Capítulo 3
Anillos y cuerpos (primer encuentro)

En este curso vamos a estudiar solamente grupos, pero para ver algunos ejemplos importantes de grupos, necesitamos revisar las definiciones de diferentes estructuras algebraicas. Estas se estudian en otros cursos y bastará que el lector conozca los ejemplos principales que voy a mencionar en este capítulo.

3.1 Anillos

3.1.1. Definición. 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 $0 \in R$ (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**.

3.1.2. Digresión. En algunos contextos naturales también surgen anillos sin identidad (donde no se cumple el axioma R4)) y anillos no asociativos (donde nose cumple R3)), pero los vamos a ignorar en este curso.

Note que respecto a la multiplicación, no se pide existencia de elementos inversos (x^{-1} tal que $xx^{-1} = 1 = x^{-1}x$) para ningún elemento.

3.1.3. Observación. *De los axiomas de arriba siguen las propiedades habituales como*

$$\begin{gathered} 0 \cdot x = x \cdot 0 = 0, \\ x \cdot (-y) = (-x) \cdot y = -xy, \\ x\,(y - z) = xy - xz, \quad (x - y)\,z = xz - yz. \end{gathered}$$

Demostración. Ejercicio para el lector. ■

Algunas propiedades conocidas se cumplen solamente en anillos conmutativos, como, por ejemplo, el teorema del binomio

$$(x + y)^n = \sum_{0 \le k \le n} \binom{n}{k} x^{n-k}\, y^k$$

En un anillo no conmutativo tenemos

$$(x + y)^2 = x^2 + xy + yx + y^2,$$

donde xy e yx no necesariamente coinciden.

3.1.4. Ejemplo. Los números enteros $\mathbb{Z}$, racionales $\mathbb{Q}$, reales $\mathbb{R}$, complejos $\mathbb{C}$ forman anillos conmutativos respecto a la adición y multiplicación habitual. ▲

3.1.5. Ejemplo. Para $n = 1, 2, 3, \ldots$ hemos notado en el capítulo 0 que sobre el conjunto

$$\mathbb{Z}/n\mathbb{Z} := \{[a]_n \mid a \in \mathbb{Z}\} = \{[0]_n, [1]_n, \ldots, [n-1]_n\}$$

formado por los restos módulo n

$$[a]_n := \{b \in \mathbb{Z} \mid a \equiv b \pmod{n}\}$$

se puede definir la adición y multiplicación mediante las fórmulas

$$\begin{aligned} [a]_n + [b]_n &:= [a + b]_n, \\ [a]_n \cdot [b]_n &:= [ab]_n. \end{aligned}$$

Se ve que $\mathbb{Z}/n\mathbb{Z}$ es un anillo conmutativo respecto a la adición y multiplicación módulo n. De hecho, estas operaciones son visiblemente asociativas y conmutativas. Las clases de equivalencia $[0]_n$ y $[1]_n$ son el cero y la identidad respectivamente. Los elementos opuestos son dados por $-[a]_n = [-a]_n$.

He aquí la tabla de adición y multiplicación para $n = 4$ (escribo simplemente "$[a]$" en vez de "$[a]_4$"):

$+$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$
$[1]$	$[1]$	$[2]$	$[3]$	$[0]$
$[2]$	$[2]$	$[3]$	$[0]$	$[1]$
$[3]$	$[3]$	$[0]$	$[1]$	$[2]$

$\cdot$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$	$[3]$
$[2]$	$[0]$	$[2]$	$[0]$	$[2]$
$[3]$	$[0]$	$[3]$	$[3]$	$[1]$

La notación "$\mathbb{Z}/n\mathbb{Z}$" será clara después de la definición de grupos cociente que veremos más adelante en nuestro curso. En algunos libros de texto se encuentra la notación "$\mathbb{Z}_n$", pero su uso en este contexto es un pecado mortal: si $n = p$ es primo, normalmente $\mathbb{Z}_p$ denota el *anillo de los enteros p-ádicos*. No lo vamos a ver en este curso, pero es algo muy importante en álgebra y aritmética. ▲

3.1.6. Ejemplo. El **anillo de los enteros de Gauss** es dado por

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

donde la adición y multiplicación están definidas de la manera habitual como para los números complejos. El cero y la identidad son los números $0 + 0 \cdot \sqrt{-1}$ y $1 + 0 \cdot \sqrt{-1}$ respectivamente. Está claro que para cualesquiera $x, y \in \mathbb{Z}[\sqrt{-1}]$ tenemos $x + y \in \mathbb{Z}[\sqrt{-1}]$ y $xy \in \mathbb{Z}[\sqrt{-1}]$ y por lo tanto todos los axiomas de anillos conmutativos se verifican fácilmente, ya que estos se cumplen para los números complejos. ▲

3.1.7. Ejemplo. Otro ejemplo del mismo tipo: consideremos el número complejo

$$\zeta_3 = e^{2\pi\sqrt{-1}/3} = -\frac{1}{2} + \frac{\sqrt{3}}{2}\sqrt{-1}.$$

Es una raíz cúbica de la unidad en el sentido de que $\zeta_3^3 = 1$. Se cumple la relación

$$\zeta_3^2 + \zeta_3 + 1 = 0.$$

(En general, el lector puede demostrar que para $\zeta_n := e^{2\pi\sqrt{-1}/n}$ se cumple $\sum_{0 \le k < n} \zeta_n^k = 0$.) Consideremos el conjunto

