# Capítulo 3

# Anillos

---

**Objetivos del capítulo**

- Se recuerda el concepto abstracto de relación binaria. Se estudian las propiedades asociadas a una relación binaria. Se pretende que propiedades que han sido estudiadas en diferentes momentos se asimilen como un mismo concepto, por ejemplo unicidad del inverso en aplicaciones biyectivas o en $\mathbb{Z}_n$.
- Se introduce la noción abstracta de Anillo y sus propiedades (anillo conmutativo, unitario). Se estudian los elementos inversibles de un anillo introduciendo la noción de anillos de división y cuerpo.
- Se empiezan a estudiar métodos para encontrar Anillos nuevos a partir de anillos dados: se estudian subanillos. La suma y el producto directo de anillos, Los anillos de matrices, de polinomios y de series formales. Se estudian el anillos de endomorfismos de un grupo abeliano.
- Se estudian las aplicaciones naturales entre anillos, los homomorfismos de anillos y sus propiedades.
- Se estudia la unitización y la característica de un anillo.

---

## 1. Operación binaria, semigrupo, monoide.

**Definición 1** Sea $X$ un conjunto no vacío. Se define una **operación binaria** en $X$ como una aplicación $* : X \times X \to X$. Normalmente, un conjunto con una operación binaria se denotará por $(X, *)$.

**Nota:** Genéricamente dados $a, b \in X$ denotaremos al producto de $a$ con $b$ como $a * b$ y se leerá $a$ operado con $b$. En casos concretos nos van a aparecer dos notaciones distinta de producto (de hecho, ya estamos acostumbrados a ellas):

- La notación multiplicativa, $a * b$, $a \cdot b$ o simplemente $ab$ (la operación simplemente se denota por yuxtaposición)
- La notación aditiva, $a + b$ (la operación se denota por "+").

**Ejemplos A**

⋆ La suma o el producto en $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Z}_n$, $\mathbb{Q}$ o $\mathbb{R}$.

⋆ La resta en $\mathbb{Z}$, $\mathbb{Q}$ o $\mathbb{R}$ (la resta no es operación en $\mathbb{N}$).

⋆ La división no es operación binaria en ninguno de estos conjuntos.

⋆ La división es una operación binaria en $\mathbb{Q} - \{0\}$ o $\mathbb{R} - \{0\}$.

⋆ El máximo común divisor y el mínimo común múltiplo son operaciones binarias en $\mathbb{Z}$.

⋆ La unión, la intersección, la diferencia o la diferencia simétrica son operaciones binarias.

⋆ La composición de aplicaciones es una operación binaria en $\Delta := \{f \mid f : X \to X\}$.

⋆ Dado un conjunto no vacío $X$, las siguientes son operaciones binarias en $X$: dado $c \in X$, para todo $a, b \in X$ definimos,

$$\begin{aligned} a * b &= a \\ a * b &= b \\ a * b &= c \end{aligned}$$

**Definición 2** Sea $X$ un conjunto no vacio y $*$ una operación en $X$. Se dice que $*$

- es **asociativa** si $\forall\ a, b, c \in X, \quad a * (b * c) = (a * b) * c.$
- es **conmutativa** si $\forall\ a, b \in X, \quad a * b = b * a.$
- Posee elemento **neutro por la derecha** si existe $e \in X$ tal que $\forall\ a \in X$, $a * e = a$.
- Posee elemento **neutro por la izquierda** si existe $e \in X$ tal que $\forall\ a \in X$, $e * a = a$.
- Posee elemento neutro si existe elemento **neutro** por la izquierda y por la derecha.

**Lema 3** Si $e$ es neutro por la izquierda y $e'$ es neutro por la derecha, entonces $e = e'$. Por lo que el elemento neutro, caso de existir es único.

$$e' = e * e' = e.$$

$e$ es neutro por la izquierda

$e'$ es neutro por la derecha

**Corolario 4** Sea $X$ un conjunto no vacío y $*$ una operación en $X$. Entonces, si $*$ posee un elemento neutro éste es único.

**Demo:** Corolario trivial de lo anterior. ■

**Nota:** Sea $X$ un conjunto con una operación que posee elemento neutro. Dependiendo de que notación estemos usando para denotar dicha operación así denotaremos al elemento neutro:

- En notación multiplicativa (la operación se denota por $*$, $\cdot$ o por yuxtaposición): al elemento neutro se le suele denotar por $e$ o a veces por 1.
- En notación aditiva (la operación se denota por $+$): al elemento neutro se le suele denotar por 0.

**Definición 5** Sea $X$ un conjunto no vacío y $*$ una operación en $X$.

• Diremos que $(X, *)$ es un **semigrupo** si $*$ es asociativa.

• Diremos que $(X, *)$ es un **monoide** si $*$ es asociativa con elemento unidad (normalmente denotado por $e$, si la notación es multiplicativa, a veces, por 1 y si es aditiva, por 0).

• Un monoide $(X, *)$ con operación $*$ conmutativa se dirá **monoide conmutativo**.

**Nota:** Tal como su nombre indica, en una operación binaria podemos operar elementos de dos en dos. Por tanto, en principio, no tiene sentido expresiones tales como $a * b * c$. No obstante, si $*$ es asociativa tenemos que $(a * b) * c = a * (b * c)$. El siguiente teorema demuestra que es innecesario el uso de paréntesis en una operación asociativa.

**Teorema 6** *Sea $(X, *)$ un semigrupo. Entonces el producto arbitrario de $n$ elementos de $X$ es independiente de la disposición de los paréntesis.*

✔**Demo:** Por hipótesis

$$(a * b) * c = a * (b * c)$$

por lo que lo podremos denotar por $a * b * c$.

$$(((a * b) * c) * d) = (a * b) * (c * d) = (a * (b * (c * d)))$$

se denotará por $a * b * c * d$. Supongamos que en un producto de $n - 1$ elementos no afecta la posición de los paréntesis y consideremos un producto de $n$ términos. Entonces:

♦ Los paréntesis del último producto serán $(a_1 * \cdots * a_k) * (a_{k+1} * \cdots * a_n)$ para algún $k \in \{1, \ldots, n-1\}$. Por la hipótesis de inducción los paréntesis interiores a éstos pueden ordenarse como mejor nos convenga. Por último, al ser la operación asociativa:

$$(a_1 * \cdots * a_k) * (a_{k+1} * (a_{k+1} * \cdots * a_n)) = (a_1 * \cdots * a_{k+1}) * (a_{k+2} * \cdots * a_n)$$
$$((a_1 * \cdots * a_{k-1}) * a_k) * (a_{k+1} * \cdots * a_n) = (a_1 * \cdots * a_{k-1}) * (a_k * \cdots * a_n)$$

Por lo que el último producto, y por tanto todos, pueden ser cambiados a nuestro antojo. Lo que demuestra el teorema. ■

**Nota:** Observar que aquí teníamos que demostrar que una propiedad era cierta para todo natural mayor que 3 y hemos adaptado el principio de inducción generalizado a este caso.

**Definición 7** Sea $(M, *)$ un monoide con elemento unidad $e$. Diremos que un elemento $a \in X$ posee

- **Inverso por la izquierda** si existe $b \in X$ tal que $b * a = e$.
- **Inverso por la derecha** si existe $b \in X$ tal que $a * b = e$.
- **Inverso** si existe $b \in X$ tal que $a * b = e = b * a$.

**Lema 8** Sea $(M, *)$ un monoide con elemento neutro $e$ y sea $a \in M$. Entonces:

(i) Si $a$ tiene un inverso por la izquierda y un inverso por la derecha, ambos coinciden y $a$ es inversible.

(ii) Si $a$ posee inverso éste es único. Por tanto lo denotaremos de forma especial. Así, el inverso de un elemento $a \in M$ se denotará por:

- $a^{-1}$ si estamos en notación multiplicativa.
- $-a$ si estamos en notación aditiva.

**Demo:** Sea $b$ inverso por la izquierda de $a$ y $b'$ inversos por la derecha de $a$. Tenemos entonces que

$$b' = e * b' = (b * a) * b' = b * (a * b') = b * e = b. \qquad \blacksquare$$

**Nota:** El inverso de un elemento no tiene porqué existir: por ejemplo en $(\mathbb{Z}_6, \cdot)$ ($\mathbb{Z}_6$ con el producto) $\overline{3}$ no tiene inverso [no hay ningún elemento de $\mathbb{Z}_6$ que cuando lo multiplico por $\overline{3}$ me de $\overline{1}$]. En $\mathbb{Z}$ con el producto no suele haber inversos (solo el 1 y el $-1$ tienen inversos). Por tanto, aunque sea muy grande la tentación (por ejemplo para resolver un ejercicio) si $a \in G$ ($G$ un conjunto con una operación) no puede aparecer de improviso el elemento $a^{-1}$ a no ser que demostremos que $a$ posee inverso, en particular $G$ tiene que ser un monoide.
**Nota:** Ya hemos estudiado muchos elementos inversible en este curso: Los opuestos para la suma en $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ ó $\mathbb{Z}_n$ verifican esta propiedad. Los inversos en $\mathbb{R}, \mathbb{Q}, \mathbb{Z}_n$ o las aplicaciones inversibles verifican esta propiedad.

**Definición 9** Sea $(M, *)$ un monoide. Se dice que un elemento $a \in M$ es una **unidad de** $M$, si es un elemento inversible de $M$. El conjunto de las unidades de un monoide $M$ se denota por $\mathcal{U}(M)$.

**Proposición 10** Sea $(M, *)$ un monoide y sean $a, b \in M$. Entonces:

(i) El elemento neutro de $M$ es una unidad.

(ii) Si $a$ es una unidad, $a^{-1}$ es una unidad y $(a^{-1})^{-1} = a$.

(iii) Si $a$ y $b$ son unidades de $M$, $a * b$ es una unidad de $M$ y $(a * b)^{-1} = b^{-1} * a^{-1}$.

(iv) En general el producto arbitrario de unidades es una unidad.

$$(a_1 * \cdots * a_{n-1} * a_n)^{-1} = a_n^{-1} * a_{n-1}^{-1} * \cdots * a_1^{-1}$$

**Demo:** (i) y (ii) son triviales.
(iii) Veamos que $b^{-1} * a^{-1}$ es el inverso de $a * b$:

$$\begin{aligned} (a * b) * (b^{-1} * a^{-1}) &= a * (b * b^{-1}) * a^{-1} = a * e * a^{-1} = e \\ (b^{-1} * a^{-1}) * (a * b) &= b^{-1} * (a^{-1} * a) * b = b^{-1} * e * b = e \end{aligned}$$

(iv) Vamos a dar una demostración por inducción: el caso $n = 2$ es el apartado anterior. Supongamos que el resultado es cierto para $n - 1$, entonces:

$$\begin{aligned} (a_1 * \cdots * a_{n-1} * a_n)^{-1} &= ((a_1 * \cdots * a_{n-1}) * a_n)^{-1} = a_n^{-1} * (a_1 * \cdots * a_{n-1})^{-1} \\ &= a_n^{-1} * a_{n-1}^{-1} \cdots * a_1^{-1} \end{aligned}$$

Lo que demuestra la proposición. $\blacksquare$

**Ejemplos B** Veamos cuales son las unidades en algunas operaciones binarias estudiadas:

$\star$ En $(\mathbb{N}, \cdot)$ sólo 1 es unidad. En $(\mathbb{Z}, \cdot)$ las unidades son $\{1, -1\}$.

$\star$ En $(\mathbb{Q}, \cdot)$ o $(\mathbb{R}, \cdot)$ las unidades son, respectivamente $\mathbb{Q} - \{0\}$ y $\mathbb{R} - \{0\}$.

$\star$ Para $(\Delta, \circ)$ con $\Delta = \{f \mid f : X \to X\}$ y $\circ$ la composición, las unidades son las aplicaciones biyectivas.

$\star$ En $(\mathbb{Z}_n, \cdot)$ las unidades son los elementos $\overline{a} \in \mathbb{Z}_n$ tales que $\mathrm{m.\,c.\,d}(n, a) = 1$.

$\star$ En $(\mathcal{M}_n(\mathbb{R}), +)$, suma de matrices, todo elemento es unidad, mientras que en $(\mathcal{M}_n(\mathbb{R}), \cdot)$ las matrices de determinante no nulo (las inversibles) son las unidades.

$\star$ Sea $X$ un conjunto no vacio. En $(\mathcal{P}(X), \cup)$ sólo $\emptyset$, que es el elemento neutro, es unidad. En $(\mathcal{P}(X), \cap)$ sólo $X$, que es el elemento neutro, es unidad. En $(\mathcal{P}(X), \triangle)$, todo elemento es unidad. ¿Quien es el elemento neutro?

# 2. Nociones básicas sobre Anillos

## 2.1. Definiciones y ejemplos

**Definición 1** Sea $G$ un conjunto no vacío y $*$ una operación en $G$. Diremos que $(G, *)$ es un **grupo** si:

- $*$ es asociativa.
- $*$ tiene elemento unidad, normalmente denotado por $e$.
- Todo elemento de $G$ tiene inverso.

Si además $*$ es conmutativa se dirá que $G$ es un **grupo abeliano**.

**Ejemplos A** $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{Z}_n$ son grupos abelianos respecto de la suma. $\mathbb{Q} - \{0\}$ y $\mathbb{R} - \{0\}$ son grupos abelianos respecto del producto. $(\mathcal{P}(X), \triangle)$ es un grupo abeliano para cualquier conjunto no vacío $X$. El conjunto de las matrices inversibles en $\mathcal{M}_2(\mathbb{R})$ con el producto es un grupo no abeliano.

**Definición 2** Un **anillo** es una terna $(R, +, \cdot)$ en donde $R$ es un conjunto y "+", "$\cdot$" son dos operaciones en $R$ tales que:

(1) $(R, +)$ es un grupo abeliano:

- Propiedad asociativa: $(a + b) + c = a + (b + c)$ para todo $a, b, c \in R$.
- Elemento neutro: existe $0 \in R$ tal que $a + 0 = 0 + a$ para todo $a \in R$
- Elemento opuesto: para todo $a \in R$ existe $-a \in R$ tal que

$$a + (-a) = (-a) + a = 0.$$

- Propiedad conmutativa: $a + b = b + a$ para todo $a, b \in R$.

