Capítulo 1
Anillos

En este capitulo primero vamos a revisar rápidamente los números complejos y luego introduciremos las nociones abstractas de anillo y cuerpo y veremos los primeros ejemplos y propiedades básicas.

1.1 Números complejos

En el capítulo anterior hemos recordado la construcción de los números racionales $\mathbb{Q}$ a partir de los números enteros $\mathbb{Z}$ y también la construcción de los números reales $\mathbb{R}$ a partir de $\mathbb{Q}$. Ahora vamos a revisar la construcción de los números complejos $\mathbb{C}$ a partir de $\mathbb{R}$. Se supone que este material es familiar al lector, así que voy a omitir algunos detalles.

Los **números complejos** pueden ser identificados con las **expresiones formales**

$$z = x + y\,i,$$

donde $x, y \in \mathbb{R}$. Las palabras "expresión formal" significan que

$$x_1 + y_1\,i = x_2 + y_2\,i \text{ si y solamente si } x_1 = x_2 \text{ e } y_1 = y_2.$$

El número x se llama la **parte real** e y se llama la **parte imaginaria** de z. Se usa la notación

$$\operatorname{Re} z := x, \quad \operatorname{Im} z := y.$$

El conjunto de los números complejos se denota por $\mathbb{C}$. El **plano complejo** es la identificación entre $\mathbb{C}$ y $\mathbb{R}^2$ dada por $z \leftrightarrow (\operatorname{Re} z, \operatorname{Im} z)$.

Las sumas están definidas **término por término**; es decir,

$$(x_1 + y_1\,i) + (x_2 + y_2\,i) := (x_1 + x_2) + (y_1 + y_2)\,i,$$

y los productos se definen mediante la multiplicación de los números reales, la identidad

$$i^2 = -1$$

y la **distibutividad**; es decir,

$$(x_1 + y_1\,i) \cdot (x_2 + y_2\,i) := (x_1 x_2 - y_1 y_2) + (x_1 y_2 + x_2 y_1)\,i.$$

Notamos que para qualesquiera $x_1, x_2 \in \mathbb{R}$ se tiene

$$(x_1 + 0 \cdot i) + (x_2 + 0 \cdot i) = (x_1 + x_2) + 0 \cdot i,$$
$$(x_1 + 0 \cdot i) \cdot (x_2 + 0 \cdot i) = x_1 x_2 + 0 \cdot i,$$

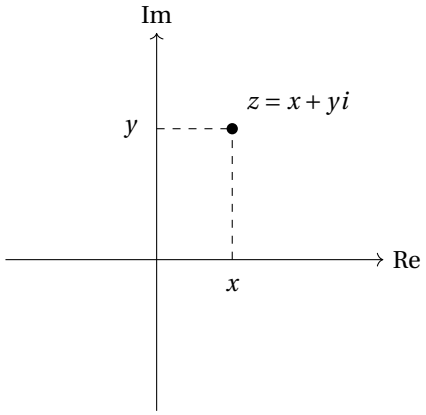

Figura 1.1: El plano complejo

y en este sentido la multiplicación compleja es una generalización de la multiplicación de números reales. Los números reales se identifican con el subconjunto formado por los números de la forma $x + 0 \cdot i$, que también se denotan por x.

1.1.1. Observación. *Las sumas y productos cumplen las siguientes propiedades.*

1) *a)* $(z_1 + z_2) + z_3 = z_1 + (z_2 + z_3)$ *para cualesquiera* $z_1, z_2, z_3 \in \mathbb{C}$.

b) El número $0 := 0 + i \cdot 0$ *cumple*

$$z + 0 = 0 + z = z$$

para todo $z \in \mathbb{C}$.

c) $z + (-z) = (-z) + z = 0$ *para todo* $z = x + iy \in \mathbb{C}$*, donde* $-z := -x - iy$.

d) $z + w = w + z$ *para cualesquiera* $z, w \in \mathbb{C}$.

2) El producto es distributivo respecto a la suma:

$$z(w_1 + w_1) = zw_1 + zw_2, \quad (z_1 + z_2)w = z_1 w + z_2 w$$

para cualesquiera $z, w_1, w_2 \in \mathbb{C}$.

3) El producto es asociativo:

$$(z_1 z_2)z_3 = z_1(z_2 z_3)$$

para cualesquiera $z_1, z_2, z_3 \in \mathbb{C}$.

4) El número $1 := 1 + i \cdot 0$ *cumple*

$$z \cdot 1 = 1 \cdot z = z$$

para todo $z \in \mathbb{C}$.

5) El producto es conmutativo:

$$zw = wz$$

para cualesquiera $z, w \in \mathbb{C}$. □

Para un número complejo $z = x + iy$ su **conjugado** se define mediante

$$\overline{z} := x - iy.$$

1.1.2. Observación. *La conjugación cumple las siguientes propiedades:*

1) $\overline{z+w} = \overline{z} + \overline{w}$ *y* $\overline{zw} = \overline{z} \cdot \overline{w}$ *para cualesquiera* $z, w \in \mathbb{C}$.

2) $\overline{\overline{z}} = z$ *para todo* $z \in \mathbb{C}$.

3) $\overline{z} = z$ *si y solo si* $z \in \mathbb{R}$. □

1.1.3. Definición. El **valor absoluto** de $z = x + yi \in \mathbb{C}$ es el número real

$$|z| := \sqrt{z\overline{z}} = \sqrt{x^2 + y^2}.$$

Notamos que $|z| \geq 0$ y $|\overline{z}| = |z|$.

1.1.4. Observación. *El valor absoluto satisface las propiedades habituales:*

1) $|z| = 0$ *si y solamente si* $z = 0$*;*

2) $|zw| = |z| \cdot |w|$ *para cualesquiera* $z, w \in \mathbb{C}$*;*

3) se cumple la ***desigualdad triangular***

$$\Big||z| - |w|\Big| \leq |z + w| \leq |z| + |w|$$

para cualesquiera $z, w \in \mathbb{C}$. □

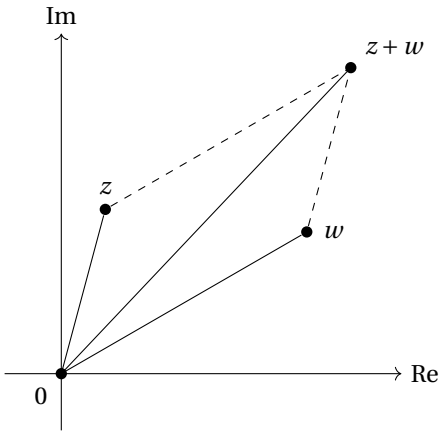

Figura 1.2: La desigualdad triangular

1.1.5. Observación. *Para todo número complejo* $z = x + yi \neq 0$ *existe un número único* $z^{-1} \in \mathbb{C}$ *tal que*

$$zz^{-1} = z^{-1}z = 1.$$

Demostración. Dado que $z\overline{z} = |z|^2$, se ve que hay que tomar

$$z^{-1} = \frac{1}{|z|^2}\,\overline{z} = \frac{x}{x^2 + y^2} - \frac{y}{x^2 + y^2}\,i.$$

Este número es único porque si hay dos $w_1, w_2 \in \mathbb{C}$ tales que $zw_1 = zw_2 = 1$, entonces

$$w_1 = w_1 \cdot 1 = w_1\,(zw_2) = (w_1 z)\,w_2 = 1 \cdot w_2 = w_2.$$ ■

1.1.6. Observación. *Para cualesquiera $z, w \in \mathbb{C}$, si se cumple $zw = 0$, entonces $z = 0$ o $w = 0$.*

Demostración. Si $zw = 0$, entonces, tomando los valores absolutos, se obtiene $|z| \cdot |w| = 0$, así que $|z| = 0$ (es decir, $z = 0$) o $|w| = 0$ (es decir, $w = 0$).

Otra prueba, usando los inversos: si tenemos $zw = 0$ y $z \neq 0$, entonces

$$w = 1 \cdot w = z^{-1} z w = z^{-1} 0 = 0.$$ ■

Usando las **coordenadas polares** en $\mathbb{R}^2$, podemos expresar cada número complejo como

$$z = r\,(\cos\phi + i \operatorname{sen}\phi), \quad \text{donde } r = |z|,\ 0 \leq \phi < 2\pi.$$

Si $z \neq 0$, entonces los números r y ϕ están definidos de modo único. La expresión de arriba se llama la **forma trigonométrica** (o **polar**) de z.