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

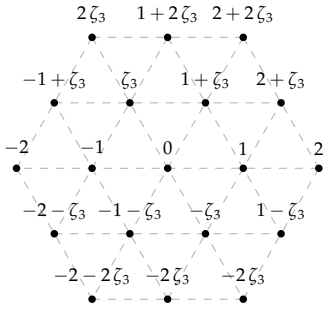
Está claro que para cualesquiera $x, y \in \mathbb{Z}[\zeta_3]$ se tiene $x + y \in \mathbb{Z}[\zeta_3]$. Para la multiplicación, si $x = a + b\,\zeta_3$ e $y = c + d\,\zeta_3$, entonces

$$(a + b\,\zeta_3) \cdot (c + d\,\zeta_3) = ac + (ad + bc)\,\zeta_3 + bd\,\zeta_3^2,$$

y usando la relación $\zeta_3^2 = 1 - \zeta_3$, podemos escribir la última expresión como

$$(ac - bd) + (bc + ad - bd)\,\zeta_3.$$

Entonces, para cualesquiera $x, y \in \mathbb{Z}[\zeta_3]$ tenemos $xy \in \mathbb{Z}[\zeta_3]$. Después de esta verificación se ve fácilmente que $\mathbb{Z}[\zeta_3]$ es un anillo conmutativo, puesto que $\mathbb{C}$ lo es. Este se llama el **anillo de los enteros de Eisenstein**[*]. El dibujo de abajo representa los enteros de Eisenstein en el plano complejo.



[*] Ferdinand Gotthold Max Eisenstein (1823–1852), matemático alemán, estudiante de Dirichlet, conocido por sus contribuciones en la teoría de números. Murió a los 29 años de tuberculosis (como Abel).

▲

3.1.8. Ejemplo. Tercer y último ejemplo de este tipo: añadamos a los números enteros la raíz cuadrada de 2:

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

Tenemos

$$(a + b\sqrt{2}) \cdot (c + d\sqrt{2}) = ac + 2bd + (ad + bc)\sqrt{2},$$

entonces para cualesquiera $x, y \in \mathbb{Z}[\sqrt{2}]$ se tiene $xy \in \mathbb{Z}[\sqrt{2}]$. El conjunto $\mathbb{Z}[\sqrt{2}]$ es un anillo conmutativo respecto a la adición y multiplicación habitual de números reales. Podemos llamar $\mathbb{Z}[\sqrt{2}]$ el **anillo de los enteros de Pitágoras**. ▲

3.1.9. Ejemplo. En general, un **entero algebraico** es un número $\alpha \in \mathbb{C}$ que satisface alguna ecuación polinomial

$$f(\alpha) = \alpha^n + a_{n-1}\,\alpha^{n-1} + \cdots + a_1\,\alpha + a_0,$$

donde $a_0, a_1, \ldots, a_{n-1} \in \mathbb{Z}$ y el coeficiente mayor a_n es igual a 1 (en este caso se dice que f es un polinomio **mónico**). Un resultado importante nos dice que todos los enteros algebraicos forman un anillo conmutativo, pero a priori no es claro para nada: si α es una raíz de un polinomio f como arriba y β es una raíz de otro polinomio

$$g(\beta) = \beta^m + b_{m-1}\,\beta^{m-1} + \cdots + b_1\,\beta + b_0,$$

entonces deben existir otros polinomios que tienen como sus raíces $\alpha \pm \beta$ y $\alpha\beta$, pero ¿cómo encontrarlos?

Por ejemplo, $\sqrt{2}$ es una raíz de la ecuación $x^2 - 2 = 0$ y $\sqrt{3}$ es una raíz de la ecuación $x^2 - 3 = 0$. Luego, la suma $\sqrt{2} + \sqrt{3}$ es una raíz de la ecuación

$$x^4 - 10\,x^2 + 1 = 0.$$

De hecho,

$$(\sqrt{2} + \sqrt{3})^2 = 2\sqrt{6} + 5, \quad (\sqrt{2} + \sqrt{3})^4 = 20\sqrt{6} + 49,$$

así que

$$(\sqrt{2} + \sqrt{3})^4 - 10\,(\sqrt{2} + \sqrt{3})^2 + 1 = 0.$$

El producto $\sqrt{2} \cdot \sqrt{3}$ es una raíz de

$$X^2 - 6 = 0.$$

En general, dados dos enteros algebraicos α y β, no es tan fácil encontrar los polinomios mónicos con coeficientes enteros que tienen $\alpha \pm \beta$ y $\alpha\beta$ como sus raíces. Vamos a ver más adelante que es siempre posible. ▲

3.2 Anillo de matrices $M_n(R)$

Todos los anillos de arriba son conmutativos. Mencionemos un ejemplo de anillos no conmutativos muy importante que seguramente es familiar al lector.

Sea R un anillo conmutativo. Entonces las matrices de $n \times n$ con elementos en R forman un anillo que vamos a denotar por $M_n(R)$. Recordemos que la adición de matrices se define término por término:

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

mientras que el producto

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

se define mediante la fórmula

$$c_{ij} := \sum_{1 \leq k \leq n} a_{ik}\, b_{kj}.$$

El cero es la matriz nula

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

y el neutro multiplicativo es la matriz identidad

$$I = \begin{pmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix}.$$

En un primer curso de álgebra lineal normalmente se considera $R = \mathbb{R}$ o $\mathbb{C}$ y se verifican los axiomas de anillos para este caso, pero el anillo específico R es irrelevante para llevar a cabo la construcción general.