(2) $(R, \cdot)$ verifica la propiedad asociativa: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ para todo $a, b, c \in R$.

(3) Se verifican las propiedades distributivas: para todos $a, b, c \in R$,

$$(a+b)\cdot c = a\cdot c + b\cdot c \qquad c\cdot(a+b) = c\cdot a + c\cdot b$$

⋆ Diremos que un **anillo** $(R, +, \cdot)$ es **conmutativo** si "$\cdot$" es conmutativa.
⋆ Diremos que un **anillo** $(R, +, \cdot)$ es **unitario** si "$\cdot$" es una operación unitaria y $R$ tiene más de un elemento (0 y 1 son dos elementos distintos de $R$).

**Nota:** La primera operación se llamará **suma**. El neutro de la suma lo denotaremos por 0. Al inverso de la suma lo llamaremos **Opuesto**. La segunda operación se llamará **producto** y la denotaremos por yuxtaposición. Al neutro del producto lo denotaremos, si existe, por 1. El inverso del producto, si existe, se llamará **inverso**.

**Ejemplos B**

- Si consideramos $(G, +)$ un grupo abeliano y definimos un producto en $G$ por: $a \cdot b := 0$ para todo $a, b \in G$, $(G, +, \cdot)$ tiene estructura de anillo conmutativo.
- $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ con las operaciones usuales (todos son anillos conmutativos y unitarios). $\mathcal{M}_n(\mathbb{R})$, el anillo de matrices sobre los Reales, con las operaciones usuales (anillo unitario, no conmutativo para $n \geq 2$). $2\mathbb{Z}$ con las operaciones usuales de $\mathbb{Z}$ (anillo conmutativo no unitario).
- Los anillos realmente no tienen que ser de "números": sea $X$ un conjunto no vacío y denotemos por $\mathcal{P}(X)$ el conjunto de partes de $X$. Entonces $(\mathcal{P}(X), \triangle, \cap)$ tiene estructura de anillo conmutativo y unitario.

  **Nota:** $\triangle$ denota la diferencia simétrica: dados $A, B \subset X$,

  $$A \triangle B := (A - B) \cup (B - A) = (A \cap B^c) \cup (B \cap A^c)$$

- Los anillos módulo n: Sea $n$ un número natural y consideremos

  $$\mathbb{Z}_n := \{0, 1, 2, \ldots, n-1\}.$$

  Observar que $\mathbb{Z}_n$ tiene $n$ elementos. Dados $a, b \in \mathbb{Z}_n$ definimos:

  - La suma de $a$ y $b$ como el resto de dividir $a + b$ por $n$.
    ⋆ $(\mathbb{Z}_n, +)$ es el grupo abeliano ya estudiado anteriormente.
  - El producto de $a$ y $b$ como el resto de dividir $a \cdot b$ por $n$.
    Entonces $(\mathbb{Z}_n, +, \cdot)$ tiene estructura de anillo conmutativo y unitario, $n \geq 2$.

**Proposición 3** Sea $(R, +, \cdot)$ un anillo. Entonces:

(i) $0 \cdot a = a \cdot 0 = 0$ para todo $a \in R$.

(ii) $a \cdot (-b) = -(a \cdot b) = (-a) \cdot b$ para todo $a, b \in R$.
Si además $R$ es unitario,

(iii) la unidad es única.

(iv) Si $a \in R$ es un elemento inversible, el inverso de $a$ es único (lo denotamos por $a^{-1}$).

✔ **Demo:** (i). Sabemos que al ser 0 el neutro de la suma, $0 + 0 = 0$. Por tanto,

$$0a = (0 + 0)a = 0a + 0a$$

Simplemente hemos aplicado la distributiva de la suma. Ahora, Si sumamos en ambos lados de la igualdad el opuesto de $0a$ tenemos,

$$0 = (-0a) + 0a = (-0a) + (0a + 0a) = ((-0a) + 0a) + 0a = 0 + 0a = 0a$$

El caso $a0 = 0$ se demuestra de forma análoga.

(ii). Queremos ver que $a(-b) = -(ab)$, es decir, que $a$ por el opuesto de $b$ es el opuesto de $ab$. Pero

$$ab + a(-b) = a(-b) + ab = a((-b) + b) = a0 = 0$$

por lo que cuando a $ab$ le sumo $a(-b)$ me da cero. Esto nos dice exactamente que el opuesto de $a$ es $a(-b)$ (ya que el opuesto es único), es decir, $-(ab) = a(-b)$. de forma análoga se demuestra que $-(ab) = (-a)b$.

(iii) y (iv). Sabemos que en cualquier operación, en particular para el producto de un anillo $R$ la unidad caso de existir es única y el inverso de un elemento, caso de existir, es único. ■

**Corolario 4 (Ejercicio)** *Sea $(R, +, \cdot)$ un anillo unitario. Entonces $0 \neq 1$.*

**Ejemplos C** *A los elementos inversibles de un anillo $R$ se les denomina unidades. El conjunto de las unidades de un anillo $R$ se denota por $\mathcal{U}(R)$.*

**Corolario 5 (Ejercicio)** *Sea $(R, +, \cdot)$ un anillo unitario. Entonces $(\mathcal{U}(R), \cdot)$ tiene estructura de grupo. Es más, si $R$ es conmutativo, $\mathcal{U}(R)$ es un grupo abeliano.*

**Definición 6** Se dice que un anillo $(R, +, \cdot)$ es un **anillo de división** si es unitario y todo elemento no nulo de $R$ tiene inverso. Si además es conmutativo, se dice que $(R, +, \cdot)$ es un **cuerpo**.

**Nota:** $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ son cuerpos. Si $p$ es un número primo, $\mathbb{Z}_p$, el anillo de congruencias módulo $p$, es un cuerpo (se ha demostrado en el corolario 7 (Pag. 40)).

**Propiedades 7** Vamos a pensar ahora en una propiedad que normalmente hemos usado en los anillos "de números" ($\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ o $\mathbb{C}$): si $a \cdot b = 0$, entonces $a = 0$ o $b = 0$. Curiosamente esta propiedad no es cierta en todo anillo: Veamos varios contraejemplos:

(1) Si consideramos las matrices de tamaño $n$ (con $n \in \mathbb{N}$, $n \geq 2$) tenemos que $(\mathcal{M}_n(\mathbb{R}), +, \cdot)$, las matrices con su suma y producto usual tienen estructura de anillo (anillo unitario, no conmutativo si $n > 1$). Y ya sabemos que podemos tener dos matrices no nulas de producto cero:

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 5 & 2 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

(2) Podemos considerar algunos anillos de congruencias modulo $n$, que son conmutativos y unitarios, $(\mathbb{Z}_n, +, \cdot)$: Por ejemplo, en $\mathbb{Z}_{12}$,

$$\bar{6} \cdot \bar{4} = \bar{0} \text{ pero } \bar{6} \neq \bar{0} \text{ y } \bar{4} \neq \bar{0}$$

**Definición 8** Sea $R$ un anillo. Se dice que un elemento no nulo $a \in R$ es:

- Un **divisor de cero por la izquierda** si existe $0 \neq b \in R$ tal que $a \cdot b = 0$.
- Un **divisor de cero por la derecha** si existe $0 \neq b \in R$ tal que $b \cdot a = 0$.

Un anillo conmutativo y unitario sin divisores de cero por la izquierda y por la derecha se denomina un **dominio de integridad** (normalmente denotaremos los dominios de integridad por D.I.)

**Corolario 9 (ejercicio)** Sea $(R, +, \cdot)$ un anillo y sea $a$ un elemento inversible de $R$. Entonces $a$ no es divisor de cero (ni por la izquierda ni por la derecha) en $R$.

**Corolario 10 (ejercicio)** Todo cuerpo es un dominio de integridad. $\mathbb{Z}$ es un D.I. que no es cuerpo.

**Definición 11** Se dice que un anillo $R$ verifica la **ley de cancelación por la izquierda** si para todo elemento no nulo $a \in R$ y para todos $x, y \in R$ se verifica que

$$ax = ay \quad \Longrightarrow \quad x = y.$$

Se dice que un anillo $R$ verifica la **ley de cancelación por la derecha** si para todo elemento no nulo $a \in R$ y para todos $x, y \in R$ se verifica que

$$xa = ya \quad \Longrightarrow \quad x = y.$$

**Proposición 12 (ejercicio)** Sea $(R, +, \cdot)$ un anillo. Las siguientes condiciones son equivalentes:

(i) $R$ no posee divisores de cero por la izquierda (Resp. derecha).

(ii) Se verifican las leyes de cancelación por la izquierda (Resp. derecha).

**Corolario 13 (ejercicio)** Para un anillo conmutativo y unitario $(R, +, \cdot)$ las siguientes condiciones son equivalentes:

(i) $R$ es un dominio de integridad.

(ii) Se verifican las leyes de cancelación en $R$. Es decir,

$$\text{Si } ax = ay \text{ con } a \neq 0, \text{ entonces } x = y$$

**Nota:** Sólo hemos escrito una de las leyes de cancelación ya que el anillo es conmutativo, con lo que la otra es inmediata.

★ Los ejercicios del 1 al 15 te pueden servir para saber si has asimilado los conceptos de esta sección.

## 2.2. Subanillos

**Definición 14** *Sea $(R, +, \cdot)$ un anillo. Se dice que $A \subset R$ es un subanillo de $R$, y se representa $A \leq R$, si:*

- *La suma de $R$ es una operación interna en $A$: $a + b \in A$ para todos $a, b \in A$.*
- *El producto de $R$ es una operación interna en $A$: $a \cdot b \in A$ para todos $a, b \in A$.*
- *$(A, +, \cdot)$ tiene estructura de anillo.*

**Nota:** Observar que los dos primeros puntos significan que la suma y el producto de $R$ definen operaciones en $A$.

**Nota:** Por tanto, para demostrar que un subconjunto $A$ de un anillo $R$ es un subanillo tenemos que demostrar 9 propiedades. No obstante algunas son triviales:

**Teorema 15** Sea $(R, +, \cdot)$ un anillo y sea $A \subset R$. Entonces $A$ es un subanillo de $R$ si y sólo si:

(i) La suma de $R$ es una operación interna en $A$: $a + b \in A$ para todos $a, b \in A$.
(ii) $0 \in A$ y para todo $a \in A$, $-a \in A$.
(iii) El producto de $R$ es una operación interna en $A$: $a \cdot b \in A$ para todos $a, b \in A$

✔ **Demo:** Supongamos en primer lugar que $A$ es un subconjunto de $R$ que verifica las propiedades (i), (ii) y (iii). Entonces,
★ $(A, +)$ es un grupo abeliano:
• (i) nos dice que la suma define una operación en $A$.
• Como se verifica (ii), $0 \in A$ y por tanto 0 es el elemento neutro de $A$ (si para todo elemento $x$ de $R$ se tiene que $x + 0 = 0 + x = x$, para todo elemento $a$ de $A$, que en particular es un elemento de $R$, se tiene que $a + 0 = 0 + a = a$).
• Si $a \in A$, por (ii), $-a \in A$ por tanto $a$ tiene opuesto en $A$, el elemento $-a$.
• por ultimo, como $x + y = y + x$ para todo elemento $x, y \in R$ se tiene que esta misma propiedad se verifica para los elementos de $A$.
★ $(A, \cdot)$ verifica la propiedad asociativa:
• (iii) nos dice que el producto define una operación en $A$.
• Como $(xy)z = x(yz)$ para todo elemento $x, y, z \in R$ se tiene que esta misma propiedad se verifica para los elementos de $A$.
★ $(A, \cdot)$ verifica la propiedad distributiva:
• Como $(x + y)z = xz + yz$ y $z(x + y) = zx + zy$ para todo elemento $x, y, z \in R$ se tiene que estas mismas propiedades se verifican para los elementos de $A$.

Por tanto, si se verifica (i), (ii) y (iii) $(A, +, \cdot)$ tiene estructura de anillo, lo que implica que es subanillo de $R$. Veamos el recíproco.

Supongamos ahora que la suma y el producto de $R$ dotan a $A$ de estructura de anillo. En primer lugar, la suma es una operación en $A$, por lo que para todo $a, b \in A$ $a + b \in A$. De forma similar, el producto es una operación en $A$ por lo que para todo $a, b \in A$ $a \cdot b \in A$. Es decir, se satisfacen (i) y (iii) del enunciado.

Veamos que también se satisface (ii). En primer lugar demostremos que $0 \in A$: Por hipótesis $(A, +)$ tiene estructura de grupo abeliano, por lo que posee un elemento neutro. Denotémoslo por $0' \in A$ (en principio nadie nos dice que tenga que ser el elemento neutro

de la suma de $R$, que denotamos por 0). Ahora, $0' = 0' + 0'$ ya que $0'$ es el neutro de $(A, +)$ pero $0' + 0 = 0'$ ya que 0 es el neutro de $R$. Por tanto,

$$0' + 0 = 0' + 0'.$$

Si sumamos en esta expresión por el opuesto de $0'$ en $R$ tenemos $0 = -0' + 0' + 0 = -0' + 0' + 0' = 0' \in A$.

Demostremos ahora que para cada $a \in A$, $-a \in A$: dado $a \in A$, como $(A, +)$ es un grupo abeliano, $a$ tiene su opuesto en $A$, denotémoslo por $a'$, así,

$$a + a' = a' + a = 0 \qquad \clubsuit$$

(ya que hemos visto que el neutro de $(A, +)$ era el 0). Pero $\clubsuit$ nos dice que $a'$ es el opuesto de $a$ en $R$, es decir, que $a' = -a$. ■

**Ejemplos D** $2\mathbb{Z} \leq \mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$.

**Lema 16 (ejercicio)** Un subanillo de un anillo unitario no tiene que ser unitario. Es más, aunque sea unitario la unidad del anillo y del subanillo no tiene que coincidir.

**Nota:** Aunque la unidad de $R$, si existe, (el elemento neutro del producto de $R$) no tiene que pertenecer al subanillo, el neutro de la suma si pertenece a cualquier subanillo, por lo que $R$ y cualquier subanillo suyo tienen el mismo neutro para la suma.

**Lema 17 (ejercicio)** Todo subanillo unitario de un dominio de integridad es un dominio de integridad. En particular, todo subanillo unitario de un cuerpo es un dominio de integridad.

★ Los ejercicios del 16 al 19 te pueden servir para saber si has asimilado los conceptos de esta sección.