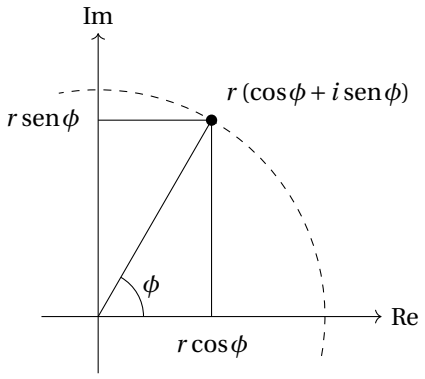

Figura 1.3: La fórma trigonométrica de números complejos

1.1.7. Proposición (La identidad de Euler[*]). *Para cualquier ϕ se tiene*

$$\cos\phi + i \operatorname{sen}\phi = e^{i\phi}.$$

Demostración. El coseno, seno y la exponencial pueden ser definidos mediante las series de potencias

$$\cos z = \sum_{n\geq 0} (-1)^n \frac{z^{2n}}{(2n)!} = 1 - \frac{z^2}{2} + \frac{z^4}{24} - \frac{z^6}{720} + \cdots,$$
$$\operatorname{sen} z = \sum_{n\geq 0} (-1)^n \frac{z^{2n+1}}{(2n+1)!} = z - \frac{z^3}{6} + \frac{z^5}{120} - \cdots,$$
$$e^z = \sum_{n\geq 0} \frac{z^n}{n!} = 1 + z + \frac{z^2}{2} + \frac{z^3}{6} + \frac{z^4}{24} + \frac{z^5}{120} + \frac{z^6}{720} + \cdots$$

—es fácil recordarlas: basta memorizar la serie de e^z, y luego $\cos z$ y $\operatorname{sen} z$ tienen series parecidas, pero alternantes; siendo una función par, $\cos z$ consiste en términos pares, y siendo una función impar, $\operatorname{sen} z$ consiste en términos pares. Calculamos que las potencias de i son

$$i^{2n} = (-1)^n, \quad i^{2n+1} = (-1)^n i.$$

Luego,

$$e^{i\phi} = \sum_{n\geq 0} \frac{(i\phi)^n}{n!} = \sum_{n\geq 0} \frac{i^n \phi^n}{n!} = \sum_{n\geq 0} (-1)^n \frac{\phi^{2n}}{(2n)!} + i \sum_{n\geq 0} (-1)^n \frac{\phi^{2n+1}}{(2n+1)!} = \cos\phi + i \operatorname{sen}\phi.$$ ■

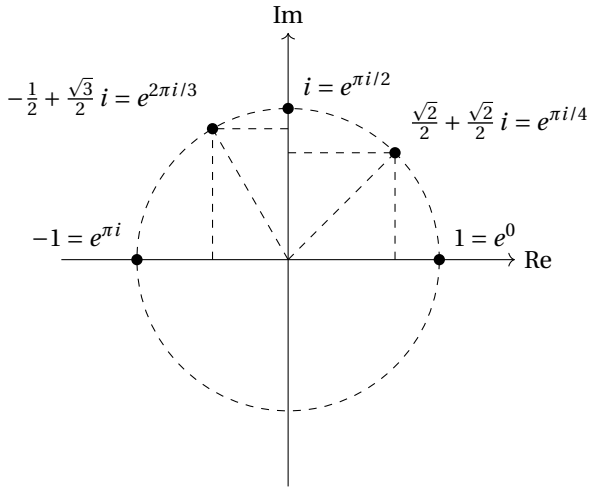

Figura 1.4: Algunos números en el plano complejo

La identidad de Euler implica que todo número complejo es de la forma $r\,e^{i\phi}$ para algún número real $r \geq 0$ y ángulo $0 \leq \phi < 2\pi$.

1.1.8. Corolario (La fórmula de de Moivre[*]). *Para $n = 1,2,3,\ldots$ se tiene*

$$(\cos\phi + i\,\mathrm{sen}\,\phi)^n = \cos(n\phi) + i\,\mathrm{sen}(n\phi).$$

Demostración. Usando la identidad de Euler,

$$(\cos\phi + i\,\mathrm{sen}\,\phi)^n = (e^{i\phi})^n = e^{in\phi} = \cos(n\phi) + i\,\mathrm{sen}(n\phi). \qquad \blacksquare$$

1.1.9. Proposición. *Para $n = 1,2,3,4,\ldots$ la ecuación*

$$z^n = 1$$

tiene precisamente n distintas raíces complejas: son

$$e^{\frac{2\pi i k}{n}}, \quad \textit{donde } k = 0,1,\ldots,n-1.$$

Demostración. Si $z^n = 1$, entonces $|z|^n = |z^n| = 1$, de donde se sigue que $|z| = 1$, así que z es de la forma

$$z = e^{i\phi} = \cos\phi + i\,\mathrm{sen}\,\phi$$

para algún ángulo $0 \leq \phi < 2\pi$. Según la fórmula de de Moivre tenemos

$$z^n = \cos(n\phi) + i\,\mathrm{sen}(n\phi) = 1,$$

así que

$$\cos(n\phi) = 1 \text{ y } \mathrm{sen}(n\phi) = 0,$$

lo que significa que

$$n\phi = 2\pi k.$$

para algún $k \in \mathbb{Z}$. Entonces,

$$\phi = \frac{2\pi k}{n}.$$

Esto nos da n diferentes ángulos que corresponden a $k = 0,1,2,\ldots,n-1$. $\blacksquare$

[*] Leonhard Euler (1707–1783) — matemático suizo, uno de los más prolíficos e importantes de toda la historia.
[*] Abraham de Moivre (1667–1754), matemático francés.

1.1.10. Definición. Los números complejos $z \in \mathbb{C}$ que cumplen $z^n = 1$ se laman las **raíces n-ésimas de la unidad**. Como acabamos de ver, son

$$1,\ \zeta_n,\ \zeta_n^2,\ \ldots,\ \zeta_n^{n-1},$$

donde

$$\zeta_n := e^{\frac{2\pi i}{n}}. \tag{1.1}$$

La notación (1.1) será utilizada muy a menudo a lo largo del curso, así que hay que recordarla. Observamos que de la misma manera, para cualquier número complejo w, las raíces de la ecuación $z^n = w$ son de la forma $\zeta_n^k \sqrt[n]{|w|}$.

Notamos que el polígono en el plano complejo que tiene como sus vértices las raíces n-ésimas de la unidad ζ_n^k es un n-ágono regular inscrito en el circulo unitario.

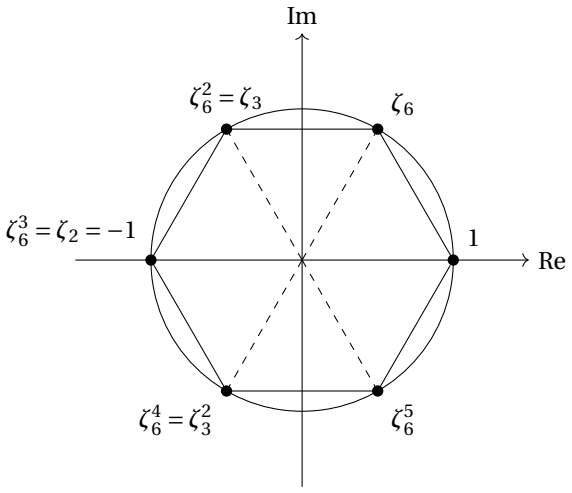

Figura 1.5: Las raíces sextas de la unidad en el plano complejo

Notamos un par de propiedades.

1) Si $m \mid n$, entonces toda raíz m-ésima es una raíz n-ésima.
   Esto se ve de la identidad $z^n = (z^m)^{n/m}$ o también de $\zeta_m = \zeta_n^{n/m}$.

2) Para cualquier $n \geq 2$ la suma de todas las raíces n-ésimas es nula:

$$1 + \zeta_n + \zeta_n^2 + \cdots + \zeta_n^{n-1} = \frac{\zeta_n^n - 1}{\zeta_n - 1} = 0$$

   —aquí hemos usado la fórmula para la serie geométrica y el hecho de que $\zeta_n \neq 1$.

1.2 Axiomas de anillos

Hasta el momento hemos revisado las construcciones de los números racionales $\mathbb{Q}$, reales $\mathbb{R}$ y complejos $\mathbb{C}$. Cada uno de estos conjuntos está formado por ciertos elementos, sobre cuáles están definidas la suma y producto que cumplen las propiedades habituales enumeradas en 1.1.1. De la misma manera, sobre el conjunto $\mathbb{Z}/n\mathbb{Z}$ de los restos módulo n están definidas las dos operaciones aritméticas. Para generalizar y axiomatizar todos estos "conjuntos de números", se introduce la noción de **anillo**.

1.2.1. Definición. Un **anillo** A es un conjunto dotado de dos operaciones: **adición**

$$\begin{aligned} +\colon A \times A &\to A, \\ (x, y) &\mapsto x + y \end{aligned}$$

y **multiplicación**

$$\begin{aligned} \cdot\colon A \times A &\to A, \\ (x, y) &\mapsto xy \end{aligned}$$

que satisfacen los siguientes axiomas.