El anillo $M_n(R)$ no es conmutativo para $n \geq 2$: por ejemplo, para $n = 2$ tenemos

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}, \tag{3.1}$$

y luego

$$\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$$

se cumple si y solamente si $1 = 0$. El lector puede verificar que esto es posible si y solamente si $R = \{0\}$ es un anillo que consiste en un elemento. Este se conoce como el **anillo nulo**.

En general, las únicas matrices que conmutan con todas las matrices son las **matrices escalares** que tienen forma

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

para algún $a \in R$. Lo vamos a ver en los ejercicios, pero el lector puede tratar de probarlo para las matrices de 2×2. Por ejemplo, se puede considerar una matriz $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ y ver qué significan las identidades $AB = BA$ para

$$B = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}.$$

3.3 Cuerpos

3.3.1. Definición. Un **cuerpo** k es un anillo conmutativo donde $1 \neq 0$ (es decir, $k \neq \{0\}$) y todo elemento no nulo es invertible. Es decir, para todo $x \neq 0$ existe x^{-1} tal que

$$xx^{-1} = x^{-1}x = 1.$$

3.3.2. Ejemplo. Los anillos conmutativos $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ son cuerpos. ▲

3.3.3. Definición. Cuando en un anillo se tiene $xy = 0$ para algunos elementos no nulos x e y, se dice que estos son **divisores de cero**. Si un anillo R no es nulo y no tiene divisores de cero, se dice que R es un **dominio de integridad**.

En otras palabras, R es un dominio de integridad si para cualesquiera $x, y \in R$ se cumple

$$\text{si } xy = 0 \text{ entonces } x = 0 \text{ o } y = 0. \tag{3.2}$$

La existencia de elementos inversos en un cuerpo garantiza que es un dominio de integridad.

3.3.4. Observación. *Todo cuerpo es un dominio de integridad.*

Demostración. En un cuerpo, si $x \neq 0$, entonces existe su inverso x^{-1} y multiplicando la identidad $xy = 0$ por x^{-1}, se obtiene

$$x^{-1}(xy) = (x^{-1}x)\, y = 1 \cdot y = y = 0.$$

De la misma manera, $y \neq 0$ implica que $x = 0$. ■

3.3.5. Ejemplo. El anillo conmutativo $\mathbb{Z}/n\mathbb{Z}$ no es un cuerpo en general. Por ejemplo, en $\mathbb{Z}/4\mathbb{Z}$ tenemos divisores de cero

$$[2]_4 \cdot [2]_4 := [2 \cdot 2]_4 = [0]_4,$$

lo que contradice (3.2). El problema es que el elemento $[2]_2$ no es invertible. ▲

3.3.6. Observación. *El anillo $\mathbb{Z}/n\mathbb{Z}$ de los restos módulo n es un cuerpo si y solamente si $n = p$ es primo.*

Demostración. Si n no es primo, es decir, $n = ab$ para algunos $a, b < n$, entonces

$$[a]_n \cdot [b]_n = [0]_n,$$

y por lo tanto $\mathbb{Z}/n\mathbb{Z}$ no es un cuerpo. En general, para un entero a existe b tal que

$$ab \equiv 1 \pmod{n}$$

(inverso módulo n) si y solamente si a es coprimo con n; es decir, $\operatorname{mcd}(a, n) = 1$. De hecho, si $\operatorname{mcd}(a, n) = 1$, entonces tenemos la identidad de Bézout[*]

$$ab + nc = 1 \quad \text{para algunos } b, c \in \mathbb{Z}.$$

Reduciendo esta identidad módulo n, se obtiene $ab \equiv 1 \pmod{n}$. En la otra dirección, supongamos que $ab \equiv 1 \pmod{n}$ para algún b. Entonces, tenemos

$$ab + nc = 1$$

para algún $c \in \mathbb{Z}$. Pero $\operatorname{mcd}(a, n)$ es el mínimo número positivo de la forma $ax + ny$ para $x, y \in \mathbb{Z}$.

En particular, si p es primo, para todo $a \not\equiv 0 \pmod{p}$ existe b tal que $ab \equiv 1 \pmod{p}$. ■

[*] El lector que no se acuerda del mcd y sus propiedades debería consultar el apéndice A.

3.3.7. Digresión. De hecho, existe un cuerpo de 4 elementos, mas es diferente de $\mathbb{Z}/4\mathbb{Z}$. He aquí su tabla de adición y multiplicación:

$+$	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

$\cdot$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

En general, todo cuerpo finito necesariamente tiene orden $q = p^k$ donde $p = 2, 3, 5, 7, 11, \ldots$ es primo y $k = 1, 2, 3, 4, \ldots$ Estos cuerpos se denotan por $\mathbb{F}_{p^k}$. Cuando $k = 1$, es la misma cosa que $\mathbb{Z}/p\mathbb{Z}$, pero para $k > 1$, como hemos notado, $\mathbb{Z}/p^k\mathbb{Z}$ no es un cuerpo, así que $\mathbb{F}_{p^k}$ tiene construcción diferente. Vamos a estudiarlo en la continuación de este curso.

He aquí una aplicación interesante de los cuerpos $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

3.3.8. Observación. *Si p es primo, entonces en el cuerpo $\mathbb{F}_p$ tenemos*

$$(x+y)^p = x^p + y^p$$

para cualesquiera $x, y \in \mathbb{F}_p$

Demostración. El teorema del binomio nos da

$$(x+y)^p = x^p + \binom{p}{1} x^{p-1}y + \binom{p}{2} x^{p-2}y^2 + \cdots + \binom{p}{p-1} xy^{p-1} + y^p.$$

Pero $p \mid \binom{p}{i}$ para $i = 1, \ldots, p-1$ (¡ejercicio!), así que todos los términos de la suma son congruentes a cero módulo p (es decir, son nulos en $\mathbb{F}_p$), excepto x^p e y^p. ■

La aplicación $x \mapsto x^p$ sobre $\mathbb{F}_p$ se conoce como la **aplicación de Frobenius**.