# 3. Homomorfismos de anillos

**Definición 1** Sean $(R, +, .)$ y $(R', +', .')$ dos anillos. Se define un **homomorfismo** de $R$ en $R'$ como una aplicación $f : R \to R'$ tal que:

$$f(a + b) = f(a) +' f(b) \quad \text{para todo } a, b \in R,$$
$$f(a \cdot b) = f(a) \cdot' f(b) \quad \text{para todo } a, b \in R.$$

- Si $f$ es inyectiva, se dice que $f$ es un **monomorfismo**.
- Si $f$ es sobreyectiva, se dice que $f$ es un **epimorfismo**.
- Si $f$ es biyectiva, se dice que $f$ es un **isomorfismo**. En este caso se dice que los anillos $R$ y $R'$ son **isomorfos**.
- Si $R = R'$, se dice que $f$ es un **endomorfismo**.
- Un endomorfismo biyectivo se le denomina un **automorfismo**.
- Si $R$ y $R'$ son dos anillos unitarios, diremos que $f : R \to R'$ es un **homomorfismos de anillos unitarios** si $f(1_R) = 1_{R'}$.

**Proposición 2** Sean $R$ y $R'$ dos anillos y sea $a$ un elemento invertible de $R$ (con inverso $a^{-1}$). Entonces:

- La aplicación nula, $f : R \to R'$ definida por $f(x) = 0'$ para todo $x \in R$ es un homomorfismo de anillos.
- La aplicación identidad, $\mathrm{Id} : R \to R$ definida por $\mathrm{Id}(x) = x$ para todo $x \in R$ es un automorfismo de anillos.
- La aplicación $f_a : R \to R$ definido por $f_a(x) = a^{-1}xa$ es un automorfismo de $R$. Llamado el **automorfismo interno** asociado al elemento inversible $a$.

✔**Demo:** (1). Veamos que la aplicación $f : R \to R'$ definida por $f(x) = 0'$ para todo $x \in R$ es un homomorfismo de anillos:

$$f(x+y) = 0 = 0+0 = f(x)+f(y) \quad \text{y} \quad f(xy) = 0 = 0 \cdot 0 = f(x) \cdot f(y)$$

(2). Veamos que la aplicación identidad es un homomorfismo de anillos:

$$\mathrm{Id}(x+y) = x+y = \mathrm{Id}(x)+\mathrm{Id}(y) \quad \text{y} \quad \mathrm{Id}(x \cdot y) = x \cdot y = \mathrm{Id}(x) \cdot \mathrm{Id}(y)$$

(3). Por último demostremos que $f_a$ verifica las propiedades que tienen que verificar los automorfismos de anillos:

$$\begin{aligned} f_a(x+y) &= a^{-1}(x+y)a = a^{-1}xa + a^{-1}ya = f_a(x) + f_a(y) \\ f_a(x \cdot y) &= a^{-1}xya = a^{-1}x(aa^{-1})ya = a^{-1}xaa^{-1}ya = f_a(x) \cdot f_a(y) \end{aligned}$$

Es más la aplicación inversa de $f_a$ es $f_{a^{-1}}$ en donde $f_{a^{-1}}(x) = (a^{-1})^{-1}xa^{-1} = axa^{-1}$ ya que

$$\begin{aligned} f_a \circ f_{a^{-1}}(x) &= f_a(axa^{-1}) = a^{-1}(axa^{-1})a = x \\ f_{a^{-1}} \circ f_a(x) &= f_{a^{-1}}(a^{-1}xa) = a(a^{-1}xa)a^{-1} = x \end{aligned}$$

Lo que demuestra el ejemplo. ■

**Lema 3** Sean $R$ y $R'$ son dos anillos y $f : R \to R'$ un homomorfismo de anillos. Entonces:

(i) $f(0) = 0$.
(ii) $f(-a) = -f(a)$

✔**Demo:** (i). Ya hemos hecho alguna demostración con la misma idea.

$$f(0) = f(0+0) = f(0) + f(0)$$

Si ahora sumamos en ambos lados el opuesto de $f(0)$ en $R'$ tenemos,

$$0' = f(0) - f(0) = f(0) + f(0) - f(0) = f(0)$$

(ii). Sea $a \in R$. Entonces

$$f(a) + f(-a) = f(a+(-a)) = f(0) = 0 \quad \text{y} \quad f(-a) + f(a) = f((-a)+a) = f(0) = 0$$

Por tanto el opuesto de $f(a)$ en $R'$ es $f(-a)$. ■

**Lema 4 (Ejercicio)** No tiene que suceder que si $R$ y $R'$ son anillos unitarios, $f(1) = 1'$.

**Proposición 5** Sean $R$ y $R'$ dos anillos, $S$ un subanillo de $R$, $S'$ un subanillo de $R'$ y $f : R \to R'$ un homomorfismo de anillos. Entonces

(i) $f(S)$ es un subanillo de $R'$.
(ii) $f^{-1}(S') := \{r \in R |\ f(r) \in S'\}$ es un subanillo de $R$.

**Demo:** (i). ★ Tenemos que ver que la suma es una operación interna en $f(S)$:
Sean $x, y \in f(S)$. Entonces existen $a, b \in S$ tales que $x = f(a)$ e $y = f(b)$. Por tanto

$$x + y = f(a) + f(b) = f(a + b) \in f(S),$$

ya que como $S$ es un subanillo de $R$, $a + b \in S$.

★ Tenemos que ver que el producto es una operación interna en $f(S)$:
Sean $x, y \in f(S)$. Entonces existen $a, b \in S$ tales que $x = f(a)$ e $y = f(b)$. Por tanto

$$x \cdot y = f(a) \cdot f(b) = f(a \cdot b) \in f(S),$$

ya que como $S$ es un subanillo de $R$, $a \cdot b \in S$.

★ Por último, como $0 \in S$ (ya que $S$ es un subanillo de $R$) $0' = f(0) \in f(S)$ y dado $x \in f(S)$ existe $a \in S$ tal que $x = f(a)$, por tanto $-x = -f(a) = f(-a) \in f(S)$, ya que $-a \in S$.

(ii). ★ Tenemos que ver que la suma es una operación interna en $f^{-1}(S')$:
Sean $a, b \in f^{-1}(S')$ (por definición $f(a), f(b) \in S'$). Entonces $f(a + b) = f(a) + f(b) \in S'$ ya que $S'$ es un subanillo de $R'$.

★ Tenemos que ver que el producto es una operación interna en $f^{-1}(S')$:
Sean $a, b \in f^{-1}(S')$ (por definición $f(a), f(b) \in S'$). Entonces $f(a \cdot b) = f(a) \cdot f(b) \in S'$ ya que $S'$ es un subanillo de $R'$.

★ Por último, $f(0) = 0' \in S'$ (ya que $S'$ es subanillo de $R'$) y por tanto $0 \in f^{-1}(S')$. Por último, si $a \in f^{-1}(S')$ (es decir, $f(a) \in S'$), $f(-a) = -f(a) \in S'$ y por tanto $-a \in f^{-1}(S')$. ■

**Corolario 6** Sean $R$ y $R'$ dos anillos, $S$ un subanillo de $R$, $S'$ un subanillo de $R'$ y $f : R \to R'$ un homomorfismo de anillos. Entonces:

(i) $\mathrm{Ker}(f) := f^{-1}(0)$, llamado el **núcleo o Ker** de $f$, es un subanillo de $R$.

(ii) $\mathrm{Im}(f) := f(R)$, llamada la **imagen** de $f$, es un subanillo de $R'$.

**Nota:** Cuando lleguemos a la estructura cociente en anillo veremos que $\mathrm{Ker}(f)$ tiene propiedades mucho más interesantes que la de ser simplemente un subanillo.

**Proposición 7** Sean $R$ y $R'$ dos anillos, $S$ un subanillo de $R$, $S'$ un subanillo de $R'$ y $f : R \to R'$ un homomorfismo de anillos. Entonces

(i) $f$ es un monomorfismo si y sólo si $\mathrm{Ker}(f) = 0$.
(ii) $f$ es un epimorfismo si y sólo si $\mathrm{Im}(f) = R'$.

✔**Demo:** (i). Recordamos que $\mathrm{Ker}(f) = \{a \in R \mid f(a) = 0'\}$. Por tanto, si $f$ es inyectiva sólo el cero puede ir al cero y por tanto $\mathrm{Ker}(f) = \{0\}$. Recíprocamente, supongamos que $\mathrm{Ker}(f) = \{0\}$ y sean $a, b \in R$ tales que $f(a) = f(b)$. Entonces

$$0' = f(a) + (-f(b)) = f(a - b)$$

por lo que $a - b \in \mathrm{Ker}(f) = \{0\}$ y por tanto $a - b = 0$, es decir, $a = b$.

(ii). es una consecuencia de ser $f$ aplicación (no intervienen las nociones de anillo para demostrar esto). ■

**Proposición 8** *Sean $(R, +, .)$ y $(R', +', .')$ dos anillos y $f : R \to R'$ un isomorfismo de anillos. Entonces $f^{-1} : R' \to R$ también es un isomorfismo de anillos.*

Cada estructura que demos en algebra tendrá su homomorfismo asociado. Por ejemplo, la noción de subanillo está ligada con la noción de monomorfismo:

**Proposición 9** Sea $R$ un subanillo de $R'$. Entonces la inclusión de $R$ en $R'$, $i : R \hookrightarrow R'$ definida por $i(r) = r$ es un monomorfismo de anillos. Es más: si $f : R \to R'$ es un monomorfismo de anillos, entonces $R$ es isomorfo a $\mathrm{Im}(f) \leq R'$ (por lo que se puede considerar que $R$ es un subanillo de $R'$).

En la proxima sección vemos más homomorfismos asociados a distintas construcciones de anillos.

★ Los ejercicios del 20 al 28 te pueden servir para saber si has asimilado los conceptos de esta sección.

# 4. Construcción de nuevos anillos

## 4.1. El producto directo de anillos.

**Proposición 1** Sea $I$ un conjunto de indices y $R_i$, $i \in I$ una familia de anillos. Entonces $\Pi_{i \in I} R_i$ Tiene estructura de anillo con la suma y el producto definidos por componentes:

$$\Pi_{i \in I} R_i := \{(r_i)_{i \in I} \quad \text{con} \quad r_i \in R_i, \quad i \in I\}$$

⋆ Con suma: $(r_i)_{i \in I} + (r'_i)_{i \in I} = (r_i + r'_i)_{i \in I}$
⋆ y producto, $(r_i)_{i \in I} \cdot (r'_i)_{i \in I} = (r_i \cdot r'_i)_{i \in I}$

**Ejemplos A** *Veamos un ejemplo antes de demostrar la proposición. Sean los anillos $\mathbb{Z}_2$ y $\mathbb{Z}_3$. Entonces la proposición anterior nos dice que*

$$\mathbb{Z}_2 \times \mathbb{Z}_3 = \{(\overline{a}, \overline{b}) \mid \overline{a} \in \mathbb{Z}_2 \ y \ \overline{b} \in \mathbb{Z}_3\} = \{(\overline{0}, \overline{0}), (\overline{0}, \overline{1}), (\overline{0}, \overline{2}), (\overline{1}, \overline{0}), (\overline{1}, \overline{1}), (\overline{1}, \overline{2})\}$$

*Con suma y producto por componentes, por ejemplo,*

$$(\overline{0}, \overline{2}) + (\overline{1}, \overline{0}) = (\overline{0} + \overline{1}, \overline{2} + \overline{0}) = (\overline{1}, \overline{2})$$
$$(\overline{0}, \overline{2}) \cdot (\overline{1}, \overline{0}) = (\overline{0} \cdot \overline{1}, \overline{2} \cdot \overline{0}) = (\overline{0}, \overline{0})$$

**Demo:** (Proposición 1 (Pag. 61)) Es claro que la suma y el producto en $\Pi_{i\in I}R_i$ están bien definidos ya que si $(r_i)_{i\in I}, (r'_i)_{i\in I} \in \Pi_{i\in I}R_i$, para cada $i \in I$, $r_i$ e $r'_i \in R_i$ y por tanto $r_i + r'_i \in R_i$ y $r_i \cdot r'_i \in R_i$, por lo que $(r_i + r'_i)_{i\in I}, (r_i \cdot r'_i)_{i\in I} \in \Pi_{i\in I}R_i$. Veamos ahora que se verifica que $(\Pi_{i\in I}R_i, +, \cdot)$ tiene estructura de anillo:
★ $(\Pi_{i\in I}R_i, +)$ tiene estructura de grupo abeliano:
⋆ Asociativa: sean $(x_i)_{i\in I}, (y_i)_{i\in I}$ y $(z_i)_{i\in I} \in \Pi_{i\in I}R_i$. Entonces,

$$\begin{aligned}[(x_i)_{i\in I} + (y_i)_{i\in I}] + (z_i)_{i\in I} &= (x_i + y_i)_{i\in I} + (z_i)_{i\in I} = ([x_i + y_i] + z_i)_{i\in I} \\ &= (x_i + [y_i + z_i])_{i\in I} = (x_i)_{i\in I} + (y_i + z_i)_{i\in I} \\ &= (x_i)_{i\in I} + [(y_i)_{i\in I} + (z_i)_{i\in I}].\end{aligned}$$

⋆ Conmutativa: sean $(x_i)_{i\in I}$ e $(y_i)_{i\in I} \in \Pi_{i\in I}R_i$. Entonces,

$$(x_i)_{i\in I} + (y_i)_{i\in I} = (x_i + y_i)_{i\in I} = (y_i + x_i)_{i\in I} = (y_i)_{i\in I} + (x_i)_{i\in I}$$

⋆ Neutro: sea $(x_i)_{i\in I} \in \Pi_{i\in I}R_i$ y consideremos $0_i \in R_i$ el neutro del anillo $R_i$. Entonces,

$$\begin{aligned}(x_i)_{i\in I} + (0_i)_{i\in I} &= (x_i + 0_i)_{i\in I} = (x_i)_{i\in I} \\ (0_i)_{i\in I} + (x_i)_{i\in I} &= (0_i + x_i)_{i\in I} = (x_i)_{i\in I}\end{aligned}$$

Por tanto el neutro para la suma en $\Pi_{i\in I}R_i$ es $(0_i)_{i\in I}$.