A1a) la adición es **asociativa**: para cualesquiera $x, y, z \in A$ tenemos

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

A1b) existe un elemento $0 \in A$ (el **cero**) tal que para todo $x \in A$ se cumple

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

A1c) para todo $x \in A$ existe un elemento $-x \in A$ (el **opuesto** de x) que satisface

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

A1d) la adición es **conmutativa**: para cualesquiera $x, y \in A$ se cumple

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

A2) la multiplicación es **distributiva** respecto a la adición: para cualesquiera $x, y, z \in A$ se cumple

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

A3) la multiplicación es **asociativa**: para cualesquiera $x, y, z \in A$ tenemos

$$(xy)z = x(yz);$$

A4) existe un elemento $1 \in A$ (la **identidad**) tal que para todo $x \in A$ se cumple

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

Además, si se cumple el axioma adicional

AC) la multiplicación es **conmutativa**: para cualesquiera $x, y \in A$ se cumple

$$xy = yx.$$

se dice que A es un **anillo conmutativo**.

1.3 Ejemplos de anillos

1.3.1. Ejemplo. Al revisar los axiomas, no debe ser sorprendente que los números enteros $\mathbb{Z}$, racionales $\mathbb{Q}$, reales $\mathbb{R}$, complejos $\mathbb{C}$ formen anillos conmutativos respecto a la adición y multiplicación habitual. ▲

1.3.2. 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

$$[a]_n + [b]_n := [a+b]_n,$$
$$[a]_n \cdot [b]_n := [ab]_n.$$

Se ve que $\mathbb{Z}/n\mathbb{Z}$ es un anillo conmutativo respecto a la adición y multiplicación módulo n, dado que $\mathbb{Z}$ lo es. Los restos $[0]_n$ y $[1]_n$ son el cero y la identidad respectivamente. Los elementos opuestos son dados por $-[a]_n = [-a]_n$. ▲

Un ejemplo extremadamente importante son los anillos de polinomios.

1.3.3. Ejemplo (Anillos de polinomios). Sea A un anillo. Un **polinomio** con coeficientes en A en una variable X es una **suma formal**

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

donde $a_i \in A$, 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: para algún n tenemos

$$f = \sum_{0 \leq i \leq n} a_i X^i = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0. \tag{1.2}$$

La palabra "suma formal" significa que $\sum_{i\geq 0} a_i X^i = \sum_{i \geq 0} b_i X^i$ si y solo si $a_i = b_i$ para todo $i \geq 0$. Para denotar las variables de polinomios, serán usadas las letras mayúsculas $X, Y, Z, \ldots$ Los términos de la forma $0 \cdot X^i$ normalmente se omiten de las expresiones como (1.2).

Las sumas de polinomios están definidas término por término:

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

Para definir los productos, basta declarar que los monomios se multiplican como

$$a_i X^i \cdot b_j X^j = a_i b_j X^{i+j},$$

y aplicar la distributividad:

$$\begin{aligned}\left(a_m X^m + a_{m-1} X^{m-1} + \cdots + a_1 X + a_0\right)&\left(b_n X^n + b_{n-1} X^{n-1} + \cdots + b_1 X + b_0\right) \\ &= a_m b_n X^{m+n} + (a_m b_{n-1} + a_{m-1} b_n) X^{m+n-1} + \cdots + (a_1 b_0 + a_0 b_1) X + a_0 b_0.\end{aligned}$$

Esto nos lleva a la fórmula

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

Dejo al lector verificar que los polinomios forman un anillo respecto a estas operaciones. Este anillo se denotará por $A[X]$. Notamos que si A es conmutativo, entonces $A[X]$ es también conmutativo (este es el caso

que nos va a interesar a continuación). Tal vez la parte menos evidente es la asociatividad de multiplicación. Para probarla, se puede observar que si

$$f = \sum_{i\geq 0} a_i X^i, \quad g = \sum_{j\geq 0} b_j X^j, \quad h = \sum_{k\geq 0} c_k X^k,$$

entonces ambas expresiones $f\,(g\,h)$ y $(f\,g)\,h$ son iguales a

$$\sum_{n\geq 0}\left(\sum_{i+j+k=n} a_i b_j c_k\right) X^n.$$

Un polinomio de la forma

$$c + 0\cdot X + 0\cdot X^2 + 0\cdot X^3 + \cdots$$

se llama un **polinomio constante** y también se denota por c. El cero en $A[X]$ es el polinomio constante 0 y la identidad es el polinomio constante 1.

Si seguimos la misma construcción, pero quitamos la condición de que $a_i = 0$, excepto un número finito de i, entonces se obtiene el **anillo de las series formales** que se denota por $A[[X]]$. Véase el ejercicio 1.9. ▲

Vamos a volver a los polinomios en el siguiente capítulo para sistematizar sus propiedades.

1.3.4. Ejemplo (Anillos de funciones). Sea X un conjunto y A un anillo. Las aplicaciones $f\colon X \to A$ forman un anillo respecto a la suma y producto **punto por punto**:

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

Los axiomas de anillos se deducen de estos axiomas para A. El cero es la aplicación constante $x \mapsto 0$ y la identidad es la aplicación constante $x \mapsto 1$. Este anillo se llama el **anillo de funciones sobre** X con valores en A y se denotará por $\mathrm{Fun}(X, A)$. Si A es un anillo conmutativo, entonces el anilo $\mathrm{Fun}(X, A)$ es también conmutativo.

Los anillos de funciones tienen mucha importancia en la geometría moderna, donde X es algún espacio geométrico y la idea principal es reconstruir X a partir de las funciones sobre X. ▲

Mencionemos un ejemplo importante de anillos no conmutativos que seguramente es familiar al lector.

1.3.5. Ejemplo (Anillos de matrices). Para un anillo A, una **matriz de** $n\times n$ **con coeficientes en** A es una tabla

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

donde $a_{ij} \in A$. En este curso vamos a denotar las matrices nada más por las letras minúsculas $a, b, c, \ldots$ La suma de matrices se define término por término:

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

mientras que el producto

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

se define mediante la fórmula

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

Este producto no es algo aleatorio: su definición viene de la composición de aplicaciones lineales.

Las matrices de $n \times n$ con coeficientes en A forman un anillo que vamos a denotar por $M_n(A)$. 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 la identidad es la matriz

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

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

El anillo $M_n(A)$ no es conmutativo para $n \ge 2$: por ejemplo, para $n = 2$ podemos considerar las matrices

$$e_{11} := \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad e_{12} := \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

Calculamos que

$$e_{11}\, e_{12} = e_{12}, \quad e_{12}\, e_{11} = 0,$$

y luego $e_{11}\, e_{12} \neq e_{12}\, e_{11}$, salvo el caso trivial cuando en A se cumple $1 = 0$. ▲

No olvidemos que las matrices sirven nada más para especificar las aplicaciones lineales $V \to V$ respecto a una base fija de V. Sin fijar una base, podemos definir de manera abstracta el anillo de aplicaciones lineales.

1.3.6. Ejemplo. Para un espacio vectorial V, sea $\mathrm{End}(V)$ el conjunto de las aplicaciones lineales $f\colon V \to V$. Definamos la suma mediante

$$(f + g)(v) := f(v) + g(v)$$

y el producto mediante la composición de aplicaciones $f \circ g$. Esto nos da una estructura de anillo no conmutativo sobre $\mathrm{End}(V)$ que se llama el **anillo de endomorfismos** de V. ▲

1.3.7. Ejemplo. Una manera común de construir nuevos anillos es tomar productos. A saber, para dos anillos A y B, el **producto** $A \times B$ se define como el producto cartesiano respecto a las operaciones

$$(a_1, b_1) + (a_2, b_2) := (a_1 + a_2, b_1 + b_2), \quad (a_1, b_1) \cdot (a_2, b_2) := (a_1 a_2, b_1 b_2).$$

Dejo al lector verificar que $A \times B$ es un anillo. Si A y B son conmutativos, entonces $A \times B$ es también conmutativo.

De la misma manera, para una familia de anillos A_i, el producto $\prod_{i\in I} A_i$ se define como el producto cartesiano respecto a las operaciones

$$(a_i)_i + (a'_i)_i := (a_i + a'_i)_i, \quad (a_i)_i \cdot (a'_i)_i := (a_i a'_i)_i.$$ ▲

1.4 Algunos no-anillos (♣)

Sería instructivo considerar algo parecido a anillo que no cumpla algún axioma de la lista.