3.3.9. Corolario (Pequeño teorema de Fermat). *: Sea p un número entero. Si a es un número entero tal que $p \nmid a$, entonces*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Demostración. Notemos que en $\mathbb{F}_p$ se cumple

$$x^p = x. \tag{3.3}$$

De hecho, si $x = [0]$ o $x = [1]$, es obvio. Luego, por inducción, si esto se cumple para $x = [a]$, entonces

$$([a+1])^p = ([a] + [1])^p = [a]^p + [1]^p = [a] + [1] = [a+1].$$

Ahora si a es un entero tal que $p \nmid a$, entonces $x = [a]$ es un elemento no nulo en $\mathbb{F}_p$, y por lo tanto es invertible. La identidad (3.3) implica

$$a^{p-1} = a^{-1}a^p = a^{-1}a = 1.$$

Es decir,

$$[a^{p-1}] = [a]^{p-1} = [1] \iff a^{p-1} \equiv 1 \pmod{p}.$$

■

3.4 Anillo de polinomios $R[X]$

3.4.1. Definición. Sea R un anillo conmutativo. Un **polinomio** con coeficientes en R en una variable X es una *suma formal*

$$f = \sum_{i\geq 0} a_i\, X^i,$$

donde $a_i \in R$, y casi todos los a_i son nulos, excepto un número finito de ellos. Esto quiere decir que la suma formal de arriba es finita: $f = \sum_{0\leq i\leq n} a_i\, X^i$ para algún n.

Las sumas de polinomios están definidas por

$$\sum_{i\geq 0} a_i\, X^i + \sum_{i\geq 0} b_i\, X^i := \sum_{i\geq 0} (a_i + b_i)\, X^i \tag{3.4}$$

y los productos por

$$\left(\sum_{i\geq 0} a_i\, X^i\right) \cdot \left(\sum_{i\geq 0} b_i\, X^i\right) := \sum_{k\geq 0} \left(\sum_{i+j=k} a_i b_j\right)\, X^k. \tag{3.5}$$

El cero es el polinomio $0 = \sum_{0\leq i\leq n} a_i\, X^i$ donde todos los coeficientes a_i son nulos y la identidad es el polinomio $1 = \sum_{0\leq i\leq n} a_i\, X^i$ donde $a_0 = 1$ y el resto de los coeficientes son nulos. Ya que R es un anillo conmutativo, de la definición de producto está claro que $f \cdot g = g \cdot f$, y también se puede ver que el producto es asociativo: $f \cdot (g \cdot h) = (f \cdot g) \cdot h$. Todos los polinomios forman un anillo conmutativo que se denota por $R[X]$.

3.4.2. Definición. Para un polinomio $f = \sum_{i\geq 0} a_i\, X^i \in R[X]$ su **grado** es dado por

$$\deg f := \text{máx}\{i \mid a_i \neq 0\}.$$

Para el polinomio nulo, se define

$$\deg 0 := -\infty.$$

Si $f = 0$ o $\deg f = 0$, se dice que f es un **polinomio constante**.

3.4.3. Proposición. *Para cualesquera $f, g \in R[X]$ se tiene*

$$\deg(fg) \leq \deg f + \deg g.$$

Además, si R es un dominio de integridad, entonces

$$\deg(fg) = \deg f + \deg g.$$

Demostración. Para $f = 0$ o $g = 0$ la identidad $\deg(fg) = \deg f + \deg g$ se cumple gracias a nuestra definición del grado del polinomio nulo. Supongamos entonces que f y g no son nulos y que $\deg f = m$, $\deg g = n$,

$$f = \sum_{0\leq i\leq m} a_i\, X^i, \quad g = \sum_{0\leq i\leq n} b_i\, X^i.$$

El coeficiente de X^k en el producto fg es $c_k = \sum_{i+j=k} a_i\, b_j$. Ya que $a_i = 0$ para $i > m$ y $b_j = 0$ para $j > n$, está claro que $c_k = 0$ para $k > n + m$, así que por lo menos se cumple $\deg(fg) \leq \deg f + \deg g$. Para $k = m + n$ tenemos

$$c_{m+n} = a_0\, b_{m+n} + a_1\, b_{m+n-1} + \cdots + a_m\, b_n + \cdots + a_{m+n-1}\, b_1 + a_{m+n}\, b_0 = a_m\, b_n$$

(casi todos los términos en la suma son nulos por la misma razón). Si R es un dominio de integridad, entonces $a_m \neq 0$ y $b_n \neq 0$ implica que $c_{m+n} = a_m\, b_n \neq 0$. Esto demuestra que $\deg(fg) = \deg f + \deg g$. ■

3.4.4. Corolario. *El anillo $R[X]$ es un dominio de integridad si y solamente si R lo es.*

Demostración. Si R es un dominio de integridad, entonces para el producto de dos polinomios tenemos

$$\deg(fg) = \deg f + \deg g.$$

En particular, si $\deg f > -\infty$ y $\deg g > -\infty$, tenemos $\deg(fg) > -\infty$. En otras palabras, $f \neq 0$ y $g \neq 0$ implica $fg \neq 0$.