⋆ Opuesto: sea $(x_i)_{i\in I} \in \Pi_{i\in I}R_i$. Para cada $k \in I$ sea $x_k$ (el elemento de $R_k$ que está en la coordenada $k$). Sea $-x_k$ su opuesto en $R_k$ y consideremos $(-x_i)_{i\in I} \in \Pi_{i\in I}R_i$. Entonces,

$$\begin{aligned}(x_i)_{i\in I} + (-x_i)_{i\in I} &= (x_i - x_i)_{i\in I} = (0_i)_{i\in I} \\ (-x_i)_{i\in I} + (x_i)_{i\in I} &= (-x_i + x_i)_{i\in I} = (0_i)_{i\in I}\end{aligned}$$

Por tanto el opuesto de $(x_i)_{i\in I}$ en $\Pi_{i\in I}R_i$ es $(-x_i)_{i\in I} \in \Pi_{i\in I}R_i$.
★ $(\Pi_{i\in I}R_i, \cdot)$ es asociativa: sean $(x_i)_{i\in I}, (y_i)_{i\in I}$ y $(z_i)_{i\in I} \in \Pi_{i\in I}R_i$. Entonces,

$$\begin{aligned}[(x_i)_{i\in I} \cdot (y_i)_{i\in I}] \cdot (z_i)_{i\in I} &= (x_i \cdot y_i)_{i\in I} \cdot (z_i)_{i\in I} = ([x_i \cdot y_i] \cdot z_i)_{i\in I} \\ &= (x_i \cdot [y_i \cdot z_i])_{i\in I} = (x_i)_{i\in I} \cdot (y_i \cdot z_i)_{i\in I} \\ &= (x_i)_{i\in I} \cdot [(y_i)_{i\in I} \cdot (z_i)_{i\in I}].\end{aligned}$$

★ $(\Pi_{i\in I}R_i, +, \cdot)$ verifica la distributiva: sean $(x_i)_{i\in I}, (y_i)_{i\in I}$ y $(z_i)_{i\in I} \in \Pi_{i\in I}R_i$. Entonces,

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

Por tanto $(\Pi_{i\in I}R_i, +, \cdot)$ tiene estructura de anillo. ■

El producto directo de anillos está ligado a la noción de proyección canónica y a cierta propiedad estructural:

**Definición 2** *Sean $R_i$, $i \in I$ una familia de anillos y sea $R = \Pi_{i\in I} R_i$ el producto directo de los $R_i$. Se define la* ***proyección "canónica"*** *de $R$ en $R_k$, con $k \in I$, como:*

$$\begin{array}{rccc} \pi_k : & R & \longrightarrow & R_k \\ & (r_i)_{i\in I} & \longmapsto & r_k. \end{array}$$

**Proposición 3 (ejercicio)** *Sea $\{R_i\}_{i\in I}$ una familia de anillos y sea $R = \Pi_{i\in I} R_i$ el producto directo de los $R_i$. Entonces, para cada $k \in I$, la proyección canónica $\pi_k : \Pi_{i\in I} R_i \to R_k$ es un epimorfismo de anillos.*

**Proposición 4 (ejercicio)** *Sea $\{R_i\}_{i\in I}$ una familia de anillos y sea $R = \Pi_{i\in I} R_i$ el producto directo de los $R_i$. Entonces,*

- *$R$ es unitario si y sólo si $R_k$ es unitario para todo $k \in I$.*
- *$R$ es conmutativo si y sólo si $R_k$ es conmutativo para todo $k \in I$.*
- *Si $\#I \geq 2$, $R$ tiene divisores de cero. Por tanto, en este caso, $R$ no puede ser dominio de integridad, ni anillo de división ni cuerpo.*

## 4.2. La suma directa de anillos.

**Proposición 5** *Sea $I$ un conjunto de indices y $\{R_i\}_{i\in I}$ una familia de anillos. Entonces*

$$\bigoplus_{i\in I} R_i = \{(r_i)_{i\in I} \in \Pi_{i\in I} R_i \mid r_i = 0 \quad \textit{para casi todo } i\}$$

*es un subanillo de $\Pi_{i\in I} R_i$, llamado la* ***suma directa externa*** *de los $R_i$*
***Nota:*** *Al ser un subanillo la suma y el producto se definen por componentes:*
⋆ *Suma por componentes: $(r_i)_{i\in I} + (r'_i)_{i\in I} = (r_i + r'_i)_{i\in I}$*
⋆ *Producto por componentes: $(r_i)_{i\in I} \cdot (r'_i)_{i\in I} = (r_i \cdot r'_i)_{i\in I}$*

**Demo:** Es claro que si sumo o multiplico dos elementos del producto con un número finito de coordenadas no nulas, obtengo un elemento con un número finito de coordenadas no nulas, ver la proposición 1 (Pag. 61) para la definición de producto directo de anillos. Es más,
⋆ $(0_i) \in \bigoplus_{i\in I} R_i$ (el elemento neutro de la suma de $\Pi_{i\in I} R_i$) y
⋆ si $(r_i)_{i\in I} \in \bigoplus_{i\in I} R_i$, su opuesto (respecto de la suma en $\Pi_{i\in I} R_i$) es $(-r_i)_{i\in I}$ que pertenece a $\bigoplus_{i\in I} R_i$.
Por tanto, por el teorema 15 (Pag. 57), $\bigoplus_{i\in I} R_i \leq \Pi_{i\in I} R_i$. ■

**Nota:** Si $\#I < \infty$ se tiene que la suma directa y el producto directo coinciden.

**Definición 6** *Sean $\{R_i\}_{i\in I}$ una familia de anillos y sea $\bigoplus_{i\in I} R_i$ la suma directa de éstos. Entonces para cada $k \in I$ se define la* ***inclusión canónica*** *de $R_k$ en $\bigoplus_{i\in I} R_i$ y se representa por*

$$\rho_k : R_k \to \bigoplus_{i\in I} R_i$$

*como $\rho_k(r_k) = (x_i)_{i\in I}$ en donde $x_i = 0$ si $i \neq k$ y $x_k = r_k$. Es decir, la upla de $\Pi_{i\in I} R_i$ que tiene todas las coordenadas cero, salvo la $k$ que vale $r_k$.*

**Proposición 7 (ejercicio)** *Sea $\{R_i\}_{i\in I}$ una familia de anillos y sea $R = \bigoplus_{i\in I} R_i$ la suma directa de los $R_i$. Entonces, para cada $k \in I$, la inclusión canónica $\rho_k : R_k \to \bigoplus_{i\in I} R_i$ es un monomorfismo de anillos.*

## 4.3. El anillo de matrices

**Proposición 8** *Sea $R$ un anillo y $n \in \mathbb{N}$. Entonces El conjunto $\mathcal{M}_n(R)$ definido como:*

$$\mathcal{M}_n(R) := \left\{ \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} \quad \text{con } a_{ij} \in R \text{ para } i,j = 1,2,\ldots,n \right\}$$

*con su suma definida por componentes y producto habitual de matrices tiene estructura de anillo. Es decir, dadas*

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} \qquad B = \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1} & b_{n2} & \cdots & b_{nn} \end{pmatrix}$$

***Nota:*** *En notación reducida, $A = (a_{ij})$ y $B = (b_{ij})$.*

- $A + B = (a_{ij} + b_{ij}) = \begin{pmatrix} a_{11}+b_{11} & a_{12}+b_{12} & \cdots & a_{1n}+b_{1n} \\ a_{21}+b_{21} & a_{22}+b_{22} & \cdots & a_{2n}+b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1}+b_{n1} & a_{n2}+b_{n2} & \cdots & a_{nn}+b_{nn} \end{pmatrix}$
- $A \cdot B = (\sum_{k=1}^{n} a_{ik} \cdot b_{kj}) = \begin{pmatrix} \sum_{k=1}^{n} a_{1k} \cdot b_{k1} & \sum_{k=1}^{n} a_{1k} \cdot b_{k2} & \cdots & \sum_{k=1}^{n} a_{1k} \cdot b_{kn} \\ \sum_{k=1}^{n} a_{2k} \cdot b_{k1} & \sum_{k=1}^{n} a_{2k} \cdot b_{k2} & \cdots & \sum_{k=1}^{n} a_{2k} \cdot b_{kn} \\ \vdots & \vdots & \ddots & \vdots \\ \sum_{k=1}^{n} a_{nk} \cdot b_{k1} & \sum_{k=1}^{n} a_{nk} \cdot b_{k2} & \cdots & \sum_{k=1}^{n} a_{nk} \cdot b_{kn} \end{pmatrix}$

**Demo:** ★ Es claro que la suma es una operación bien definida en $\mathcal{M}_n(R)$. Es más, la suma se define componente a componente, por lo que (siguiendo la demostración del producto cartesiano de anillos), $(\mathcal{M}_n(R), +)$ es un grupo abeliano. Observar que el elemento neutro para la suma es

$$0 = \begin{pmatrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}$$

y el opuesto para un elemento $A = (a_{ij}) \in \mathcal{M}_n(R)$ es $-A = (-a_{ij})$.

★ Es claro que el producto es una operación bien definida en $\mathcal{M}_n(R)$. Algo más complicado será demostrar la propiedad asociativa. Usemos la notación reducida:

$$(A \cdot B) \cdot C = (\sum_{r=1}^{n} a_{ir} \cdot b_{rj}) \cdot (c_{ij}) = (\sum_{r,s=1}^{n} (a_{ir} \cdot b_{rs}) \cdot c_{sj})$$

$$A \cdot (B \cdot C) = (a_{ij}) \cdot (\sum_{s=1}^{n} b_{is} \cdot c_{sj}) = (\sum_{r,s=1}^{n} a_{ir} \cdot (b_{rs} \cdot c_{sj}))$$

**Nota:** Una demostración con notación matricial la puedes encontrar al final del tema.

★ Demostremos las propiedades distributivas. Usemos la notación reducida:

$$\begin{aligned}(A+B)\cdot C &= (a_{ij}+b_{ij})\cdot(c_{ij}) = (\sum_{r=1}^{n}(a_{ir}+b_{ir})\cdot c_{rj}) = (\sum_{r=1}^{n} a_{ir}\cdot c_{rj}) + (\sum_{r=1}^{n} b_{ir}\cdot c_{rj}) \\ &= A\cdot C + B\cdot C \\ A\cdot(B+C) &= (a_{ij})\cdot(b_{ij}+c_{ij}) = (\sum_{r=1}^{n} a_{ir}\cdot(b_{rj}+c_{rj})) = (\sum_{r=1}^{n} a_{ir}\cdot b_{rj}) + (\sum_{r=1}^{n} a_{ir}\cdot c_{rj}) \\ &= A\cdot B + A\cdot C\end{aligned}$$

**Proposición 9 (ejercicio)** *Sea $R$ un anillo y $n\in\mathbb{N}$. Entonces*

*(i)* $\mathcal{M}_n(R)$ *es unitario si y sólo si $R$ es unitario.*

*(i)* $\mathcal{M}_n(R)$ *tiene divisores de cero si $n\leq 2$. Por tanto, en este caso, $\mathcal{M}_n(R)$ no puede ser ni dominio de integridad, ni anillo de división ni cuerpo.*

*(ii)* $\mathcal{M}_n(R)$ *es conmutativo si y sólo si $R$ es conmutativo y $n=1$.*

*(iii)* $\mathcal{M}_n(R)$ *es un anillo de división si y sólo si $R$ es un anillo de división y $n=1$.*

*(iv)* $\mathcal{M}_n(R)$ *es un cuerpo si y sólo si $R$ es un cuerpo y $n=1$.*

★ Los ejercicios del 29 al 33 te pueden servir para saber si has asimilado los conceptos de esta sección.

## 4.4. El anillo de polinomios y el anillo de series formales

### El anillo de series formales

**Proposición 10** Sea $R$ un anillo. Se define el anillo de series formales sobre $R$ y se representa por $R[[X]]$ como el conjunto:

$$R[[X]] := \{\sum_{n=0}^{\infty} a_n X^n | \quad \text{con } a_n\in R\}$$

con suma y producto dado por:

(i) Suma por componentes: $\sum_{n=0}^{\infty} a_n X^n + \sum_{n=0}^{\infty} b_n X^n = \sum_{n=0}^{\infty}(a_n+b_n)X^n$.

(ii) Producto: $\sum_{n=0}^{\infty} a_n X^n \cdot \sum_{n=0}^{\infty} b_n X^n = \sum_{n=0}^{\infty}\left(\sum_{k=0}^{n} a_k\cdot b_{n-k}\right)X^n$.

**Demo:** La suma en $R[[X]]$ coincide con la suma por componentes, por lo que la demostración de que $(R[[X]],+)$ es un grupo abeliano es la misma a la dada para demostrar que la suma en el producto cartesiano de anillos dota a éste de estructura un grupo abeliano.