1.4.1. Ejemplo. Para los polinomios

$$f = \sum_{i\geq 0} a_i\, X^i,\ g = \sum_{i\geq 0} b_i\, X^i \in A[X]$$

tomemos la suma habitual y el producto dado por la sustitución

$$f \circ g := f(g(X)) := \sum_{k\geq 0} a_k \left(\sum_{i\geq 0} b_i\, X^i\right)^k.$$

Notamos que

$$(f_1 + f_2) \circ g = f_1 \circ g + f_2 \circ g,$$

pero en general

$$f \circ (g_1 + g_2) \neq f_1 \circ g_1 + f_1 \circ g_2.$$

Por ejemplo, si $f = X^2$, $g_1 = X$, $g_2 = 1$, entonces

$$f \circ (g_1 + g_2) = X^2 + 2X + 1, \text{ mientras que } f \circ g_1 + f \circ g_2 = X^2 + 1.$$

Estas dos expresiones no coinciden si $2 \neq 0$ en A. Este ejemplo demuestra la importancia de tener en el caso no conmutativo dos condiciones de distributividad: por la izquierda y por la derecha. ▲

1.4.2. Ejemplo. Recordemos que sobre el espacio $\mathbb{R}^3$ se puede definir el **producto cruz**

$$\times : \mathbb{R}^3 \times \mathbb{R}^3 \to \mathbb{R}^3$$

mediante

$$u \times v := \begin{vmatrix} \vec{e}_1 & \vec{e}_2 & \vec{e}_3 \\ u_1 & u_2 & u_3 \\ v_1 & v_2 & v_3 \end{vmatrix} := \begin{vmatrix} u_2 & u_3 \\ v_2 & v_3 \end{vmatrix} \vec{e}_1 - \begin{vmatrix} u_1 & u_3 \\ v_1 & v_3 \end{vmatrix} \vec{e}_2 + \begin{vmatrix} u_1 & u_2 \\ v_1 & v_2 \end{vmatrix} \vec{e}_3,$$

donde

$$\vec{e}_1 := (1,0,0),\ \vec{e}_2 := (0,1,0),\ \vec{e}_3 := (0,0,1);$$
$$u = (u_1, u_2, u_3), \quad v = (v_1, v_2, v_3).$$

El lector puede verificar que el producto cruz es distributivo respecto a la adición habitual de vectores:

$$u \times (v + w) = u \times v + u \times w, \quad (u + v) \times w = u \times w + v \times w.$$

Notamos que para cualquier $u \in \mathbb{R}^3$ se cumple

$$u \times u = \vec{0}.$$

En particular, tenemos

$$(u + v) \times (u + v) = \underbrace{u \times u}_{=\vec{0}} + u \times v + v \times u + \underbrace{v \times v}_{=\vec{0}},$$

así que

$$v \times u = -u \times v.$$

Esto significa que se tiene una especie de anillo no conmutativo. Sin embargo, hay dos problemas.

1) Primero, falta la identidad: esta tendría que cumplir $\vec{\imath}\times\vec{\imath}=\vec{\imath}$, pero $\vec{\imath}\times\vec{\imath}=\vec{0}$, y el vector nulo $\vec{0}$ claramente no funciona como la identidad.

2) El producto cruz no es asociativo: en general

$$(u\times v)\times w\neq u\times(v\times w),$$

y en lugar de la asociatividad se cumple la **identidad de Jacobi**

$$u\times(v\times w)+v\times(w\times u)+w\times(u\times v)=0.$$

Usando el producto cruz, se puede definir una estructura de anillo no sobre $\mathbb{R}^3$, sino sobre $\mathbb{R}^4$. Identifiquemos los elementos de $\mathbb{R}^4$ con pares (a,u), donde $a\in\mathbb{R}$ y $u\in\mathbb{R}^3$. Las operaciones

$$\begin{aligned}(a,u)+(b,v)&:=(a+b,u+v),\\(a,u)\cdot(b,v)&:=(ab-u\cdot v,\,av+bu+u\times v).\end{aligned}$$

definen un anillo no conmutativo que se conoce como el **anillo de cuaterniones** y se denota por $\mathbb{H}$[*]. Véase el ejercicio 1.5. ▲

1.4.3. Ejemplo. He aquí otro ejemplo parecido: para dos matrices $a,b\in M_n(A)$ definamos su **conmutador** como la matriz

$$[a,b]:=ab-ba. \tag{1.3}$$

Notamos que $[a,b]=0$ si y solo si las matrices conmutan: $ab=ba$. Tenemos $[a,a]=0$ y $[a,b]=-[b,a]$. En general,

$$[[a,b],c]\neq[a,[b,c]],$$

pero para cualesquiera $a,b,c\in M_n(A)$ se cumple la identidad de Jacobi

$$[a,[b,c]]+[b,[c,a]]+[c,[a,b]]=0$$

—dejo al lector el placer de desarrollar los corchetes según la definición (1.3) y verificar que todos los términos se cancelan. ▲

Para nosotros, el término "anillo" siempre asume la existencia de identidad y la asociatividad del producto, así que $\mathbb{R}^3$ con el producto cruz y las matrices con el conmutador $[-,-]$ no son anillos. Son casos particulares de algo llamado "anillos de Lie[**]", que es también una estructura sumamente importante, pero no la vamos a estudiar en este curso.

1.5 Subanillos

Si tenemos un anillo A y un subconjunto $B\subseteq A$, para asegurarnos que B es también un anillo respecto a la misma suma y producto, basta verificar que B contiene 0 y 1 y que las operaciones $(x,y)\mapsto x+y$, $x\mapsto -x$, $(x,y)\mapsto xy$ se restringen a B. Esto nos lleva a la noción de subanillo.

1.5.1. Definición. Sea A un anillo. Se dice que un subconjunto $B\subseteq A$ es un **subanillo** de A si

1) B es cerrado respecto a la adición y elementos opuestos:

   a) $0\in B$,

[*] La letra $\mathbb{H}$ conmemora al descubridor de cuaterniones, el matemático irlandés William Rowan Hamilton (1805–1865).
[**] Sophus Lie (1842–1899), matemático noruego, conocido por sus trabajos en la teoría de grupos de Lie.

b) $x+y \in B$ para cualesquiera $x, y \in B$,

c) $-x \in B$ para todo $x \in B$;

2) B es cerrado respecto a la multiplicación:

a) $1 \in B$,

b) $xy \in B$ para cualesquiera $x, y \in B$.

El lector puede comprobar que en este caso B es también un anillo respecto a las mismas operaciones que A.

1.5.2. Observación. *Sea A un anillo. Si $A_i \subseteq A$ son subanillos, entonces $\bigcap_i A_i$ es un subanillo.* □

1.5.3. Ejemplo. Tenemos una cadena de subanillos

$$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}.$$ ▲

1.5.4. Ejemplo. Los números naturales $\mathbb{N}$ no forman un subanillo de $\mathbb{Z}$: si $n \in \mathbb{N}$, entonces $-n \notin \mathbb{N}$, salvo cuando $n = 0$. ▲

1.5.5. Ejemplo. Las matrices de la forma

$$\begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix}, \quad x \in A$$

cumplen todas las condiciones, salvo que la matriz identidad no está entre ellas. Entonces, tales matrices no forman un subanillo de $M_2(A)$ según nuestra definición de arriba. ▲

1.5.6. Ejemplo. El **anillo de los enteros de Gauss**[*] es dado por

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

Se ve fácilmente que este es un subanillo de $\mathbb{C}$. ▲

1.5.7. Ejemplo. Otro ejemplo del mismo tipo: consideremos la raíz cúbica de la unidad $\zeta_3 := e^{2\pi i/3}$ y 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, caculamos que

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

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

$$(ac - bd) + (ad + bc - bd)\zeta_3 \in \mathbb{Z}[\zeta_3].$$

Después de esta verificación se ve que $\mathbb{Z}[\zeta_3]$ es un subanillo de $\mathbb{C}$. Este se llama el **anillo de los enteros de Eisenstein**[**]. ▲

[*] Carl Friedrich Gauss (1777–1855) — matemático alemán. Entre otras cosas, escribió a los veintiún años su tratado "Disquisitiones arithmeticae" que revolucionó el área de la teoría de números.

[**] 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.

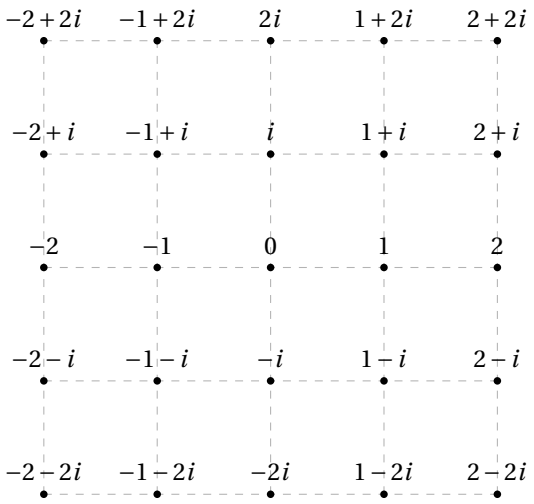

Figura 1.6: Los enteros de Gauss $\mathbb{Z}[i]$ en el plano complejo

1.5.8. Ejemplo. Sea $n \neq 1$ un entero libre de cuadrados[*]. Pongamos

$$\mathbb{Q}(\sqrt{n}) := \{a + b\sqrt{n} \mid a, b \in \mathbb{Q}\}.$$

Este es un subanillo de $\mathbb{R}$ si $n > 0$ y un subanillo de $\mathbb{C}$ si $n < 0$. Por ejemplo, calculemos los productos:

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

Por las mismas consideraciones, el conjunto

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

es un subanillo de $\mathbb{Q}(\sqrt{n})$.