Viceversa, si $R[X]$ es un dominio de integridad, el anillo R corresponde a los polinomios de grado 0 y por lo tanto es también un dominio de integridad. ■

3.4.5. Comentario. Por nuestra definición, un polinomio es una suma formal $\sum_{i\geq 0} a_i\, X^i$ donde casi todos los coeficientes son nulos. Si permitimos existencia de un número infinito de coeficientes no nulos, estas sumas formales forman un anillo conmutativo respecto a la suma y producto dados por las mismas fórmulas (3.4) y (3.5). Este anillo se llama el **anillo de series formales en** X y se denota por $R[\![X]\!]$. Si R es un dominio de integridad, entonces $R[\![X]\!]$ es también un dominio de integridad. Sin embargo, esto se demuestra de otra manera: la noción de grado no tiene sentido si en $\sum_{i\geq 0} a_i\, X^i$ puede haber coeficientes no nulos de grado arbitrariamente grande. Para los detalles, haga los ejercicios al final de este capítulo.

3.4.6. Definición. Para un polinomio $f = \sum_{0\leq i\leq n} a_i\, X^i \in R[X]$ y un elemento $c \in R$ la **evaluación de f en** c es el elemento

$$f(c) := \sum_{0\leq i\leq n} a_i\, c^i \in R.$$

Si $f(c) = 0$, se dice que c es una **raíz** (o un **cero**) de f.

3.4.7. Proposición. *Sea $f \in R[X]$ un polinomio no nulo con coeficientes en un dominio de integridad R. Entonces f tiene $\leq \deg f$ raíces distintas en R.*

3.4.8. Ejemplo. El polinomio cuadrático $f = X^2 + 1 \in \mathbb{C}[X]$ tiene dos raíces complejas $\pm\sqrt{-1} \in \mathbb{C}$. Si lo consideramos como un polinomio en $\mathbb{R}[X]$, entonces este no tiene raíces.

El polinomio $f = X^2 + 1 \in \mathbb{F}_3[X]$ no tiene raíces en $\mathbb{F}_3$: tenemos

$$f([0]) = [1], \quad f([1]) = [2], \quad f([2]) = [2]^2 + [1] = [2].$$

El polinomio $f = 2\,X^4 - 3\,X^3 + 3\,X^2 - 3\,X + 1 \in \mathbb{Z}[X]$ puede ser escrito como

$$f = 2\,(X-1)\,(X-\sqrt{-1})\,(X+\sqrt{-1})\,(X-1/2).$$

Su única raíz en $\mathbb{Z}$ es 1.

El polinomio $f = 2\,X^2 + 2\,X \in \mathbb{Z}/4\mathbb{Z}$ es cuadrático, pero todo elemento de $\mathbb{Z}/4\mathbb{Z}$ es su raíz:

$$f([0]) = f([1]) = f([2]) = f([3]) = [0].$$

Esto no contradice el enunciado de arriba, ya que $\mathbb{Z}/4\mathbb{Z}$ no es un dominio de integridad. ▲

Para demostrar 3.4.7, necesitamos el siguiente resultado auxiliar.

3.4.9. Lema. *Sea $f \in R[X]$ un polinomio con coeficientes en un anillo conmutativo R. Entonces $f(c) = 0$ para algún $c \in R$ si y solamente si*

$$f = (X - c) \cdot g$$

para algún polinomio $g \in R[X]$.

Demostración (división sintética). En una dirección es obvio: si podemos escribir

$$f = (X - c) \cdot g,$$

entonces la evaluación en c nos da

$$f(c) = (c - c) \cdot g(c) = 0.$$

En la otra dirección, supongamos que $\deg f = n$ y escribamos

$$f = \sum_{0 \le i \le n} a_i \, X^i.$$

Es posible encontrar g de la forma deseada de grado $n - 1$. Escribamos

$$g = \sum_{0 \le i \le n-1} b_i \, X^i,$$

donde b_i son ciertos coeficientes que necesitamos encontrar. Analicemos la identidad

$$f = (X - c) \cdot g + b_{-1},$$

donde $b_{-1} \in R$ es alguna constante. Tenemos

$$\sum_{0 \le i \le n} a_i \, X^i = (X - c) \sum_{0 \le i \le n-1} b_i \, X^i + b_{-1}.$$

Desarrollando la parte derecha, se obtiene

$$\sum_{0 \le i \le n} a_i \, X^i = \sum_{1 \le i \le n} b_{i-1} \, X^i - \sum_{0 \le i \le n-1} c \, b_i \, X^i + b_{-1} = \sum_{0 \le i \le n-1} (b_{i-1} - c \, b_i) \, X^i + b_{n-1} \, X^n.$$

Esto corresponde al siguiente sistema de ecuaciones sobre los b_i:

$$\begin{aligned}
a_n &= b_{n-1}, \\
a_{n-1} &= b_{n-2} - c b_{n-1}, \\
a_{n-2} &= b_{n-3} - c b_{n-2}, \\
&\dots \\
a_1 &= b_0 - c b_1, \\
a_0 &= b_{-1} - c \, b_0
\end{aligned}$$

y nos lleva a las recurrencias

$$\begin{aligned}
b_{n-1} &= a_n, \\
b_{n-2} &= a_{n-1} + c b_{n-1}, \\
b_{n-3} &= a_{n-2} + c b_{n-2}, \\
&\dots \\
b_i &= a_{i+1} + c b_{i+1}, \\
&\dots \\
b_0 &= a_1 + c b_1, \\
b_{-1} &= a_0 + c b_0
\end{aligned}$$