★ Veamos que el producto es asociativo. Primero dos identidades:

$$(\star_1)\ \sum_{k=0}^{n}\sum_{s=0}^{n-k} a_{ks} = \sum_{k=0}^{n}\sum_{s=0}^{n-k} a_{sk}. \qquad (\star_2)\ \sum_{r=0}^{n} a_r = \sum_{r=0}^{n} a_{n-r}.$$

En $(\star_1)$ simplemente estamos reordenando los sumandos. En ambos sumatorios se suman los elementos

$$\begin{array}{ccccc} a_{00} & a_{01} & \dots & a_{0\,n-1} & a_{0n} \\ a_{10} & a_{11} & \dots & a_{1\,n-1} & \\ \vdots & \vdots & \iddots & & \\ a_{n-1\,0} & a_{n-1\,1} & & & \\ a_{n0} & & & & \end{array}$$

En el primer termino de $(\star_1)$ los estamos sumando por filas mientras que en el segundo término de $(\star_1)$ los estamos sumando por columnas. En $(\star_2)$ sumamos los elementos $a_1 + a_2 + \cdots + a_n$ en el primer término de la identidad y sumamos $a_n + \cdots + a_2 + a_1$ en el segundo.

$$\begin{aligned} &\star\left(\sum_{n=0}^{\infty} a_n X^n \cdot \sum_{n=0}^{\infty} b_n X^n\right) \cdot \sum_{n=0}^{\infty} c_n X^n = \sum_{n=0}^{\infty}\left(\sum_{s=0}^{n} a_s \cdot b_{n-s}\right) X^n \cdot \sum_{n=0}^{\infty} c_n X^n \\ &= \sum_{n=0}^{\infty}\left(\sum_{k=0}^{n}\left(\sum_{s=0}^{k} a_s \cdot b_{k-s}\right) \cdot c_{n-k}\right) X^n = \sum_{n=0}^{\infty}\left(\sum_{k=0}^{n}\sum_{s=0}^{k} a_s \cdot b_{k-s} \cdot c_{n-k}\right) X^n \end{aligned}$$

$$\begin{aligned} &\star \sum_{n=0}^{\infty} a_n X^n \cdot \left(\sum_{n=0}^{\infty} b_n X^n \cdot \sum_{n=0}^{\infty} c_n X^n\right) = \sum_{n=0}^{\infty} a_n X^n \cdot \sum_{n=0}^{\infty}\left(\sum_{k=0}^{n} b_k \cdot c_{n-k}\right) X^n \\ &= \sum_{n=0}^{\infty}\sum_{k=0}^{n}\left(a_k \cdot \left(\sum_{s=0}^{n-k} b_s \cdot c_{n-s-k}\right)\right) X^n = \sum_{n=0}^{\infty}\left(\sum_{k=0}^{n}\sum_{s=0}^{n-k} a_k \cdot b_s \cdot c_{n-s-k}\right) X^n \\ &=^{(\star_2^s)} \sum_{n=0}^{\infty}\left(\sum_{k=0}^{n}\sum_{s=0}^{n-k} a_k \cdot b_{n-k-s} \cdot c_s\right) X^n =^{(\star_1)} \sum_{n=0}^{\infty}\left(\sum_{k=0}^{n}\sum_{s=0}^{n-k} a_s \cdot b_{n-k-s} \cdot c_k\right) X^n \\ &=^{(\star_2^*)} \sum_{n=0}^{\infty}\left(\sum_{k=0}^{n}\sum_{s=0}^{k} a_s \cdot b_{k-s} \cdot c_{n-k}\right) X^n \end{aligned}$$

En donde, en $(\star_2^s)$ sumamos $s$ desde $n-k$ a 0 ($s$ hace el papel de $r$ en $(\star_2)$) y en $(\star_2^k)$ sumamos $k$ desde $n$ a 0 ($k$ hace el papel de $r$ en $(\star_2)$).

★ Veamos que el producto es distributivo.

$$\begin{aligned} &\star\left(\sum_{n=0}^{\infty} a_n X^n + \sum_{n=0}^{\infty} b_n X^n\right) \cdot \sum_{n=0}^{\infty} c_n X^n = \sum_{n=0}^{\infty}(a_n + b_n) X^n \cdot \sum_{n=0}^{\infty} c_n X^n = \\ &= \sum_{n=0}^{\infty}\left(\sum_{k=0}^{n}(a_k + b_k) \cdot c_{n-k}\right) X^n = \sum_{n=0}^{\infty}\left(\sum_{k=0}^{n} a_k \cdot c_{n-k} + b_k \cdot c_{n-k}\right) X^n \\ &= \sum_{n=0}^{\infty} a_n X^n \cdot \sum_{n=0}^{\infty} c_n X^n + \sum_{n=0}^{\infty} b_n X^n \cdot \sum_{n=0}^{\infty} c_n X^n \end{aligned}$$

$$\begin{aligned} &\star \sum_{n=0}^{\infty} c_n X^n \cdot \left(\sum_{n=0}^{\infty} a_n X^n + \sum_{n=0}^{\infty} b_n X^n\right) = \sum_{n=0}^{\infty} c_n X^n \cdot \sum_{n=0}^{\infty}(a_n + b_n) X^n = \\ &= \sum_{n=0}^{\infty}\left(\sum_{k=0}^{n} c_k \cdot (a_{n-k} + b_{n-k})\right) X^n = \sum_{n=0}^{\infty}\left(\sum_{k=0}^{n} c_k \cdot a_{n-k} + c_k \cdot b_{n-k}\right) X^n \\ &= \sum_{n=0}^{\infty} c_n X^n \cdot \sum_{n=0}^{\infty} a_n X^n + \sum_{n=0}^{\infty} c_n X^n \cdot \sum_{n=0}^{\infty} b_n X^n \end{aligned}$$

Por lo que $R[[X]]$ tiene estructura de anillo. ■

**Teorema 11** Sea $R$ un anillo. Entonces la aplicación $i : R \to R[[X]]$ definida por $i(a) = a + \sum_{n=1}^{\infty} 0X^n$ es un monomorfismo de anillos. Por tanto podemos considerar $R$ como subanillo del anillo de series formales, $R \approx i(R) \leq R[[X]]$.

**Proposición 12 (ejercicio)** *Sea $R$ un anillo y sea $R[[X]]$ el anillo de series formales con coeficientes en $R$. Entonces:*

*(i) $R$ es unitario si y sólo si $R[[X]]$ es unitario.*
*(ii) $R$ es conmutativo si y sólo si $R[[X]]$ es conmutativo.*
*(ii) $R$ es D.I si y sólo si $R[[X]]$ es D.I.*

En el anillo de series formales suceden algunos hechos curiosos. Por ejemplo, si $R$ es un anillo unitario $1 + X$ es un elemento inversible de $R[[X]]$ con inverso $\sum_{n=0}^{\infty}(-1)^n X^n$. Es más:

**Proposición 13 (ejercicio)** *Sea $R$ un anillo unitario y sea $R[[X]]$ el anillo de series formales con coeficientes en $R$. Entonces un elemento $\sum_{n=0}^{\infty} a_n X^n \in R[[X]]$ es inversible si y sólo si $a_0$ es un elemento inversible de $R$.*

**Corolario 14** *Sea $\mathbb{F}$ es un cuerpo. Entonces*

$$\sum_{n=0}^{\infty} a_n X^n \in \mathbb{F}[[X]] \text{ es inversible si y sólo si } a_0 \neq 0.$$

### El anillo de polinomios

**Proposición 15** Sea $R$ un anillo. Se define el anillo de polinomios con coeficientes en $R$, y se denota por $R[X]$ como el subanillo de $R[[X]]$ consistente en las series con sólo un número finito de coeficientes no nulos, es decir:

$$R[X] := \{\sum_{k=0}^{n} a_k X^k | \quad \text{con } n \in \mathbb{N} \text{ y } a_k \in R,\ k = 1, 2, \ldots, n\}$$

**Demo:** Claramente la suma y el producto son operaciones internas en $R[X]$. Por otro lado $0 \in R[X]$ y el opuesto de un polinomio $p(X)$ es $-p(X)$ que también pertenece a $R[X]$. ■

**Definición 16** Sea $R$ un anillo y sea $R[X]$ el anillo de polinomios con coeficientes en $R$. Se define el grado de un polinomio $p(X) = \sum_{k=0}^{n} a_k X^k$ y se denota por $\deg(p(X))$, como el mayor $k \in \mathbb{N}$ tal que $a_k \neq 0$.

Como corolario del Teorema 11 (Pag. 67) tenemos:

**Corolario 17** $R$ puede verse como subanillo de $R[X]$ consistente en todos los polinomios de grado cero.

**Proposición 18 (ejercicio)** Sea $R$ un anillo y sea $R[X]$ el anillo de polinomios con coeficientes en $R$ y sean $p(X), q(X) \in R[X]$. Entonces

(i) $R$ es conmutativo si y sólo si $R[X]$ es conmutativo.
(ii) $R$ es unitario si y sólo si $R[X]$ es unitario.

(iii) $R$ es dominio de integridad si y sólo si $R[X]$ es dominio de integridad.

(iv) $\deg(p(X)+q(X)) \leq \text{Max}(\deg(p(X)), \deg(q(X)))$.

(v) $\deg(p(X)\cdot q(X)) \leq \deg(p(X)) + \deg(q(X))$.

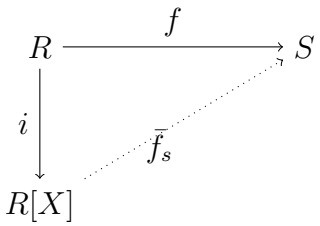
(vi) Es más, $R$ no posee divisores de cero si para todo $p(X), q(X) \in R[X]$ se tiene que

$$\deg(p(X)\cdot q(X)) = \deg(p(X)) + \deg(q(X)).$$

**Nota:** Observar que podemos considerar $R$ como un subanillo de $R[X]$: dado $a \in R$, podemos suponer que $a$ es un polinomio de grado cero en $R[X]$. Más formalmente, la aplicación $i : R \to R[X]$ definida por $i(a) = a$ es un monomorfismo de anillos.

Cuando $R$ es conmutativo nos encontramos con algunas propiedades extra en el anillo de polinomios:

**Proposición 19** Sean $R$ y $S$ dos anillos conmutativos y sea $a \in S$. Entonces para todo homomorfismos de anillos $f : R \longrightarrow S$ existe un único homomorfismo $\bar{f}_s : R[X] \longrightarrow S$ tal que $\bar{f}_s(X) = s$ y hace conmutativo al siguiente diagrama:




**Demo:** Estas demostraciones tienen su estrategia de demostración. Supongamos por un momento que existe este homomorfismo de anillos $\bar{f}_s$ que hace conmutativo el diagrama (y veamos quien tiene que ser). Dado un elemento $a \in R$ tenemos que

$$f(a) = \bar{f}_s \circ i(a) = \bar{f}_s(a + 0X + 0X^2 + \cdots)$$

y por hipótesis $f(X) = s$. Por tanto, dado un polinomio $p(x) = a_0 + a_1x + \cdots + a_nX^n$ tenemos que

$$\begin{aligned}\bar{f}_s(p(x)) &= \bar{f}_s(a_0 + a_1x + \cdots + a_nX^n) = \bar{f}_s(a_0) + \bar{f}_s(a_1x) + \cdots + \bar{f}_s(a_nX^n)\\ &= \bar{f}_s(a_0) + \bar{f}_s(a_1)\bar{f}_s(x) + \cdots + \bar{f}_s(a_n)\bar{f}_s(X)^n = f(a_0) + f(a_1)s + \cdots + f(a_n)s^n\end{aligned}$$

Esta igualdad nos esta diciendo cual es la única posibilidad que tenemos para definir $\bar{f}_s$. Por tanto ya hemos demostrado la unicidad. Demostremos ahora que esta definición de $\bar{f}_s$ verifica lo que dice el teorema: Por construcción $\bar{f}_s$ hace conmutativo el diagrama y $\bar{f}_s(x) = s$ por tanto sólo tenemos que demostrar que es un homomorfismo de anillos.

Sean $p(x) = a_0 + a_1x + \cdots + a_nX^n$ y $q(x) = b_0 + b_1x + \cdots + b_nX^n$ (puedo representarlos "con el mismo grado" completando el de grado menor con ceros) dos polinomios de $R[X]$. Entonces

$$\begin{aligned}
\bar{f}_s(p(x)+q(x)) &= \bar{f}_s(a_0+a_1x+\cdots+a_nX^n+b_0+b_1x+\cdots+b_nX^n)\\
&= \bar{f}_s(a_0+b_0+(a_1+b_1)x+\cdots+(a_n+b_n)X^n)\\
&= f(a_0+b_0)+f(a_1+b_1)s+\cdots+f(a_n+b_n)s^n)\\
&= f(a_0)+f(a_1)s+\cdots+f(a_n)s^n+f(b_0)+f(b_1)s+\cdots+f(b_n)s^n\\
&= \bar{f}_s(p(x))+\bar{f}_s(q(x))\\
\bar{f}_s(p(x)\cdot q(x)) &= \bar{f}_s(a_0+a_1x+\cdots+a_nX^n)\cdot(b_0+b_1x+\cdots+b_nX^n))\\
&= \bar{f}_s(\sum_{i=0}^{2n}\left(\sum_{j=0}^{i}a_j\cdot b_{i-j}\right)X^i) = \sum_{i=0}^{2n}\left(\sum_{j=0}^{i}f(a_j\cdot b_{i-j})\right)s^i\\
&= \sum_{i=0}^{2n}\left(\sum_{j=0}^{i}f(a_j)\cdot f(b_{i-j})\right)s^i\\
&=^{\star} (f(a_0)+f(a_1)s+\cdots+f(a_n)s^n)\cdot(f(b_0)+f(b_1)s+\cdots+f(b_n)s^n)\\
&= \bar{f}_s(p(x))\cdot\bar{f}_s(xq(x))
\end{aligned}$$

Observar que el paso que está marcado con $\star$ es cierto al ser $R$ un anillo conmutativo. Por tanto, $\bar{f}_s$ es un homomorfismo de anillo, lo que demuestra el teorema. ■

**Definición 20** *Sea $R$ un anillo conmutativo y sea $R[X]$ el anillo de polinomios con coeficientes en $R$. Dado $s \in R$ y $p(X) \in R[X]$ se define al evaluación de $p(X)$ en $s$ y se representa por $p(s)$ como $\bar{i}_s(p(X))$.*

**Nota:** Observar que tal como se demostró en la proposición anterior, si consideramos el polinomio $p(X) = a_0 + a_1X + \cdots + a_nX^n \in R[X]$, y el elemento $s \in R$

$$p(s) := \bar{i}_s(p(X)) = a_0 + a_1s + \cdots + a_ns^n$$

★ Los ejercicios del 34 al 37 te pueden servir para saber si has asimilado los conceptos de esta sección.

## 4.5. La unitización de un anillo

En la siguiente proposición vamos a demostrar que todo anillo se puede ver como subanillo de un anillo unitario:

Sea $R$ un anillo y sea $\mathbb{Z}$ el anillo de los enteros. Entonces podemos definir una aplicación $\Phi : \mathbb{Z} \times R \to R$ definida por:

$$\Phi(n,z) = \begin{cases} z+z+\cdots^{n)}+z, & n>0\\ 0, & n=0\\ -z-z-\cdots^{-n)}-z, & n<0. \end{cases}$$

Normalmente esta aplicación se denota simplemente por yuxtaposición, $\Phi(n,x) = nx$ y satisface las siguientes propiedades:

$$\begin{aligned}
(n+m)x &= nx+mx & n(x+y) &= nx+ny\\
(nm)x &= n(mx) & n(xy) &= (nx)y = x(ny)
\end{aligned}$$

**Proposición 21** *Sea $R$ un anillo. Entonces $\mathbb{Z} \times R$ con suma y producto:*

$$(\lambda, r) + (\mu, r') := (\lambda + \mu, r + r')$$
$$(\lambda, r).(\mu, r') := (\lambda\mu, \lambda r' + \mu r + r.r')$$

*Tiene estructura de anillo unitario. Es más, la aplicación $\psi : R \to \mathbb{Z} \times R$ dada por $\psi(r) = (0, r)$ es un monomorfismo de anillos.*

**Definición 22** Sea $R$ un anillo. Se define la unitización de $R$, y se representa por $R^1$ como $R$, si éste ya es un anillo unitario o $\mathbb{Z} \times R$ caso de que $R$ no sea unitario.