En el caso cuando $n \equiv 1 \pmod 4$, se puede considerar el conjunto más grande

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

Este es también un subanillo de $\mathbb{Q}(\sqrt{n})$. La parte menos evidente son los productos:

$$\left(a + b\,\frac{1+\sqrt{n}}{2}\right)\left(c + d\,\frac{1+\sqrt{n}}{2}\right) = ac + bd\,\frac{1+2\sqrt{n}+n}{4} + (ad + bc)\,\frac{1+\sqrt{n}}{2}.$$

Ahora ya que $n = 4k + 1$ para algún $k \in \mathbb{Z}$,

$$\frac{1+2\sqrt{n}+n}{4} = \frac{1+\sqrt{n}}{2} + k,$$

así que el producto pertenece a $\mathbb{Z}\Big[\frac{1+\sqrt{n}}{2}\Big]$.

[*] Es decir, $p^2 \nmid n$ para ningún primo p. Los primeros números libres de cuadrados son

$$\pm 1, \pm 2, \pm 3, \pm 5, \pm 6, \pm 7, \pm 10, \pm 11, \pm 13, \pm 14, \pm 15, \pm 17, \ldots$$

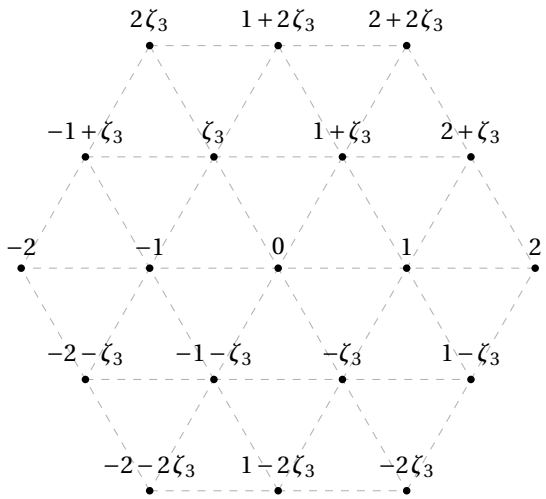

Figura 1.7: Los enteros de Eisenstein $\mathbb{Z}[\zeta_3]$ en el plano complejo

Tenemos una cadena de subanillos

$$\mathbb{Z} \subset \mathbb{Z}[\sqrt{n}] \subset \mathbb{Z}\left[\frac{1+\sqrt{n}}{2}\right] \subset \mathbb{Q}(\sqrt{n}) \subset \mathbb{C}.$$

En particular, para $n=-3$ se obtiene el anillo $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$. Notamos que $\zeta_3 = \frac{1+\sqrt{-3}}{2} - 1$, de donde se ve que $\mathbb{Z}[\zeta_3] = \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$. ▲

1.5.9. Ejemplo. Sea A un anillo. Los polinomios constantes

$$c + 0\cdot X + 0\cdot X^2 + 0\cdot X^3 + \cdots$$

forman un subanillo del anillo de polinomios $A[X]$. Los polinomios $A[X]$ forman un subanillo del anillo de las series formales $A[[X]]$ (véase el ejercicio 1.9). ▲

1.5.10. Ejemplo. Para $n = 1,2,3,\ldots$ y para $p = 2,3,5,7,11,\ldots$ primo los conjuntos

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

son subanillos de $\mathbb{Q}$. ▲

1.5.11. Ejemplo. Para un conjunto X y un anillo A el anillo de funciones $\mathrm{Fun}(X,A)$ tiene como su subanillo las funciones constantes dadas por $x \mapsto c$ para $c \in A$ fijo.

En el anillo $\mathrm{Fun}(\mathbb{R},\mathbb{R})$ tenemos los siguientes subanillos:

$$\{\text{funciones constantes}\} \subset \{\text{funciones continuas}\} \subset \mathrm{Fun}(\mathbb{R},\mathbb{R}).$$ ▲

1.5.12. Ejemplo. Los anillos $\mathbb{Z}$ y $\mathbb{Z}/n\mathbb{Z}$ no tienen subanillos propios. En efecto, si $A \subseteq \mathbb{Z}$ es un subanillo, entonces $1 \in A$, y luego para cualquier $n = 1,2,3,\ldots$ se tiene

$$\pm\underbrace{(1+\cdots+1)}_{n} \in A,$$

así que $A = \mathbb{Z}$. De la misma manera, para un subanillo $A \subseteq \mathbb{Z}/n\mathbb{Z}$ tenemos necesariamente $[1]_n \in A$, pero para todo $a = 1,2,3,4,\ldots$ se cumple

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

1.6 Algunas observaciones respecto a los axiomas

Varias propiedades naturales de la suma y producto en un anillo A se siguen de los axiomas.

1) La asociatividad de la adición y multiplicación implican la asociatividad generalizada: para las expresiones
$$x_1 + \cdots + x_n \quad \text{y} \quad x_1 \cdots x_n$$
cualquier modo de poner los paréntesis da el mismo resultado. En el capitulo anterior ya hemos visto cómo probarlo por inducción sobre n.

2) La identidad y el cero son únicos: en efecto, si hay dos elementos 0 y $0'$ que satisfacen la propiedad del cero y 1 y $1'$ que satisfacen la propiedad de la identidad, entonces
$$0 = 0 + 0' = 0' \quad \text{y} \quad 1 = 1 \cdot 1' = 1'.$$

3) Los elementos opuestos están definidos de modo único. En efecto, si
$$x + y = y + x = 0, \quad x + z = z + x = 0,$$
entonces
$$y = y + 0 = y + (x + z) = (y + x) + z = 0 + z = z.$$

4) La sustracción $(x, y) \mapsto x - y$ no se introduce como una operación especial, sino por la definición,
$$x - y := x + (-y).$$

5) Para las sumas funciona la cancelación: para cualesquiera $x, y, z \in A$ se tiene
$$x + z = y + z \Longrightarrow x = y.$$
En efecto, basta notar que si $x + z = y + z$, entonces $x = x + z + (-z) = y + z + (-z) = y$.

6) En general, la cancelación para los productos no funciona: la identidad $xz = yz$ no necesariamente implica que $x = y$. Por ejemplo, en el anillo $\mathbb{Z}/6\mathbb{Z}$ se tiene $[2] \cdot [2] = [5] \cdot [2]$, aunque $[2] \neq [5]$.

7) Para todo $x \in A$ se cumple
$$-(-x) = x.$$

8) Para todo $x \in A$ se cumple
$$0 \cdot x = x \cdot 0 = 0.$$
En efecto, tenemos
$$0 \cdot x = (0 + 0) \cdot x = 0 \cdot x + 0 \cdot x,$$
y luego por la cancelación, $0 \cdot x = 0$. De la misma manera se demuestra que $x \cdot 0 = 0$.

9) Los axiomas permiten que $1 = 0$, pero en este caso para todo $x \in A$ se tiene
$$x = x \cdot 1 = x \cdot 0 = 0,$$
así que A consiste en un solo elemento 0. Tal anillo se llama el **anillo nulo** y se denota por 0.

10) Para cualesquiera $x, y \in A$ se tiene
$$x \cdot (-y) = (-x) \cdot y = -xy.$$
En particular,
$$x \cdot (-1) = (-1) \cdot x = -x.$$
En efecto, tenemos por la distributividad
$$x \cdot (-y) + xy = x(-y + y) = 0,$$
así que $x \cdot (-y) = -xy$. De la misma manera se verifica que $(-x) \cdot y = -xy$.

11) Para cualesquiera $x, y \in A$ se tiene
$$x(y - z) = xy - xz, \quad (x - y)z = xz - yz.$$

1.6.1. Definición. Un número natural $n = 1, 2, 3, \ldots$ puede ser visto como un elemento de A poniendo
$$n := \underbrace{1 + \cdots + 1}_{n} \in A,$$
y de la misma manera, para los enteros negativos,
$$-n := -(\underbrace{1 + \cdots + 1}_{n}) \in A.$$
(No estamos diciendo que diferentes $n \in \mathbb{Z}$ corresponden a diferentes elementos de A; por ejemplo, $2 = 5 = 8 = \cdots$ en $\mathbb{Z}/3\mathbb{Z}$.) Esto nos permite multiplicar cualquier elemento $x \in A$ por $n = 1, 2, 3, \ldots$:
$$nx = (\underbrace{1 + \cdots + 1}_{n})\, x = \underbrace{x + \cdots + x}_{n}, \quad (-n)\, x = -(nx).$$
Con estas definiciones se cumplen las propiedades esperadas:
$$n(x + y) = nx + ny,$$
$$(m + n)\, x = mx + nx,$$
$$(mn)\, x = m(nx),$$
$$1 \cdot x = x.$$
De la misma manera, para $x \in A$ y $n = 1, 2, 3, \ldots$ se define
$$x^n := \underbrace{x \cdots x}_{n} \quad \text{y} \quad x^0 := 1.$$
Notamos que
$$x^m x^n = x^{m+n}, \quad (x^m)^n = x^{mn},$$
y si A es un anillo conmutativo (!), entonces
$$(xy)^n := \underbrace{xy \cdots xy}_{n} = x^n y^n.$$

1.6.2. Proposición (Fórmula del binomio). *Si A es un anillo conmutativo (!), entonces para cualesquiera $x, y \in A$ y $n = 0, 1, 2, 3, \ldots$ se cumple*
$$(x + y)^n = \sum_{\substack{i,j \geq 0 \\ i+j=n}} \binom{n}{i} x^i y^j = \sum_{0 \leq i \leq n} \binom{n}{i} x^{n-i} y^i,$$
donde $\binom{n}{i}$ denota el coeficiente binomial $\frac{n!}{i! \cdot (n-i)!}$.