que definen el polinomio g y la constante b_{-1}. Evaluando en $X = c$ ambas partes de la identidad

$$f = (X - c) \cdot g + b_{-1},$$

se obtiene

$$b_{-1} = f(c) = 0.$$

■

3.4.10. Comentario. Las recurrencias de la demostración precedente nos dan un modo eficaz de calcular el valor $f(c)$ para un polinomio $f = \sum_{0 \le i \le n} a_i X^n$: si

$$b_{n-1} = a_n \quad \text{y} \quad b_i = a_{i+1} + c b_{i+1} \text{ para } -1 \le i \le n-1,$$

entonces

$$f(c) = b_{-1}.$$

Esto se conoce como el **algoritmo de Horner**[*]. Note que usando las recurrencias de arriba, $f(c)$ puede ser calculado usando solamente n sumas y n multiplicaciones, lo que es mucho más eficaz que calcular directamente

$$a_0 + a_1 c + a_2 c^2 + \cdots + a_n c^n.$$

Ahora estamos listos para probar 3.4.7.

Demostración de 3.4.7. Inducción sobre $n = \deg f$. Si $n = 0$, entonces f, siendo un polinomio constante no nulo, no tiene raíces. Para el paso inductivo, notamos que si $c \in R$ es una raíz de f, entonces

$$f = (X - c)\, g$$

para algún polinomio $g \in R[X]$. Luego,

$$\deg f = \deg(X - c) \cdot \deg g$$

(aquí se usa la hipótesis que R es un dominio de integridad), así que $\deg g = n - 1$ y por la hipótesis de inducción sabemos que g tiene $\le n - 1$ raíces. Toda raíz de g es una raíz de f, y si $c' \neq c$ es una raíz de f, entonces la identidad en R

$$0 = f(c') = (c - c') \cdot g(c')$$

implica que $g(c') = 0$ y c' es una raíz de g (de nuevo, se usa la hipótesis que R es un dominio de integridad). Podemos concluir que f tiene $\le n$ diferentes raíces. ■

3.4.11. Comentario. A veces hay cierta confusión entre los polinomios y funciones polinomiales. Para cualquier polinomio $f \in R[X]$ la evaluación define una función

$$\begin{aligned} R &\to R, \\ c &\mapsto f(c). \end{aligned}$$

Sin embargo, no siempre existe una correspondencia biyectiva entre las aplicaciones que surgen de esta manera y los elementos de $R[X]$. Por ejemplo, para $R = \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ hay solamente p^p diferentes aplicaciones $\mathbb{F}_p \to \mathbb{F}_p$, mientras que el anillo $\mathbb{F}_p[X]$ es infinito: sus elementos son las expresiones formales $\sum_{0 \le i \le n} a_i X^i$ con $a_i \in \mathbb{F}_p$.

Para dar un ejemplo específico: el polinomio $X^p - X \in \mathbb{F}_p[X]$ evaluado en cualquier elemento de $\mathbb{F}_p$ nos da 0, gracias al pequeño teorema de Fermat que acabamos de revisar arriba, mientras que $X^p - X$ no es nulo como un elemento de $\mathbb{F}_p[X]$ (es decir, como una *expresión formal*).

[*] William George Horner (1786–1837), matemático inglés.

3.5 ¿Para qué sirven los anillos?

Hay mucho más ejemplos importantes de anillos conmutativos y cuerpos, pero no es el tema principal de nuestro curso, así que por el momento es todo. Los anillos conmutativos tienen mucha importancia en las matemáticas modernas. En muchas situaciones hay una correspondencia

$$\text{Objetos geométricos (“espacios”)} \longleftrightarrow \text{Objetos algebraicos hechos de anillos conmutativos.}$$

A veces para solucionar problemas geométricos, se puede pasar a los objetos algebraicos correspondientes. Por otro lado, hay muchos objetos algebraicos que surgen naturalmente en la teoría de números; un ejemplo básico son los anillos como $\mathbb{Z}$, $\mathbb{Z}[\sqrt{-1}]$, $\mathbb{Z}[\sqrt{2}]$ que hemos visto arriba. A tales objetos se puede asociar ciertos “espacios” y aplicar la intuición geométrica para resolver problemas aritméticos. Es uno de los temas principales de las matemáticas a partir de los años 50-60 del siglo pasado. Preguntar a un matemático moderno si él prefiere trabajar con objetos algebraicos o usar la intuición geométrica es como preguntarse si uno prefiere quedarse ciego o sordo.

Los cuerpos son un caso muy especial de anillos, y de hecho, bajo la correspondencia geométrica-algebraica que mencioné, a un cuerpo corresponde un espacio que consiste solo de un punto. Los anillos $\mathbb{Z}$, $\mathbb{Z}[\sqrt{-1}]$, $\mathbb{Z}[\sqrt{2}]$ son también bastante sencillos: si los cuerpos tienen dimensión 0, estos tienen dimensión 1. Hay anillos de dimensiones superiores, por ejemplo si consideramos el anillo de polinomios $R[X]$, la dimensión sube por 1:

$$\dim R[X] = \dim R + 1.$$

En particular, la dimensión de $k[X]$ para un cuerpo k es igual a 1. También hay anillos de dimensión infinita, pero no los vamos a encontrar en este curso.

3.6 Espacios vectoriales

Para terminar, recordemos la definición de espacios vectoriales que el lector probablemente conoce de cursos de álgebra lineal.