# 5. La característica de un anillo

**Definición 1** Sea $R$ un anillo. Si existe el menor natural $n \in \mathbb{N}$ tal que $a + \overset{n)}{\cdots} + a = 0$ para todo $a \in R$ se dice que la característica de $R$ es $n$. En caso contrario se dice que la característica de $R$ es cero.

**Ejemplos A** *Dado $n \in \mathbb{N}$, la característica de $\mathbb{Z}_n$ es $n$. La característica de $\mathbb{Z}$ es cero.*

**Proposición 2** Sea $R$ un anillo unitario. Entonces la característica de $R$ o es cero o el menor natural tal que $1 + \overset{n)}{\cdots} + 1 = 0$ (o excluyente).

**Demo:** Si no existe ningún $k \in \mathbb{N}$ tal que $1 + \overset{k)}{\cdots} + 1 = 0$, entonces, por definición, la característica de $R$ es cero. Supongamos que existe un $k \in \mathbb{N}$ tal que $1 + \overset{k)}{\cdots} + 1 = 0$ y sea $n$ el menos natural que cumple esta propiedad. entonces, para todo $a \in R$,

$$a + \overset{k)}{\cdots} + a = a1 + \overset{k)}{\cdots} + a1 = a(1 + \overset{k)}{\cdots} + 1) = a0 = 0$$

Por lo que $n$ es la característica de $R$. ■

**Proposición 3 (ejercicio)** La característica de un anillo y de su unitización no tienen que coincidir. Es más, si $R$ no es unitario la característica de $R^1$ es cero.

**Proposición 4 (ejercicio)** ¿Se te ocurre una nueva construcción para "sumergir" un anillo no unitario en un anillo unitario manteniendo la característica?

**Proposición 5** La característica de un dominio de integridad $D$ es cero o un número primo.

**Demo:** Si la característica de $D$ es cero no hay nada que demostrar. Supongamos por tanto que $D$ tiene característica $n \in \mathbb{N}$. Por reducción al absurdo, si $n$ no fuera primo, existiría $r, s \in \mathbb{N}$, con $1 < r, s < n$ tales que $n = rs$. En este caso,

$$0 = 1 + \overset{n)}{\cdots} + 1 = (1 + \overset{r)}{\cdots} + 1)(1 + \overset{s)}{\cdots} + 1).$$

Lo que implicaría, al ser $n$ el menor natural con $1 + \overset{n)}{\cdots} + 1 = 0$ que $1 + \overset{r)}{\cdots} + 1$ y $1 + \overset{s)}{\cdots} + 1$ son dos elementos no nulos de $D$ de producto cero, una contradicción ya que en $D$ no hay divisores de cero. ■

★ Los ejercicios del 38 al 42 te pueden servir para saber si has asimilado los conceptos de esta sección.

# 6. Los Cuaterniones de Hamilton

Hasta ahora no hemos visto un anillo de división que no sea conmutativo, es decir, un anillo de división que no sea cuerpo. Veamos aquí el primero.

La construcción del anillo de los cuaterniones de Hamilton es muy parecida a como se construye $\mathbb{C}$, los números complejos, a partir de $\mathbb{R}$, el cuerpo de los reales:

Vamos a considerar como conjunto base $\mathbb{H} := \mathbb{R}\times\mathbb{R}\times\mathbb{R}\times\mathbb{R}$. Denotamos los siguientes elementos como:

$$\begin{aligned} 1 &:= (1,0,0,0) & i &:= (0,1,0,0)\\ j &:= (0,0,1,0) & k &:= (0,0,0,1) \end{aligned}$$

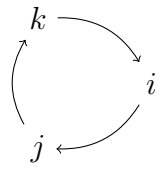
Con esta notación tenemos que los elementos de $\mathbb{H}$ son de la forma

$$\mathbb{H} := \{\alpha_1 + \alpha_2 i + \alpha_3 j + \alpha_4 k \ |\alpha_i \in \mathbb{R}, i = 1,\dots,4\}.$$

En este conjunto definimos la suma por componentes, con lo que $(\mathbb{H},*)$ tiene estructura de grupo abeliano (es una mera comprobación). Definimos el producto en $\mathbb{H}$ siguiendo las siguientes reglas:

$$i^2 = -1 \quad j^2 = -1 \quad k^2 = -1 \quad 1\cdot h = h\cdot 1 \ \forall h \in \mathbb{H} \quad \text{y}$$

Si multiplicas dos de estos siguiendo la dirección de las flechas te da el siguiente, $i\cdot j = k \quad j\cdot k = i \quad k\cdot i = j$. Si multiplicas dos de estos en sentido contrario a las flechas te da el siguiente cambiado de signo, $j\cdot i = -k \quad k\cdot j = -i \quad i\cdot k = -j$.




Todos los demás productos aparecen aplicado la propiedad distributiva:

$$\begin{aligned} (\alpha_1 + \alpha_2 i + \alpha_3 j + \alpha_4 k)\cdot(\beta_1 + \beta_2 i + \beta_3 j + \beta_4 k) :&= \alpha_1\beta_1 - \alpha_2\beta_2 - \alpha_3\beta_3 - \alpha_4\beta_4\\ &+ (\alpha_1\beta_2 + \alpha_2\beta_1 + \alpha_3\beta_4 - \alpha_4\beta_3)i\\ &+ (\alpha_1\beta_3 - \alpha_2\beta_4 + \alpha_3\beta_1 + \alpha_4\beta_2)j\\ &+ (\alpha_1\beta_4 + \alpha_2\beta_3 - \alpha_3\beta_2 + \alpha_4\beta_1)k \end{aligned}$$

**Teorema 1** Con las notaciones anteriores, $(\mathbb{H},+,\cdot)$ es un anillo de división no conmutativo (por tanto no es un cuerpo).

**Demo:** El principio de la demostración de la proposición 1 (Pag. 61) nos demuestra que $(\mathbb{H},+)$ es un grupo abeliano, por lo que sólo nos tenemos que preocupar de demostrar las demás propiedades:

$\star$ La asociatividad del producto: Denotemos por $p_1 = 1, p_2 = i, p_3 = j, p_4 = k$. Tenemos entonces

$$\left((\sum_{r=1}^{4}\alpha_i p_i)(\sum_{s=1}^{4}\beta_i p_i)\right)(\sum_{t=1}^{4}\gamma_i p_i) = \sum_{r,s,t=1}^{4}\alpha_r\beta_s\gamma_t\,(p_r p_s)p_t$$

$$(\sum_{r=1}^{4}\alpha_i p_i)\left((\sum_{s=1}^{4}\beta_i p_i)(\sum_{t=1}^{4}\gamma_i p_i)\right) = \sum_{r,s,t=1}^{4}\alpha_r\beta_s\gamma_t\,p_r(p_s p_t)$$

Luego, si para todo $r, s, t \in \{1, 2, 3, 4\}$, $(p_r p_s)p_t = p_r(p_s p_t)$, entonces los dos sumatorios anteriores serán iguales y habremos demostrado la propiedad asociativa.

(a). Si $r = 1$ o $s = 1$ o $t = 1$, entonces $(p_1 p_s)p_t = p_s p_t = p_1(p_s p_t)$.

(b). Si $r = s = k$, $(p_r p_r)p_r = -p^r = p_r(p_r p_r)$. Veamos las siguientes 24 igualdades restantes:

| | | |
|---|---|---|
| $(ii)j = -j = ik = i(ij)$ | $(ij)i = ki = j = -ik = i(ji)$ | $(ji)i = -ki = -j = j(ii)$ |
| $(ii)k = -k = -ij = i(ik)$ | $(ik)i = -ji = k = ij = i(ki)$ | $(ki)i = ji = -k = k(ii)$ |
| $(jj)k = -k = ji = j(jk)$ | $(jk)j = ij = k = -ji = j(kj)$ | $(kj)j = -ij = -k = k(jj)$ |
| $(jj)i = -i = -jk = j(ji)$ | $(ji)j = -kj = i = jk = j(ij)$ | $(ij)j = kj = -i = i(jj)$ |
| $(kk)i = -i = kj = k(ki)$ | $(ki)k = jk = i = -kj = k(ik)$ | $(ik)k = -jk = -i = i(kk)$ |
| $(kk)j = -j = -ki = k(kj)$ | $(kj)k = -ik = j = ki = k(jk)$ | $(jk)k = ik = -j = j(kk)$ |
| $(ij)k = k^2 = i^2 = i(jk)$ | $(ji)k = -k^2 = -j^2 = j(ik)$ | $(ik)j = -j^2 = -i^2 = i(kj)$ |
| $(ki)j = j^2 = k^2 = k(ij)$ | $(jk)i = i^2 = j^2 = j(ki)$ | $(kj)i = -i^2 = -k^2 = k(ji)$ |

$\star$ Es claro que $(\mathbb{H}, +, \cdot)$ es unitario, con unidad 1.

$\star$ Es claro que $(\mathbb{H}, +, \cdot)$ no es conmutativo, ya que $ij = k$, y $ji = -k$.

$\star$ Tenemos que demostrar ahora que todo elemento no nulo de $(\mathbb{H}, +, \cdot)$ posee un inverso. Pero,

$$(\alpha_1 + \alpha_2 i + \alpha_3 j + \alpha_4 k) \cdot (\alpha_1 - \alpha_2 i - \alpha_3 j - \alpha_4 k) = \alpha_1^2 + \alpha_2^2 + \alpha_3^2 + \alpha_4^2$$

por tanto, si $h = \alpha_1 + \alpha_2 i + \alpha_3 j + \alpha_4 k \neq 0$, $0 \neq \alpha_1^2 + \alpha_2^2 + \alpha_3^2 + \alpha_4^2 \in \mathbb{R}$ y

$$h^{-1} = \frac{\alpha_1}{\alpha_1^2 + \alpha_2^2 + \alpha_3^2 + \alpha_4^2} - \frac{\alpha_2}{\alpha_1^2 + \alpha_2^2 + \alpha_3^2 + \alpha_4^2} i - \frac{\alpha_3}{\alpha_1^2 + \alpha_2^2 + \alpha_3^2 + \alpha_4^2} j - \frac{\alpha_4}{\alpha_1^2 + \alpha_2^2 + \alpha_3^2 + \alpha_4^2} k$$

Lo que demuestra que todo elemento no nulo de $\mathbb{H}$ posee inverso.

$\star$ Por último la distributiva es evidente, por la propia definición del producto. ■

**Definición 2** *Sea $(\mathbb{H}, +, \cdot)$ el anillo de división de los Cuaterniones de Hamilton. Se define:*

- *El conjugado de un elemento $h = \alpha_1 + \alpha_2 i + \alpha_3 j + \alpha_4 k \in \mathbb{H}$ y se denota por $\overline{h}$ como $\overline{h} := \alpha_1 - \alpha_2 i - \alpha_3 j - \alpha_4 k$.*
- *Se define la norma de un elemento $h = \alpha_1 + \alpha_2 i + \alpha_3 j + \alpha_4 k \in \mathbb{H}$ y se denota por $|h|$ como $|h| := \alpha_1^2 + \alpha_2^2 + \alpha_3^2 + \alpha_4^2$.*

**Nota:** Observar que el inverso de un elemento no nulo $h \in \mathbb{H}$ es $h^{-1} = \frac{\overline{h}}{|h|}$.

# 7. Ampliación de contenidos

## 7.1. Anillos de endomorfismos de un grupo abeliano

**Nota:** El conjunto de los homomorfismos entre dos anillos $R$ y $R'$ no tiene muy buenas propiedades, ya que ni la suma natural de aplicaciones es un homomorfismo: si consideramos la identidad en $\mathbb{Z}$, el anillo de los enteros, se tiene que $Id + Id$ no es un homomorfismo. ¿Cuales son los endomorfismos de $\mathbb{Z}$?

**Definición 1** *Sean $G$ y $G'$ dos grupos. Se define un* ***homomorfismo de grupos*** *de $G$ en $G'$ como una aplicación $f : G \to G'$ tal que:*

$$f(a+b) = f(a) +' f(b) \quad \text{para todo } a, b \in G$$

*Se define* $\mathrm{Hom}(G, G')$ *como el conjunto de todos los homomorfismos de $G$ en $G'$. Por* $\mathrm{End}(G)$ *denotaremos al conjunto de todos los homomorfismos de $G$ en $G$.*

**Proposición 2** *Sean $G$ y $G'$ dos grupos. Entonces*

*(1)* $\mathrm{Hom}(G, G')$ *es un grupo con la suma usual: dados $f, g \in \mathrm{Hom}(G, G')$,*

$$f + g : G \to G' \quad \text{definida por} \quad f + g(a) = f(a) + g(a).$$

*Es mas, si $G'$ es conmutativo,* $\mathrm{Hom}(G, G')$ *es un grupo abeliano*

*(2)* $\mathrm{End}(G)$ *con la suma usual y la composición de aplicaciones,* $(\mathrm{End}(G), +, \circ)$ *es un anillo unitario.*

**Teorema 3** *Todo anillo es isomorfo a un subanillo de un anillo de endomorfismos de un cierto grupo abeliano.*

**Demo:** Consideremos $R^1$ con su estructura de grupo abeliano. Veamos que la aplicación $\Phi : R \to \mathrm{End}(R^1)$ definida por $\Phi_r(r') = rr'$ es un monomorfismos de anillos: dados $r_1$ y $r_2$ elementos de $R$,

- $\Phi_{r_1+r_2}(r') = (r_1 + r_2)r' = r_1r' + r_2r' = \Phi_{r_1}(r') + \Phi_{r_2}(r')$
- $\Phi_{r_1}\Phi_{r_2}(r') = r_1(r_2r') = (r_1r_2)r' = \Phi_{r_1r_2}(r')$

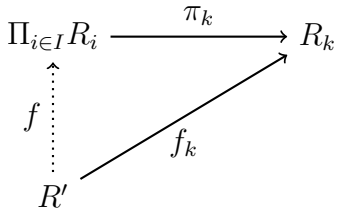
Lo que demuestra que es un homomorfismo de anillos. Por último, si $\Phi_r = 0$, $0 = \Phi_r(1) = r$, lo que demuestra que es inyectiva. ■

**Nota:** Este teorema nos dice como son todos los anillos (resultado poco útil).

**Nota:** La aplicación inversa de un automorfismo $f : R \to R$ es precisamente el inverso de $f$ en $\mathrm{End}(R)$ (considerado $R$ únicamente como grupo abeliano).