Demostración. Esta fórmula obviamente se cumple para $n = 0, 1$. Luego, si esta se cumple para n, tenemos

$$\begin{aligned}(x+y)^{n+1} = (x+y)^n (x+y) &= \sum_{0\le i\le n} \binom{n}{i} x^{n+1-i} y^i + \sum_{0\le i\le n} \binom{n}{i} x^{n-i} y^{i+1} \\ &= \sum_{0\le i\le n+1} \binom{n}{i} x^{n+1-i} y^i + \sum_{1\le i\le n+1} \binom{n}{i-1} x^{n+1-i} y^i \\ &= \sum_{0\le i\le n+1} \left(\binom{n}{i} + \binom{n}{i-1} \right) x^{n+1-i} y^i = \sum_{0\le i\le n+1} \binom{n+1}{i} x^{n+1-i} y^i.\end{aligned}$$

(Note que para desarrollar el producto $(x+y)^n (x+y)$ se usa la conmutatividad.) ■

En un anillo *no conmutativo*, en general $(xy)^n \neq x^n y^n$, y la fórmula del binomio tampoco tiene por qué funcionar: por ejemplo, $(x+y)^2 = x^2 + xy + yx + y^2$, pero no es cierto que $xy = yx$. Haga el ejercicio 1.10 de abajo.

Podemos resumir esta sección diciendo que en un anillo abstracto A se cumplen prácticamente todas las propiedades habituales que uno espera de las operaciones aritméticas; solo hay que tener cuidado con la conmutatividad.

1.7 Divisores de cero y dominios

En los anillos como $\mathbb{C}$ y sus subanillos, el producto de dos números no nulos tampoco es nulo. Sin embargo, esto no es cierto, por ejemplo, en $\mathbb{Z}/6\mathbb{Z}$: se tiene $[2]\cdot[3] = [0]$, aunque $[2], [3] \neq [0]$. Para estudiar estos fenómenos, se introducen las siguientes nociones.

1.7.1. Definición. Sea A un anillo.

1) Si para $x \in A$ existe un elemento no nulo $y \in A$ tal que $xy = 0$ o $yx = 0$, entonces se dice que x es un **divisor de cero**.

2) Si para $x \in A$ se cumple
$$x^n := \underbrace{x \cdots x}_{n} = 0$$
para algún $n = 1, 2, 3, \ldots$, entonces se dice que x es un elemento **nilpotente**, o simplemente un **nilpotente**.

3) Si para $e \in A$ se cumple
$$e^2 = e,$$
entonces se dice que e es un elemento **idempotente**, o simplemente un **idempotente**.

Notamos que cualquier nilpotente es un divisor de cero. Un idempotente distinto de 1 es también un divisor de cero: si $e^2 = e$, entonces
$$e^2 - e = e(e-1) = 0,$$
donde $e - 1 \neq 0$.

1.7.2. Definición.

1) Un divisor de cero distinto de 0 se llama un **divisor de cero no trivial**.

2) Un nilpotente distinto de 0 se llama un **nilpotente no trivial**.

3) Un idempotente distintio de 0 y 1 se llama un **idempotente no trivial**.

1.7.3. Definición. Un anillo A se llama un **dominio de integridad**[*] (o simplemente un **dominio**) si se cumplen las siguientes condiciones:.

1) A es conmutativo,

2) $A \neq 0$,

3) A no tiene divisores de cero no triviales.

Notamos que la última condición es equivalente a

$$xy = 0 \Longrightarrow x = 0 \text{ o } y = 0$$

o también a

$$x \neq 0 \text{ e } y \neq 0 \Longrightarrow xy \neq 0.$$

1.7.4. Observación. *Un anillo conmutativo no nulo A es un dominio si y solo si en A funciona la cancelación para los productos: para cualesquiera $x, y, z \in A$ se tiene*

$$xz = yz,\ z \neq 0 \Longrightarrow x = y.$$

Demostración. Supongamos que A es un dominio. Si $xz = yz$, entonces

$$(x - y)\, z = xz - yz = 0.$$

Ahora si $z \neq 0$, entonces $x - y = 0$; es decir, $x = y$.

Viceversa, si en A tenemos la cancelación, entonces $xy = 0$ para $y \neq 0$ puede ser escrito como $xy = 0 \cdot y$, y luego cancelando y se obtiene $x = 0$. Esto demuestra que A es un dominio. ■

1.7.5. Ejemplo. Los números complejos $\mathbb{C}$ forman un dominio, y por ende cualquier subanillo de $\mathbb{C}$ (como $\mathbb{Z}$, $\mathbb{Z}[\sqrt{n}]$, $\mathbb{Q}(\sqrt{n})$, etc.) es también un dominio. ▲

1.7.6. Proposición. *Si A es un dominio, entonces el anillo de polinomios $A[X]$ es también un dominio.*

Demostración. Para dos polinomios no nulos

$$f = a_m X^m + \cdots + a_1 X + a_0,$$
$$g = b_n X^n + \cdots + b_1 X + b_0$$

con $a_m, b_n \neq 0$ tenemos

$$f g = \left(a_m X^m + \cdots + a_1 X + a_0\right)\left(b_n X^n + \cdots + b_1 X + b_0\right) = a_m b_n X^{m+n} + \cdots + a_0 b_0,$$

donde $a_m b_n \neq 0$, dado que A es un dominio. Entonces, $f g \neq 0$. ■

Aunque al principio uno puede pensar que un anillo conmutativo que no es un dominio es algo patológico, es todo lo contrario: divisores de cero, nilpotentes e idempotentes surgen muy a menudo en muchos contextos importantes.

1.7.7. Ejemplo. El anillo $\mathbb{Z}/n\mathbb{Z}$ tiene divisores de cero no triviales si y solamente si n es un número compuesto.

En efecto, si $n = ab$ para algunos $0 < a, b < n$, entonces tenemos $[a]_n \cdot [b]_n = [ab]_n = [0]_n$, aunque $[a]_n, [b]_n \neq [0]_n$. Viceversa, si $n = p$ es un número primo, entonces $[a]_p \cdot [b]_p = [ab]_p = [0]_p$ si y solo si $p \mid ab$, lo que implica $p \mid a$ o $p \mid b$; es decir, $[a]_p = [0]_p$ o $[b]_p = [0]_p$. ▲

[*] No confundir con dominio de integración.

Dejo al lector pensar cómo en los anillos $\mathbb{Z}/n\mathbb{Z}$ surgen nilpotentes e idempotentes no triviales. Por ejemplo, para $n = 12$ el resto $[6]_{12}$ es nilpotente: tenemos $6^2 = 36 \equiv 0 \pmod{12}$. Los restos $[-3]_{12}$ y $[4]_{12}$ son idempotentes:

$$(-3)^2 = 9 \equiv -3, \quad 4^2 \equiv 4 \pmod{12}.$$

1.7.8. Ejemplo. En el producto de anillos $A \times B$ con $A, B \neq 0$ los elementos de la forma $(a,0)$ y $(0,b)$ son divisores de cero: se tiene

$$(a,0)\cdot(0,b) = (0,0).$$

Los elementos $(0,1)$ y $(1,0)$ son idempotentes. Entonces, el producto de dos anillos no nulos nunca es un dominio. ▲

1.7.9. Ejemplo. Los anillos de funciones suelen tener muchos divisores de cero. Por ejemplo, consideremos el anillo de las aplicaciones $\mathbb{R} \to \mathbb{R}$. Consideremos las aplicaciones $f, g\colon \mathbb{R} \to \mathbb{R}$ definidas por

$$f(x) := \begin{cases} x, & x \geq 0, \\ 0, & x < 0; \end{cases} \qquad g(x) := \begin{cases} 0, & x \geq 0, \\ x, & x < 0. \end{cases}$$

Tenemos $fg = 0$, aunque $f \neq 0$ y $g \neq 0$. ▲

1.7.10. Ejemplo. En el anillo de matrices $M_n(A)$ hay muchos divisores de cero, nilpotentes e idempotentes no triviales. Por ejemplo, para las matrices

$$e_{11} := \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad e_{12} := \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad e_{21} := \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \quad e_{22} := \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

tenemos

$\cdot$	e_{11}	e_{12}	e_{21}	e_{22}
e_{11}	e_{11}	e_{12}	0	0
e_{12}	0	0	e_{11}	e_{12}
e_{21}	e_{21}	e_{22}	0	0
e_{22}	0	0	e_{21}	e_{22}

Todas estas matrices son divisores de cero; e_{11} y e_{22} son idempotentes, mientras que e_{12} y e_{21} son nilpotentes. ▲

1.8 Característica

1.8.1. Definición. Sea A un anillo. El número mínimo $n = 1, 2, 3, \ldots$ tal que

$$n := \underbrace{1 + \cdots + 1}_{n} = 0$$

se llama la **característica** de A y se denota por $\operatorname{char} A = n$. Cuando $n \neq 0$ para todo n, se pone $\operatorname{char} A = 0$.