3.6.1. Definición. Sea k un cuerpo. Un **espacio vectorial** es un conjunto V dotado de dos operaciones

$$\begin{aligned} +\colon V \times V &\to V, \\ (u, v) &\mapsto u + v; \\ \cdot\colon k \times V &\to V, \\ (a, u) &\mapsto a \cdot u. \end{aligned}$$

Los elementos de V se llaman **vectores** mientras que los elementos de k se llaman **escalares**. La operación $+$ se llama la **adición** de vectores y la operación $\cdot$ se llama la **acción** de los escalares sobre los vectores. Se pide que se cumplan los siguientes axiomas.

V1) V es un grupo abeliano respecto a la operación $+$; es decir, la adición es asociativa:

$$(u + v) + w = u + (v + w) \quad \text{para cualesquiera } u, v, w \in V,$$

existe el elemento neutro (**vector nulo**) $0 \in V$ tal que

$$0 + u = u + 0 = u \quad \text{para todo } u \in V,$$

para todo vector $u \in V$ existe el **vector opuesto** $-u$ tal que

$$u + (-u) = (-u) + u = 0 \quad \text{para todo } u \in V,$$

y la adición es conmutativa:

$$u + v = v + u \quad \text{para cualesquiera } u, v \in V.$$

V2) La multiplicación por escalares es bilineal: se cumple

$$(a + b) \cdot u = a \cdot u + b \cdot u \quad \text{para cualesquiera } a, b \in k,\ u \in V$$

y

$$a \cdot (u + v) = a \cdot u + a \cdot v \quad \text{para todo } a \in k,\ u, v \in V.$$

V3) La multiplicación por escalares es compatible con la multiplicación en k:

$$(ab) \cdot u = a \cdot (b \cdot u) \quad \text{para cualesquiera } a, b \in k,\ u \in V.$$

V4) La multiplicación por la identidad de k es la indentidad:

$$1 \cdot u = u \quad \text{para todo } u \in V.$$

Muchas propiedades habituales siguen de V1)–V4):

1) $a \cdot 0 = 0$ para todo $a \in k$,
2) $0 \cdot u = 0$ para todo $u \in V$,
3) $(-1) \cdot u = -u$ para todo $u \in V$,
4) $a \cdot (-u) = -(a \cdot u)$ para todo $a \in k$, $u \in V$,
5) $a \cdot (u - v) = a \cdot u - a \cdot v$ para todo $a \in k$, $u, v \in V$,
6) $(a - b) \cdot u = a \cdot u - b \cdot u$ para cualesquiera $a, b \in k$, $u \in V$.

3.6.2. Ejemplo. Si k es un cuerpo y $n = 0, 1, 2, 3, \ldots$ es un número natural fijo, entonces el conjunto

$$k^n := \underbrace{k \times \cdots \times k}_{n} = \{(a_1, \ldots, a_n) \mid a_i \in k\}$$

respecto a las operaciones

$$(a_1, \ldots, a_n) + (b_1, \ldots, b_n) := (a_1 + b_1, \ldots, a_n + b_n)$$

y

$$a \cdot (a_1, \ldots, a_n) := (aa_1, \ldots, aa_n)$$

forma un espacio vectorial. El vector nulo es dado por $0 = (0, \ldots, 0)$ y los vectores opuestos son $-(a_1, \ldots, a_n) = (-a_1, \ldots, -a_n)$.

Para $n = 0$ tenemos $k^0 := \{0\}$ que se llama el **espacio vectorial nulo**. ▲

El lector debe conocer bien los espacios como $\mathbb{R}^n$ y $\mathbb{C}^n$. En geometría y análisis a veces se usan estructuras extra sobre estos espacios como una métrica, la topología asociada, productos interiores, etc. Todo esto no hace parte de la definición abstracta de espacios vectoriales. Sin embargo, muchos resultados básicos que se estudian en un curso introductivo de álgebra lineal siguen de los axiomas V1)–V4).

3.6.3. Definición. Una **base** de un espacio vectorial V es una familia de vectores $(u_i)_{i\in I}$ tal que todo vector $u \in V$ puede ser escrito como una combinación lineal de los u_i:

$$u = \sum_{i\in I} a_i \cdot u_i,$$

donde $a_i = 0$ para todo i, excepto un número finito. Además, se pide que los u_i sean linealmente independientes; es decir,

$$\text{si } \sum_{i\in I} a_i \cdot u_i = 0, \text{ entonces } a_i = 0 \text{ para todo } i \in I.$$

3.6.4. Ejemplo. El espacio k^n viene con una base canónica dada por

$$e_1 := (1,0,0,\ldots,0), \quad e_2 := (0,1,0,\ldots,0), \quad \ldots, \quad e_n = (0,0,0,\ldots,1).$$

▲

Recordemos que todo espacio vectorial V posee una base y todas las bases tienen la misma cardinalidad que es la **dimensión** de V. La existencia de base en cualquier espacio vectorial se demuestra mediante el lema de Zorn.