## 7.2. Propiedad fundamental del producto directo de anillos

**Proposición 4** *Sean $R_i$, $i \in I$ una familia de anillos y sea $R = \Pi_{i\in I} R_i$ el producto directo de los $R_i$. Entonces para cada anillo $R'$ y cada familia de homomorfismos de anillos $f_i : R' \to R_i$ existe un único homomorfismo de anillos $f : R' \to R$ tal que para cada $k \in I$ el siguiente diagrama es conmutativo:*




*Es más, Si $\hat{R}$ es un anillo y $\rho_i : \hat{R} \to R_i$ son una familia de epimorfismos de anillos tales que para cada anillo $R'$ y cada familia de homomorfismos de anillos $f_i : R' \to R_i$ existe un único homomorfismo de anillos $f : R' \to \hat{R}$ tal que para cada $k \in I$ el diagrama anterior es conmutativo, entonces $\hat{R}$ es isomorfo a $\Pi_{i\in I} R_i$.*

**Demo:** Tenemos que demostrar la existencia y unicidad del homomorfismo $f : R' \to R$ que hace conmutativo el diagrama. La estrategia que vamos a usar para demostrarlo va a consistir en demostrar que hay una única aplicación que hace conmutativo el diagrama y para luego demostrar que esta única posibilidad es el homomorfismo de anillos que buscamos:

1-. Supongamos que existe $f : R' \to \Pi_{i\in I} R_i$ tales que $\pi_k \circ f = f_k$ tenemos entonces que dado $r' \in R'$, $f_k(r') = \pi_k(f(r'))$, por lo que la coordenada k-esima de $f(r')$ es $f_k(r')$. Así, $f(r')$ tiene que ser forzosamente $(f_i(r'))_{i\in I}$.

2-. Comprobemos entonces que la aplicación $f : R' \to \Pi_{i\in I} R_i$ definido por $f(r') = (f_i(r'))_{i\in I}$ es un homomorfismo de anillos que verifica el enunciado:

⋆ ¿Es homomorfismo de grupos?

$$\begin{aligned} f(r'_1 + r'_2) &= (f_i(r'_1 + r'_2))_{i\in I} = (f_i(r'_1) + f_i(r'_2))_{i\in I} = (f_i(r'_1))_{i\in I} + (f_i(r'_2))_{i\in I} \\ &= f(r'_1) + f(r'_2) \end{aligned}$$

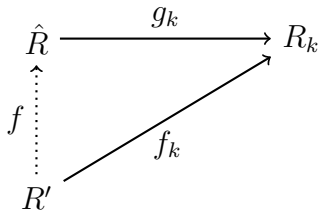
⋆ ¿Es homomorfismo de anillos?

$$\begin{aligned} f(r'_1.r'_2) &= (f_i(r'_1.r'_2))_{i\in I} = (f_i(r'_1).f_i(r'_2))_{i\in I} = (f_i(r'_1))_{i\in I}.(f_i(r'_2))_{i\in I} \\ &= f(r'_1)f(r'_2) \end{aligned}$$

⋆ ¿Hace conmutativo los diagramas? Pues claro

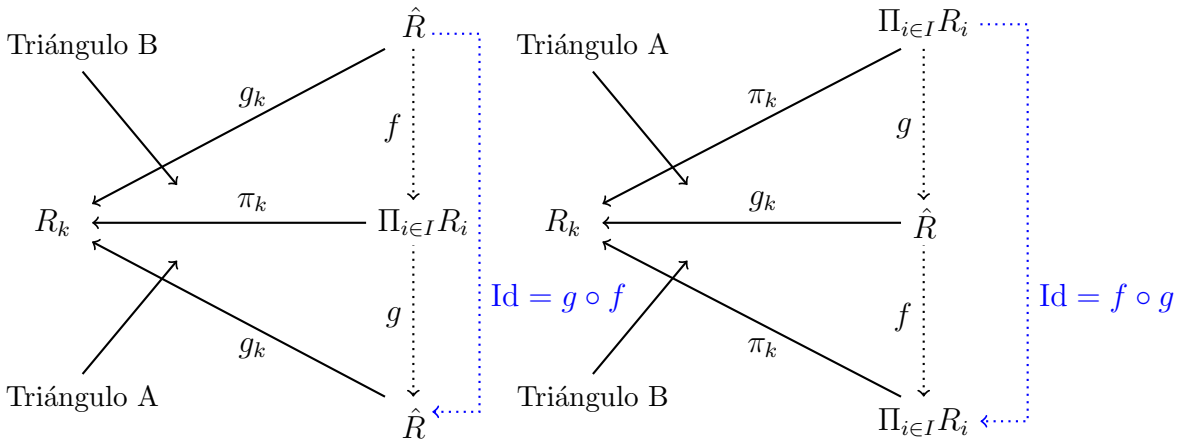
$$\pi_k \circ f(r') = \pi_k((f_i(r'))_{i\in I})) = f_k(r').$$

Veamos ahora que todo anillo con estas propiedades es isomorfo al producto cartesiano de los $\{R_i\}_{i\in I}$. Sea $\hat{R}$ un anillo y $g_i : \hat{R} \to R_i$ una familia de epimorfismos de anillos tales que para cada anillo $R'$ y cada familia de homomorfismos de anillos $f_i : R' \to R_i$ existe un único homomorfismo de anillos $f : R' \to \hat{R}$ tal que para cada $k \in I$ el diagrama




es conmutativo.

Si consideramos ahora $R' = \Pi_{i\in I} R_i$ y $f_i = \pi_i$ las proyecciones canónicas tenemos:



En donde $f$ es la única aplicación que hace conmutativo el triángulo B (aquí estamos aplicando que $\Pi_{i\in I}R_i$ verifica la propiedad del producto cartesiano, apartado 1-.) y en donde $g$ es la única aplicación que hace conmutativo el triángulo A (aquí estamos aplicando que, por hipótesis, $\hat{R}$ satisface la propiedad). Ahora,

$$g_k \circ \mathrm{Id} = g_k = \pi_k \circ g = (g_k \circ f) \circ g = g_k \circ (f \circ g)$$

Luego como $\hat{R}$ verifica la propiedad, $\mathrm{Id}_{\hat{R}} = f \circ g$ (estamos haciendo uso de la unicidad de la solución). Pero igualmente, si nos fijamos en el exterior del segundo diagrama,

$$\pi_k \circ \mathrm{Id} = \pi_k = g_k \circ f = (\pi_k \circ g) \circ f = \pi_k \circ (g \circ f)$$

Luego como $\Pi_{i\in I}R_i$ verifica la propiedad, $\mathrm{Id}_{\Pi_{i\in I}R_i} = g \circ f$ (estamos haciendo uso de la unicidad de la solución). Por tanto $f$ y $g$ son isomorfismo de anillos lo que demuestra que $\Pi_{i\in I}R_i$ y $\hat{R}$ son isomorfos. ■

## 7.3. Asociatividad en el producto de matrices

$$\left[\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} \cdot \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1} & b_{n2} & \cdots & b_{nn} \end{pmatrix}\right] \cdot \begin{pmatrix} c_{11} & c_{12} & \cdots & c_{1n} \\ c_{21} & c_{22} & \cdots & c_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ c_{n1} & c_{n2} & \cdots & c_{nn} \end{pmatrix} =$$

$$\begin{pmatrix} \sum_{r=1}^n a_{1r}\cdot b_{r1} & \sum_{r=1}^n a_{1r}\cdot b_{r2} & \cdots & \sum_{r=1}^n a_{1r}\cdot b_{rn} \\ \sum_{r=1}^n a_{2r}\cdot b_{r1} & \sum_{r=1}^n a_{2r}\cdot b_{r2} & \cdots & \sum_{r=1}^n a_{2r}\cdot b_{rn} \\ \vdots & \vdots & \ddots & \vdots \\ \sum_{r=1}^n a_{nr}\cdot b_{r1} & \sum_{r=1}^n a_{nr}\cdot b_{r2} & \cdots & \sum_{r=1}^n a_{nr}\cdot b_{rn} \end{pmatrix} \cdot \begin{pmatrix} c_{11} & c_{12} & \cdots & c_{1n} \\ c_{21} & c_{22} & \cdots & c_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ c_{n1} & c_{n2} & \cdots & c_{nn} \end{pmatrix} =$$

$$\begin{pmatrix} \sum_{r,s=1}^n (a_{1r}\cdot b_{rs})\cdot c_{s1} & \sum_{r,s=1}^n (a_{1r}\cdot b_{rs})\cdot c_{s2} & \cdots & \sum_{r,s=1}^n a_{1r}\cdot b_{rs})\cdot c_{sn} \\ \sum_{r,s=1}^n (a_{2r}\cdot b_{rs})\cdot c_{s1} & \sum_{r,s=1}^n (a_{2r}\cdot b_{rs})\cdot c_{s2} & \cdots & \sum_{r,s=1}^n (a_{2r}\cdot b_{rs})\cdot c_{sn} \\ \vdots & \vdots & \ddots & \vdots \\ \sum_{r,s=1}^n (a_{nr}\cdot b_{rs})\cdot c_{s1} & \sum_{r,s=1}^n (a_{nr}\cdot b_{rs})\cdot c_{s2} & \cdots & \sum_{r,s=1}^n (a_{nr}\cdot b_{rs})\cdot c_{sn} \end{pmatrix}$$

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} \cdot \left[\begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1} & b_{n2} & \cdots & b_{nn} \end{pmatrix} \cdot \begin{pmatrix} c_{11} & c_{12} & \cdots & c_{1n} \\ c_{21} & c_{22} & \cdots & c_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ c_{n1} & c_{n2} & \cdots & c_{nn} \end{pmatrix}\right] =$$

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} \cdot \begin{pmatrix} \sum_{s=1}^n b_{1s}\cdot c_{s1} & \sum_{s=1}^n b_{1s}\cdot c_{s2} & \cdots & \sum_{s=1}^n b_{1s}\cdot c_{sn} \\ \sum_{s=1}^n b_{2s}\cdot c_{s1} & \sum_{s=1}^n b_{2s}\cdot c_{s2} & \cdots & \sum_{s=1}^n b_{2s}\cdot c_{sn} \\ \vdots & \vdots & \ddots & \vdots \\ \sum_{s=1}^n b_{ns}\cdot c_{s1} & \sum_{s=1}^n b_{ns}\cdot c_{s2} & \cdots & \sum_{s=1}^n b_{ns}\cdot c_{sn} \end{pmatrix} =$$

$$\begin{pmatrix} \sum_{r,s=1}^n a_{1r}\cdot (b_{rs}\cdot c_{s1}) & \sum_{r,s=1}^n a_{1r}\cdot (b_{rs}\cdot c_{s2}) & \cdots & \sum_{r,s=1}^n a_{1r}\cdot (b_{rs}\cdot c_{sn}) \\ \sum_{r,s=1}^n a_{2r}\cdot (b_{rs}\cdot c_{s1}) & \sum_{r,s=1}^n a_{2r}\cdot (b_{rs}\cdot c_{s2}) & \cdots & \sum_{r,s=1}^n a_{2r}\cdot (b_{rs}\cdot c_{sn}) \\ \vdots & \vdots & \ddots & \vdots \\ \sum_{r,s=1}^n a_{nr}\cdot (b_{rs}\cdot c_{s1}) & \sum_{r,s=1}^n a_{nr}\cdot (b_{rs}\cdot c_{s2}) & \cdots & \sum_{r,s=1}^n a_{nr}\cdot (b_{rs}\cdot c_{sn}) \end{pmatrix}$$

# 8. Ejercicios del Tema

**1** Decir si los siguientes conjuntos, con las operaciones indicadas, tienen estructura de anillo. En caso afirmativo: ¿son conmutativos?, ¿unitarios?, ¿de división?... ¿cuáles son sus elementos inversibles?

(i) $\mathbb{Z}^+$ con la suma y producto usual.

(ii) $\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ con la suma y producto usual.

(iii) $\mathbb{N}$ con primera operación: el producto y segunda operación la potencia, es decir:
"$a + b$ igual a $ab$" y "$a$ por $b$ igual a $a^b$".

(iv) $\{x \in \mathbb{Q} \mid 3x \in \mathbb{Z}\}$ con las operaciones usuales.

**2** Sea $X$ un conjunto no vacío, $\mathcal{P}$ el conjunto de partes de $X$ y $\triangle$ la operación diferencia simétrica. Demuestra que $(\mathcal{P}(X), \triangle, \cap)$ es un anillo conmutativo y unitario. Da una condición necesaria y suficiente para que sea dominio de integridad.

**3** Sea $(R, +, \cdot)$ un anillo y sea $a \in R$. Demuestra que $R$ con su misma suma y un nuevo producto dado por $x \cdot_a y = xay$ tiene estructura de anillo, es decir, que $(R, +, \cdot_a)$ tiene estructura de anillo. ¿Se te ocurre alguna condición para que este nuevo anillo sea unitario?

**4** Sea $R$ un anillo unitario y sea $\mathcal{U}(R)$ el conjunto de los elementos inversibles de $R$. Demuestra que el producto de $R$ define una operación en $\mathcal{U}(R)$ que dota a éste de estructura de grupo. Demuestra que si $R$ es un anillo conmutativo, $(\mathcal{U}(R), \cdot)$ es un grupo abeliano.