1.8.2. Ejemplo. Los anillos $A = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ (y cualquier subanillo de $\mathbb{C}$) y los anillos correspondientes $A[X]$, $M_n(A)$ son de característica 0.

Los anillos $A = \mathbb{Z}/n\mathbb{Z}$ y los anillos correspondientes $A[X]$, $M_n(A)$ son de característica n. ▲

1.8.3. Observación. *Si A no tiene divisores de cero no triviales, entonces la característica de A es 0 o un número primo p.*

Demostración. Asumamos que $\operatorname{char} A = n$, donde $n = ab$ es un número compuesto con $0 < a, b < n$. Luego,

$$\underbrace{(1+\cdots+1)}_{a}\underbrace{(1+\cdots+1)}_{b} = \underbrace{1+\cdots+1}_{ab} = 0.$$

Pero por nuestra hipótesis sobre A, esto implicaría que

$$\underbrace{1+\cdots+1}_{a} = 0 \text{ o } \underbrace{1+\cdots+1}_{b} = 0,$$

lo que contradice la minimalidad de n. ■

1.8.4. Observación (Fórmula del binomio en característica p). *Sea p un número primo y A un anillo conmutativo de característica p. Entonces, para cualesquiera $x, y \in A$ se tiene*

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

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 nulos en A, excepto x^p e y^p. ■

La aplicación $x \mapsto x^p$ del resultado anterior se conoce como el **endomorfismo de Frobenius**[*].

1.8.5. Corolario (Pequeño teorema de Fermat[**]). *Si p es un número primo, entonces*

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

Demostración. Hay que probar que en el anillo $\mathbb{Z}/p\mathbb{Z}$ se cumple $x^p = x$ para todo x. De hecho, si $x = [0]$ o $x = [1]$, es obvio. Luego, por inducción, si esto se cumple para $x = [a]$, entonces

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

1.9 Unidades (elementos invertibles)

1.9.1. Definición. En un anillo A se dice que $x \in A$ es una **unidad**[***] (o un elemento **invertible**) si existe $x^{-1} \in A$ (el elemento **inverso**) tal que

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

El conjunto de las unidades en A se denotará por $A^\times$.

Si x es una unidad, su inverso es único: si existen dos elementos y e y' que son inversos a x, entonces

$$y = y \cdot 1 = y \cdot (x \cdot y') = (y \cdot x) \cdot y' = 1 \cdot y' = y'.$$

1.9.2. Observación. *Las unidades cumplen las siguientes propiedades.*

[*] Ferdinand Georg Frobenius (1849–1917) — matemático alemán, conocido por sus contribuciones en la teoría de las ecuaciones diferenciales, teoría de números, teoría de grupos y teoría de representación.

[**] Pierre de Fermat (1601–1665) — matemático francés, conocido por su trabajo en la teoría de números.

[***] No confundir con la identidad 1.

1) Se tiene $1 \in A^\times$.

2) Si $x, y \in A^\times$*, entonces* $xy \in A^\times$*; a saber,*

$$(xy)^{-1} = y^{-1}x^{-1}.$$

3) Si $x \in A^\times$*, entonces* $x^{-1} \in A^\times$*; a saber,* $(x^{-1})^{-1} = x$. □

1.9.3. Observación. *Si* $B \subseteq A$ *es un subanillo, entonces* $B^\times \subseteq A^\times$. □

1.9.4. Ejemplo. Las únicas unidades en el anillo de enteros $\mathbb{Z}$ son ± 1. ▲

1.9.5. Ejemplo. En el anillo de los números racionales $\mathbb{Q}$ cualquier elemento no nulo es invertible: para $\frac{a}{b}$ con $a \neq 0$ se tiene

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

1.9.6. Ejemplo. En el anillo de los enteros de Gauss $\mathbb{Z}[i]$, supongamos que $\alpha \in \mathbb{Z}[i]$ es invertible, así que existe $\alpha^{-1} \in \mathbb{Z}[i]$ tal que $\alpha\alpha^{-1} = 1$. Luego,

$$|\alpha| \cdot |\alpha^{-1}| = 1,$$

así que

$$|\alpha|^2 \cdot |\alpha^{-1}|^2 = 1.$$

Notamos que para cualquier $\alpha = a + bi \in \mathbb{Z}[i]$, el cuadrado del valor absoluto $|\alpha|^2 = a^2 + b^2$ es un número entero. Entonces, si α es invertible, la ecuación de arriba implica que $|\alpha| = 1$. Viceversa, si $|\alpha| = 1$, entonces

$$\alpha^{-1} = \frac{1}{|\alpha|^2}\,\overline{\alpha} = \overline{\alpha} \in \mathbb{Z}[i],$$

así que las unidades en $\mathbb{Z}[i]$ son precisamente los elementos de valor absoluto 1:

$$\mathbb{Z}[i]^\times = \{\pm 1, \pm i\} = \{1, \zeta_4, \zeta_4^2, \zeta_4^3\}.$$ ▲

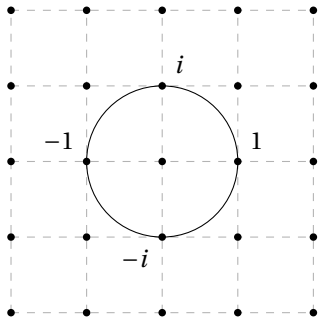

Figura 1.8: Unidades en los enteros de Gauss $\mathbb{Z}[i]$

1.9.7. Ejemplo. Calcular los elementos invertibles en un anillo no es tan fácil como uno puede pensar. Por ejemplo, tenemos

$$\frac{1}{1+\sqrt{2}} = \frac{1-\sqrt{2}}{(1+\sqrt{2})(1-\sqrt{2})} = \frac{1-\sqrt{2}}{1-2} = -1+\sqrt{2},$$

así que $1+\sqrt{2}$ es invertible en el anillo $\mathbb{Z}[\sqrt{2}]$. Luego, todas las potencias de $1+\sqrt{2}$ son también invertibles: para cualquier $n = 2, 3, 4, \ldots$

$$((1+\sqrt{2})^n)^{-1} = ((1+\sqrt{2})^{-1})^n = (-1+\sqrt{2})^n \in \mathbb{Z}[\sqrt{2}].$$

Los números $(1+\sqrt{2})^n$ son diferentes:

$$1+\sqrt{2} < (1+\sqrt{2})^2 < (1+\sqrt{2})^3 < (1+\sqrt{2})^4 < \cdots$$

Entonces, en el anillo $\mathbb{Z}[\sqrt{2}]$ hay un número infinito de unidades. ▲

1.9.8. Ejemplo. Un número $a \in \mathbb{Z}$ es invertible módulo $n = 1,2,3,\ldots$ si y solamente si $\mathrm{mcd}(a,n) = 1$:

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{[a]_n \mid \mathrm{mcd}(a,n) = 1\}.$$

En particular,

$$\begin{aligned}
(\mathbb{Z}/2\mathbb{Z})^\times &= \{[1]_1\},\\
(\mathbb{Z}/3\mathbb{Z})^\times &= \{[1]_3, [2]_3\},\\
(\mathbb{Z}/4\mathbb{Z})^\times &= \{[1]_4, [3]_4\},\\
(\mathbb{Z}/5\mathbb{Z})^\times &= \{[1]_5, [2]_5, [3]_5, [4]_5\},\\
(\mathbb{Z}/6\mathbb{Z})^\times &= \{[1]_6, [5]_6\},\\
(\mathbb{Z}/7\mathbb{Z})^\times &= \{[1]_7, [2]_7, [3]_7, [4]_7, [5]_7, [6]_7\},\\
(\mathbb{Z}/8\mathbb{Z})^\times &= \{[1]_8, [3]_8, [5]_8, [7]_8\},\\
(\mathbb{Z}/9\mathbb{Z})^\times &= \{[1]_9, [2]_9, [4]_9, [5]_9, [7]_9, [8]_9\},\\
(\mathbb{Z}/10\mathbb{Z})^\times &= \{[1]_{10}, [3]_{10}, [7]_{10}, [9]_{10}\},\\
&\ldots
\end{aligned}$$

En efecto, asumamos que $\mathrm{mcd}(a,n) = 1$. Entonces, la **identidad de Bézout** nos da

$$ab + nc = 1$$

para algunos $b, c \in \mathbb{Z}$. Luego, $ab \equiv 1 \pmod{n}$, así que $[a]_n^{-1} = [b]_n$.