3.6.5. Ejemplo. $\mathbb{R}$ es un espacio vectorial sobre $\mathbb{Q}$ y por lo tanto posee una base sobre $\mathbb{Q}$. Es decir, existe una familia de números reales linealmente independientes sobre $\mathbb{Q}$ tal que todo número $x \in \mathbb{R}$ es una combinación lineal de ellos. Esta base se conoce como la **base de Hamel**. Es infinita y no es explícita; su existencia puede ser justificada por el lema de Zorn. ▲

3.7 Ejercicios

Ejercicio 3.1. *Sea p un número primo. Demuestre que los coeficientes binomiales $\binom{p}{i}$ son divisibles por p para $i = 1, \ldots, p-1$.*

Ejercicio 3.2. *Para $n = 2, 3, 4, 5, \ldots$ consideremos la raíz de la unidad $\zeta_n := e^{2\pi i/n} \in \mathbb{C}$.*

1) *Demuestre la identidad $1 + \zeta_n + \zeta_n^2 + \cdots + \zeta_n^{n-1} = 0$.*

2) *Consideremos el conjunto*

$$\mathbb{Z}[\zeta_n] := \{a_0 + a_1\,\zeta_n + a_2\,\zeta_n^2 + \cdots + a_{n-1}\,\zeta_n^{n-1} \mid a_i \in \mathbb{Z}\}.$$

Demuestre que es un anillo conmutativo respecto a la suma y adición habitual de los números complejos.

Ejercicio 3.3. *Deduzca de los axiomas de anillos las siguientes propiedades:*

$$0 \cdot x = x \cdot 0 = 0, \quad x \cdot (-y) = (-x) \cdot y = -xy, \quad x\,(y - z) = xy - xz, \quad (x - y)\,z = xz - yz$$

para cualesquiera $x, y, z \in R$.

Ejercicio 3.4. *En un anillo R puede ser que $0 = 1$. Pero en este caso R tiene solo un elemento.*

1) *Demuestre que un conjunto $R = \{0\}$ que consiste en un elemento puede ser dotado de modo único de una estructura de un anillo conmutativo. Este anillo se llama el **anillo nulo**.*

2) *Demuestre que si en un anillo R se cumple $1 = 0$, entonces $R = \{0\}$.*

Ejercicio 3.5. *Para un número fijo $n = 1, 2, 3, \ldots$ consideremos el conjunto de fracciones con n en el denominador:*

$$\mathbb{Z}[1/n] := \left\{ \frac{m}{n^k} \;\middle|\; m \in \mathbb{Z},\ k = 0, 1, 2, 3, \ldots \right\} \subset \mathbb{Q}.$$

De modo similar, para un número primo fijo $p = 2, 3, 5, 7, 11, \ldots$ consideremos las fracciones con denominador no divisible por p:

$$\mathbb{Z}_{(p)} := \left\{ \frac{a}{b} \;\middle|\; a, b \in \mathbb{Z},\ b \neq 0,\ p \nmid b \right\} \subset \mathbb{Q}.$$

Verifique que $\mathbb{Z}[1/n]$ y $\mathbb{Z}_{(p)}$ son anillos conmutativos respecto a la suma y producto habituales.

Ejercicio 3.6. *Sea R un anillo conmutativo. Una **serie formal de potencias** con coeficientes en R en una variable X es una suma formal*

$$f = \sum_{i \geq 0} a_i\, X^i,$$

donde $a_i \in R$. A diferencia de polinomios, se puede tener un número infinito de coeficientes no nulos. Las sumas y productos de series formales están definidos por

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

1) *Note que las series formales forman un anillo conmutativo. Este se denota por $R[\![X]\!]$.*

2) *Verifique la identidad*

$$(1 + X) \cdot (1 - X + X^2 - X^3 + X^4 - X^5 + \cdots) = 1$$

en $R[\![X]\!]$ (es decir, los coeficientes de la serie formal al lado derecho son $a_0 = 1$ y $a_i = 0$ para $i > 0$).

3) *Para $R = \mathbb{Q}$ verifique la identidad* $\left(\sum_{i\geq 0} \frac{X^i}{i!}\right)^n = \sum_{i\geq 0} \frac{n^i}{i!} X^i$ *en el anillo de series formales* $\mathbb{Q}[\![X]\!]$.

Ejercicio 3.7. *Para una serie de potencias $f \in R[\![X]\!]$ sea $v(f)$ el mínimo índice tal que el coeficiente correspondiente no es nulo:*

$$v(f) := \min\{i \mid a_i \neq 0\};$$

y si $f = 0$, pongamos $v(0) := +\infty$.

1) *Demuestre que para cualesquiera $f, g \in R[\![X]\!]$ se cumple la desigualdad*

$$v(fg) \geq v(f) + v(g)$$

y la igualdad $v(fg) = v(f) + v(g)$ si R es un dominio de integridad.

2) *Demuestre que $R[\![X]\!]$ es un dominio de integridad si y solamente si R lo es.*

Ejercicio 3.8. *Sea R un anillo conmutativo. En el anillo de matrices $M_n(R)$ denotemos por e_{ij} para $1 \leq i, j \leq n$ la matriz cuyos coeficientes son nulos, salvo el coeficiente (i, j) que es igual a 1. Sea $A \in M_n(R)$ una matriz arbitraria de $n \times n$ con coeficientes en R.*

1) *Demuestre que en el producto de matrices $e_{ij}\, A$ la fila i es igual a la fila j de A y el resto de los coeficientes son nulos.*

2) *Demuestre que en el producto de matrices $A\, e_{ij}$ la columna j es igual a la columna i de A y el resto de los coeficientes son nulos.*

3) *Demuestre que*

$$e_{ij}\, A = A\, e_{ij}$$

*para todo $1 \leq i, j \leq n$, $i \neq j$ si y solamente si A es una **matriz escalar**:*

$$A = aI = \begin{pmatrix} a & & & \\ & a & & \\ & & \ddots & \\ & & & a \end{pmatrix}$$

para algún $a \in R$.

4) *Concluya que las únicas matrices en $M_n(R)$ que conmutan con todas las matrices son las matrices escalares.*