**5** Sea $R$ un anillo. Demuestra que si $a \in R$ es un divisor de cero, entonces $a$ no es inversible.

**6** ¿Puedes encontrar un anillo $R$ con divisores de cero por la izquierda pero sin divisores de cero por la derecha?

**7** Sea $(R, +, \cdot)$ un anillo. Demuestra que las siguientes condiciones son equivalentes:

(i) $R$ no posee divisores de cero por la izquierda (Resp. derecha).

(ii) Se verifican las leyes de cancelación por la izquierda (Resp. derecha).

**8** Demuestra que para un anillo conmutativo y unitario $(R, +, \cdot)$ las siguientes condiciones son equivalentes:

(i) $R$ es un dominio de integridad.

(ii) Se verifican las leyes de cancelación en $R$. Es decir,

$$\text{Si } ax = ay \text{ con } a \neq 0, \text{ entonces } x = y$$
$$\text{Si } xa = ya \text{ con } a \neq 0, \text{ entonces } x = y$$

**9** Sea $(R, +, \cdot)$ un anillo. Demuestra que $R$ verifica la ley de cancelación por la izquierda si y sólo si verifica la ley de cancelación por la derecha.

**10** Demuestra que en un anillo unitario $(R, +, \cdot)$ el cero (neutro para la suma) y el 1 (neutro para el producto) son elementos distintos.

**11** ¿Es posible dar una estructura de anillo en el conjunto $\mathbb{Z}$ en donde la primera operación sea el producto? ¿Y en la que la segunda operación sea la suma? Demuestra que no es posible o construye dicha operación. *

**12** Sea $R$ un anillo unitario y $a \in R$ tal que existe $b \in R$ con $ab = 1$. Demuestra que son equivalentes: *

- $a$ no es inversible.
- existe $b' \in R$ con $b' \neq b$ y $ab' = 1$.
- $a$ es divisor de cero.

Demuestra que en las condiciones anteriores, $R$ contiene un idempotente no trivial (distinto de 0 y 1). *

**13** Sea $R$ un anillo. Demuestra que si para todo $a, b \in R$ la ecuación $aX = b$ tiene a lo sumo una solución, entonces en $R$ no hay divisores de cero. ¿Es cierto del recíproco? *

**14** Demuestra que en $\mathbb{Z}_{12}$ la ecuación $X^2 - 1 = 0$ tiene más de dos soluciones. Demuestra que en un dominio de integridad la ecuación anterior sólo posee, a lo sumo, dos soluciones. ¿Sabrías encontrar un anillo en donde sólo posea una?

**15** Sea $R$ un anillo. Un elemento $x \in R$ se dice idempotente si $x = x^2$. Demuestra que un anillo en donde todo elemento es idempotente es conmutativo. *

**16** Sea $R$ un anillo y $e \in R$ un idempotente. Demuestra que

$$eRe := \{exe \mid x \in R\} = \{x \in R \mid xe = ex = x\}$$

es un subanillo unitario de $R$ (que no se te olvide comprobar la igualdad de los conjuntos anteriores). Demuestra que si $eRe = R$, entonces $e = 1$.

**17** Demuestra que todo subanillo unitario de un dominio de integridad es un dominio de integridad. En particular, todo subanillo unitario de un cuerpo es un dominio de integridad.

**18** Demuestra que si $R$ es un anillo unitario y $S$ es un subanillo suyo, $S$ no tiene por qué ser unitario. Es más, si $S$ es unitario las unidades de $R$ y $S$ pueden no coincidir. *

**19** Sea $R$ un anillo sin divisores de cero y $S$ un subanillo de $R$. Demuestra que si $S$ es unitario, entonces $R$ es unitario con la misma unidad.

**20** Sea $R$ un anillo y $f : R \to \mathcal{M}_2(R)$ definido por $f(r) = \begin{pmatrix} r & 0 \\ 0 & 0 \end{pmatrix}$. Demuestra que $f$ es un monomorfismo de anillos.

**21** Sean $n, m \in \mathbb{N}$ primos entre si. Demuestra que la aplicación $f : \mathbb{Z}_{nm} \to \mathbb{Z}_n \times \mathbb{Z}_m$ definida por $f(\overline{r}) = (\overline{r}, \overline{r})$ es un isomorfismo de anillos. (Acuérdate de demostrar que $f$ está bien definida)

**22** Sea $R$ un anillo y $f : R \to R$ un homomorfismo de anillos. Demuestra que la aplicación $\hat{f} : \mathcal{M}_2(R) \to \mathcal{M}_2(R)$ definido por $\hat{f}(a_{ij}) = (f(a_{ij}))$ es un homomorfismo de anillos. Demuestra que si $f$ es un monomorfismo $\hat{f}$ también lo es. ¿Si $f$ es un epimorfismo, $\hat{f}$ tiene que serlo?

**23** Encuentra un homomorfismo $f : R \to R'$ con $R$ y $R'$ anillos unitarios y $f(1_R) \neq 1_{R'}$.

**24** ¿Cuales son los endomorfismos de $\mathbb{Z}$?

**25** Sea $R$ un anillo. Encuentra dos monomorfismo de anillos $f : R \to \mathcal{M}_2(R)$.

**26** Se dice que una propiedad (que pueda poseer un anillo) es estructural si siempre que la verifique un anillo $R$ la verifica cualquier anillo isomorfo a él ($R$ y $R'$ son isomorfos si existe un isomorfismo $f : R \to R'$). Demuestra que ser conmutativo, ser unitario, no poseer divisores de cero, poseer $n$ elementos inversibles son propiedades estructurales. ¿Se te ocurre alguna más?

**27** Demuestra que no hay ningún isomorfismo entre $\mathbb{Z}_4$ y $\mathbb{Z}_2 \times \mathbb{Z}_2$.

**28** Sean $R$ y $R'$ dos anillos y $f : R \to R'$ un homomorfismo de anillos. Entonces:

(i) Si $R$ es un anillo unitario, $\mathrm{Im}(f)$ es un anillo unitario con unidad $f(1)$.
(ii) Si $a$ es un elemento inversible de $R$, $f(a)$ es un elemento inversible de $\mathrm{Im}(f)$.
(iii) Si $f$ es sobreyectiva, entonces $f(1) = 1'$ y $f(a)$ es inversible para todo elemento inversible $a \in R$.
(iv) Si $R$ y $R'$ son unitarios y $f(1) = 1'$, $f(a)$ es inversible para todo elemento inversible $a \in R$.

**29** *Sea $\{R_i\}_{i\in I}$ una familia de anillos y sea $R = \Pi_{i\in I} R_i$ el producto directo de los $R_i$. Demuestra que para cada $k \in I$, la proyección canónica $\pi_k : \Pi_{i\in I} R_i \to R_k$ es un epimorfismo de anillos.*

**30** *Sean $\{R_i\}_{i\in I}$, $\{S_i\}_{i\in I}$ dos familia de anillos indizadas en el mismo conjunto $I$. Supongamos que para cada $i \in I$ existe un homomorfismo de anillos $f_i : R_i \to S_i$. Demuestra que existe un único homomorfismo de anillos $f : \{R_i\}_{i\in I} \to \{S_i\}_{i\in I}$ tal que $f_i \circ \pi_i^r = \pi_i^s \circ f$.*

**31** *Sea $\{R_i\}_{i\in I}$ una familia de anillos y sea $R = \Pi_{i\in I} R_i$ el producto directo de los $R_i$. Demuestra que,*

- *$R$ es unitario si y sólo si $R_k$ es unitario para todo $k \in I$.*
- *$R$ es conmutativo si y sólo si $R_k$ es conmutativo para todo $k \in I$.*
- *Si $\#I \geq 2$, $R$ tiene divisores de cero. Por tanto, en este caso, $R$ no puede ser dominio de integridad, anillo de división o cuerpo.*

**32** *Sea $\{R_i\}_{i\in I}$ una familia de anillos y sea $R = \bigoplus_{i\in I} R_i$ la suma directa de los $R_i$. Demuestra que para cada $k \in I$, la inclusión canónica $\rho_k : R_k \to \bigoplus_{i\in I} R_i$ es un monomorfismo de anillos.*

**33** *Sea $R$ un anillo y $n \in \mathbb{N}$. Demuestra los siguientes enunciados:*

*(i)* $\mathcal{M}_n(R)$ *es unitario si y sólo si* $R$ *es unitario.*
*(i)* $\mathcal{M}_n(R)$ *tiene divisores de cero si* $n \leq 2$*. Por tanto, en este caso,* $\mathcal{M}_n(R)$ *no puede ser dominio de integridad, anillo de división o cuerpo.*
*(ii)* $\mathcal{M}_n(R)$ *es conmutativo si y sólo si* $R$ *es conmutativo y* $n = 1$*.*
*(iii)* $\mathcal{M}_n(R)$ *es un anillo de división si y sólo si* $R$ *es un anillo de división y* $n = 1$*.*
*(iv)* $\mathcal{M}_n(R)$ *es un cuerpo si y sólo si* $R$ *es un cuerpo y* $n = 1$*.*

**34** *Sea* $R$ *un anillo y sea* $R[[X]]$ *el anillo de series formales con coeficientes en* $R$*. Entonces:*

*(i)* $R$ *es unitario si y sólo si* $R[[X]]$ *es unitario.*
*(ii)* $R$ *es conmutativo si y sólo si* $R[[X]]$ *es conmutativo.*
*(ii)* $R$ *es D.I si y sólo si* $R[[X]]$ *es D.I.*

**35** *Sea* $R$ *un anillo unitario y sea* $R[[X]]$ *el anillo de series formales con coeficientes en* $R$*. Entonces un elemento* $\sum_{n=0}^{\infty} a_n X^n \in R[[X]]$ *es inversible si y sólo si* $a_0$ *es un elemento inversible de* $R$*.*

**36** *Sea* $R$ *un anillo unitario y sea* $R[[X]]$ *el anillo de series formales con coeficientes en* $R$*.Calcula el inverso de la serie* $p(x) = 1 - x$*.*

**37** Sea $R$ un anillo y sea $R[X]$ el anillo de polinomios con coeficientes en $R$ y sean $p(X), q(X) \in R[X]$. Entonces

(i) $R$ es conmutativo si y sólo si $R[X]$ es conmutativo.
(ii) $R$ es unitario si y sólo si $R[X]$ es unitario.
(iii) $R$ es dominio de integridad si y sólo si $R[X]$ es dominio de integridad.
(iv) $\deg(p(X) + q(X)) \leq \text{Max}(\deg(p(X)), \deg(q(X)))$.
(v) $\deg(p(X) \cdot q(X)) \leq \deg(p(X)) + \deg(q(X))$.
(vi) Es más, $R$ no posee divisores de cero si para todo $p(X), q(X) \in R[X]$ se tiene que

$$\deg(p(X) \cdot q(X)) = \deg(p(X)) + \deg(q(X)).$$

**38** Sea $R$ un anillo sin divisores de cero y sea $R^1$ su unitización. ¿Puede suceder que $R^1$ tenga divisores de cero?

**39** Demuestra que la característica de un anillo y de su unitización no tienen que coincidir. Es más, si $R$ no es unitario la característica de $R^1$ es cero.

**40** ¿Se te ocurre una nueva construcción para "sumergir" un anillo no unitario en un anillo unitario manteniendo la característica? $\boxed{*}$

**41** Sea $R$ un anillo (no necesariamente unitario) de característica 6. Demuestra que en $R$ hay divisores de cero.

**42** Sea $R$ un anillo de característica $n$ y $S$ un anillo de característica $m$. Determina la característica de los siguientes anillos:

(i) El anillo producto cartesiano, $R^n$
(ii) El anillo producto cartesiano, $R \times S$.
(iii) El anillo de polinomios, $R[X]$.
(iv) El anillo de matrices, $\mathcal{M}_k(R)$.

**43** Sea $(M, *)$ un monoide. Demuestra que si existe $a \in M$, $a$ distinto del neutro, con $a^2 = a$, entonces $(M, *)$ no es un grupo. [*]

**44** *Sea $\mathbb{H}$ el anillo de los cuaterniones de Hamilton. Calcula la norma y el inverso de los siguientes elementos:*

$$1 + i + j + k, \quad 1 - i + j - k \quad 1 + i$$

**45** *Sea $\mathbb{H}$ el anillo de los cuaterniones de Hamilton. Calcula todos los elementos $x$ de $\mathbb{H}$ que verifiquen que $x^2 + 1 = 0$.*

**46** Se dice que un elemento $x$ en un anillo $R$ es nilpotente si existe $n \in \mathbb{N}$, con $n > 1$, tal que $x^n = 0$. Encuentra una condición necesaria y suficiente para que $\mathbb{Z}_n$ no tenga elementos nilpotentes. Calcula los nilpotentes de $\mathbb{Z}_{120}$. [*]

**47** Demuestra que un anillo $R$ no posee elementos nilpotentes si y sólo si el único elemento $x \in R$ tal que $x^2 = 0$ es $x = 0$.

**48** Demuestra que en un anillo sin divisores de cero los únicos (posibles) idempotentes son 0 y 1 (llamados idempotentes triviales). Encuentra algún idempotente no trivial en $\mathcal{M}_n(\mathbb{R})$.

**49** Demuestra que en un anillo sin idempotentes no triviales, si $ab = 1$ entonces $ba = 1$.

**50** Sea $R$ un anillo con al menos dos elementos. Supongamos que para cada $0 \neq x \in R$ existe un **único** $y \in R$ con $x = xyx$. Demuestra que: $R$ no tiene divisores de cero. Si $xyx = x$, entonces $yxy = y$. $R$ es unitario. $R$ es un anillo de división. [**]

**51** Encuentra un anillo $R$ que no sea de división y tal que para cada $x \in R$ exista $y \in R$ con $x = xyx$. [*]

**52** ¿Puedes encontrar un anillo $R$ y un elemento $a$ tal que $a$ sea divisor de cero por la derecha pero no sea divisor de cero por la izquierda? [**]

**53** Da un ejemplo de un anillo $R$ no conmutativo tal que el conjunto de sus elementos inversibles, $\mathcal{U}(R)$ sea un grupo abeliano y otro en el que sea un grupo no abeliano (con el producto de $R$). [**]

**54** Sea $(M, *)$ un monoide. Demuestra que $M$ es un grupo si para todo $a, b \in M$ la ecuación $a \cdot X = b$ tiene solución (es decir, existe $s \in M$ tal que $a \cdot s = b$. [*]

**El símbolo [$*$] significa dificultad moderada y [$**$] dificultad media.**