $VIV(J) = V(J)$ y $IVI(X) = I(X)$.*

**Ejercicio 11.20 (**).**

*1) Demuestre que $I(\mathbb{A}^n(k)) = (0)$ si $k$ es un cuerpo infinito.*

*2) Note que $X^p - X \in I(\mathbb{A}^1(\mathbb{F}_p))$, así que esto es falso para cuerpos finitos.*

## Anillos cociente

Corto 3
06.09.18

**Ejercicio 11.21.** *Sea $R$ un anillo conmutativo y sea $N(R)$ su nilradical. Demuestre que el anillo cociente $R/N(R)$ no tiene nilpotentes; es decir, $N(R/N(R)) = 0$.*

**Ejercicio 11.22.** *Sea $R$ un anillo conmutativo y sea $I \subseteq R$ un ideal. Demuestre que $M_n(R)/M_n(I) \cong M_n(R/I)$.*

**Ejercicio 11.23.** *Sea $k$ un cuerpo y $c \in k$. Consideremos el homomorfismo de evaluación*

$$ev_c \colon k[X] \to k, \quad f \mapsto f(c).$$

*1) Demuestre que $\ker ev_c = (X - c)$ es el ideal generado por el polinomio lineal $X - c$.*

*2) Deduzca del primer teorema de isomorfía que $k[X]/(X - c) \cong k$.*

*3*) De modo similar, demuestre que para $c_1, \ldots, c_n \in k$ se tiene $k[X_1, \ldots, X_n]/(X_1 - c_1, \ldots, X_n - c_n) \cong k$. Sugerencia: considere el automorfismo de $k[X_1, \ldots, X_n]$ dado por $X_i \mapsto X_i + c_i$.*

**Ejercicio 11.24.** *Demuestre que el cociente $\mathbb{Q}[X]/(X^2 + 5)$ es isomorfo al cuerpo*

$$\mathbb{Q}(\sqrt{-5}) := \{x + y\sqrt{-5} \mid x, y \in \mathbb{Q}\}$$

*(en particular, verifique que $\mathbb{Q}(\sqrt{-5})$ es un cuerpo).*

**Ejercicio 11.25.** *Para el anillo de los enteros de Gauss $\mathbb{Z}[\sqrt{-1}]$ demuestre que*

$$\mathbb{Z}[\sqrt{-1}]/(1 + \sqrt{-1}) \cong \mathbb{Z}/2\mathbb{Z}, \quad \mathbb{Z}[\sqrt{-1}]/(1 + 2\sqrt{-1}) \cong \mathbb{Z}/5\mathbb{Z}.$$

**Ejercicio 11.26.** *Consideremos el anillo de los enteros de Gauss $\mathbb{Z}[\sqrt{-1}]$ y los ideales*

$$I = (1 + \sqrt{-1}), \quad J = (1 + 2\sqrt{-1}).$$

1) *Demuestre que* $I + J = \mathbb{Z}[\sqrt{-1}]$.

2) *Demuestre que* $IJ = (1 - 3\sqrt{-1})$.
*Sugerencia: note que en cualquier anillo conmutativo, se tiene* $(x) \cdot (y) = (xy)$ *para cualesquiera* $x, y \in R$.

3) *Demuestre que* $\mathbb{Z}[\sqrt{-1}]/(1 - 3\sqrt{-1}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ *usando el teorema chino del resto.*

**Ejercicio 11.27.** *Demuestre el segundo teorema de isomorfía para anillos.*

**Ejercicio 11.28.** *Demuestre el tercer teorema de isomorfía para anillos.*

## Productos de anillos

**Ejercicio 11.29.** *Sean* $R$ *y* $S$ *anillos y sean* $I \subseteq R$, $J \subseteq S$ *ideales bilaterales.*

1) *Demuestre que*
$$I \times J := \{(x, y) \mid x \in I,\ y \in J\}$$
*es un ideal bilateral en el producto* $R \times S$.

2) *Demuestre que todos los ideales bilaterales en* $R \times S$ *son de esta forma.*
*Sugerencia: para un ideal bilateral* $A \subseteq R \times S$ *considere* $I = p_1(A)$ *y* $J = p_2(A)$ *donde*
$$\begin{array}{ccccc} R & \xleftarrow{p_1} & R \times S & \xrightarrow{p_2} & S \\ r & \longleftarrow\!\shortmid & (r, s) & \shortmid\!\longrightarrow & s \end{array}$$
*son las proyecciones canónicas.*

**Ejercicio 11.30.**

1) *Sean* $R$ *y* $S$ *dos anillos no nulos. Demuestre que el producto* $R \times S$ *tiene divisores de cero.*

2) *Demuestre que el producto de dos anillos no nulos nunca es un cuerpo.*
*Sugerencia: para un ideal bilateral* $A \subseteq R \times S$ *considere* $I = p_1(A)$ *y* $J = p_2(A)$ *donde*
$$\begin{array}{ccccc} R & \xleftarrow{p_1} & R \times S & \xrightarrow{p_2} & S \\ r & \longleftarrow\!\shortmid & (r, s) & \shortmid\!\longrightarrow & s \end{array}$$
*son las proyecciones canónicas.*

# Bibliografía

[Ful2008] William Fulton, *Algebraic curves. An introduction to algebraic geometry*, 2008.
http://www.math.lsa.umich.edu/~wfulton/CurveBook.pdf

[Lam2001] Tsit-Yuen Lam, *A first course in noncommutative rings*, second ed., Graduate Texts in Mathematics, vol. 131, Springer-Verlag New York, 2001.
http://dx.doi.org/10.1007/978-1-4419-8616-0