Viceversa, asumamos que para $[a]_n$ existe $[b]_n$ tal que $[a]_n \cdot [b]_n = 1$. Luego, $ab \equiv 1 \pmod{n}$, lo que significa que

$$ab + nc = 1.$$

para algún $c \in \mathbb{Z}$. Pero esta identidad implica que $\mathrm{mcd}(a,n) = 1$. (Recordemos que $\mathrm{mcd}(a,n)$ es el mínimo número positivo de la forma $ax + ny$ para $x, y \in \mathbb{Z}$.) ▲

La función

$$\phi(n) := |(\mathbb{Z}/n\mathbb{Z})^\times| = \#\{0 \le a \le n-1 \mid \mathrm{mcd}(a,n) = 1\}$$

se llama la **función ϕ de Euler**. He aquí algunos de sus valores:

n:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\phi(n)$:	1	1	2	2	4	2	6	4	6	4	10	4	12	6	8
n:	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
$\phi(n)$:	8	16	6	18	8	12	10	22	8	20	12	18	12	28	8

1.9.9. Proposición. *Si $p = 2,3,5,7,11,\ldots$ es primo y $k = 1,2,3,4,\ldots$, entonces*

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

Demostración. Consideramos los números

$$a = 0, 1, 2, \ldots, p^k - 2, p^k - 1.$$

En esta lista hay p^k elementos. Luego, $\mathrm{mcd}(a, p^k) = 1$ si y solamente si $p \nmid a$. Los números en la esta tales que $p \mid a$ son los múltiplos de p: $0, p, 2p, 3p, \ldots$—cada p-ésimo número, en total p^k/p de ellos. Entonces,

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

1.10 Cuerpos

1.10.1. Definición. Un **cuerpo** k es un anillo conmutativo tal que

1) $k \neq 0$,

2) todo elemento no nulo de k es invertible.

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

1.10.3. Ejemplo. El cuerpo más pequeño posible consiste en dos elementos 0 y 1 con las siguientes operaciones:

$+$	0	1
0	0	1
1	0	0

$\cdot$	0	1
0	0	0
1	0	1

▲

1.10.4. Ejemplo. Para $n \neq 1$ un entero libre de cuadrados, consideremos el anillo

$$\mathbb{Q}(\sqrt{n}) := \{a + b\sqrt{n} \mid a, b \in \mathbb{Q}\}.$$

Este es un cuerpo: para $a + b\sqrt{n} \neq 0$ calculamos

$$(a + b\sqrt{n})^{-1} = \frac{a - b\sqrt{n}}{(a + b\sqrt{n})(a - b\sqrt{n})} = \frac{a}{a^2 - nb^2} - \frac{b}{a^2 - nb^2}\sqrt{n} \in \mathbb{Q}(\sqrt{n}).$$

Aquí es importante que $a^2 - nb^2 \neq 0$ si $(a, b) \neq (0, 0)$. En efecto, si $n < 0$, tenemos una suma de a^2 y un múltiplo positivo de b^2 que puede ser nula solo cuando $a = b = 0$. Si $n > 0$, entonces $a^2 - nb^2 = 0$ implica que $n = \left(\frac{a}{b}\right)^2$ que no es el caso porque n es libre de cuadrados. ▲

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

1.10.5. Observación. *Todo cuerpo es un dominio.*

Demostración. Supongamos que $xy = 0$, donde $x \neq 0$. Si estamos en un cuerpo, para x existe su inverso x^{-1}, y multiplicando la identidad $xy = 0$ por x^{-1}, se obtiene

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

donde la parte izquierda es igual a $(x^{-1}x)\, y = 1 \cdot y = y$, y la parte derecha es igual a 0. ■

1.10.6. Proposición. *$\mathbb{Z}/n\mathbb{Z}$ es un cuerpo si y solamente si $n = p$ es primo.*

Demostración. Si $n = p$ es primo, entonces $\operatorname{mcd}(a, p) = 1$ para todo $a = 1, \ldots, p - 1$ y todos los restos no nulos $[1]_p, [2]_p, \ldots, [p-1]_p$ son invertibles. Si n es compuesto, ya hemos notado que $\mathbb{Z}/n\mathbb{Z}$ no es un dominio, y en particular no es un cuerpo. ■

1.10.7. Notación. Para un número primo p el cuerpo $\mathbb{Z}/p\mathbb{Z}$ se denota por $\mathbb{F}_p$.

1.10.8. Ejemplo. Sea $\mathbb{F}_4$ el espacio vectorial de dimensión 2 sobre el cuerpo $\mathbb{F}_2$, generado por los elementos 1 y α. Este espacio tiene 4 elementos:

$$\mathbb{F}_4 = \{0, 1, \alpha, \alpha + 1\}.$$

La adición de vectores nos da

$+$	0	1	α	$\alpha+1$
0	0	1	α	$\alpha+1$
1	1	0	$\alpha+1$	α
α	α	$\alpha+1$	0	1
$\alpha+1$	$\alpha+1$	α	1	0

Definamos la multiplicación mediante $0\cdot x = x\cdot 0 = 0$, $1\cdot x = x\cdot 1 = x$ para todo x y la identidad

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

Luego,

$$\alpha(\alpha+1)=\alpha^2+\alpha=1$$

y

$$(\alpha+1)^2=\alpha^2+1^2=\alpha.$$

$\cdot$	0	1	α	$\alpha+1$
0	0	0	0	0
1	0	1	α	$\alpha+1$
α	0	α	$\alpha+1$	1
$\alpha+1$	0	$\alpha+1$	1	α

Se puede verificar que lo que tenemos es un cuerpo de cuatro elementos. ▲

1.10.9. Digresión. 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.

1.10.10. Definición. Si L es un cuerpo y $K\subseteq L$ es su subanillo que es también un cuerpo. En este caso se dice que K es un **subcuerpo** de L. También se dice que $K\subseteq L$ es una **extensión de cuerpos**.

1.10.11. Observación. *Si $K\subseteq L$ es una extensión de cuerpos, entonces L es un espacio vectorial sobre K respecto a la suma en L y la multiplicación de los elementos de L por elementos de K.* □

1.10.12. Ejemplo. Hemos visto las siguientes extensiones de cuerpos:

$$\mathbb{Q}\subset\mathbb{R}\subset\mathbb{C},\quad \mathbb{Q}\subset\mathbb{Q}(\sqrt{n})\subset\mathbb{C}.$$

El cuerpo $\mathbb{F}_4=\{0,1,\alpha,\alpha+1\}$ que hemos construido arriba contiene un subcuerpo $\mathbb{F}_2=\{0,1\}$. ▲

1.11 Cuerpos de fracciones

> Un hombre es como una fracción cuyo numerador es lo que es y cuyo denominador es lo que él piensa de sí mismo.
>
> León Tolstoi

La construcción de los números racionales $\mathbb{Q}$ a partir de los números enteros $\mathbb{Z}$ puede ser generalizada a cualquier dominio.

1.11.1. Construcción. Sea A un dominio. Consideremos la siguiente relación sobre $A \times A \setminus \{0\}$:

$$(a,b) \sim (a',b') \iff ab' = a'b.$$

Esta relación es visiblemente reflexiva y simétrica. Para ver que es transitiva, notamos que si

$$(a,b) \sim (a,b), \quad (a',b') \sim (a'',b''),$$

entonces

$$ab' = a'b, \quad a'b'' = a''b'.$$

Luego, usando que A es conmutativo (!)

$$b'(ab'') = (ab')\,b'' = (a'b)\,b'' = b(a'b'') = b(a''b') = b'(a''b).$$

Dado que A es un dominio (!), podemos cancelar b' y concluir que $ab'' = a''b$; es decir, que $(a,b) \sim (a'',b'')$.

Denotemos la clase de equivalencia de (a,b) por la fracción

$$\frac{a}{b} := [(a,b)]$$

y pongamos

$$\operatorname{Frac} A := (A \times A \setminus \{0\})/\sim = \left\{ \frac{a}{b} \;\middle|\; a,b \in A,\ b \neq 0 \right\}.$$

Definamos la suma y producto de fracciones mediante

$$\frac{a}{b} + \frac{c}{d} := \frac{ad+cb}{bd}, \quad \frac{a}{b} \cdot \frac{c}{d} := \frac{ac}{bd}.$$

1.11.2. Observación. *Las operaciones de arriba están bien definidas y definen una estructura de anillo conmutativo sobre* $\operatorname{Frac} A$. *El cero es la fracción* $\frac{0}{1}$ *y la identidad es la fracción* $\frac{1}{1}$. □

Notamos que una fracción es nula precisamente cuando su numerador es nulo:

$$\frac{a}{b} = \frac{0}{1} \iff a = 0.$$

Ahora toda fracción $\frac{a}{b} \neq \frac{0}{1}$ admite inversa:

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

Esto significa que $\operatorname{Frac} A$ es un cuerpo.

Notamos que tenemos la aplicación inyectiva $a \mapsto \frac{a}{1}$:

$$\frac{a}{1} = \frac{a'}{1} \iff a = a'.$$

De esta manera las fracciones con 1 en el numerador pueden ser identificadas con A.

1.11.3. Definición. Para un dominio A, el cuerpo $\operatorname{Frac} A$ que acabamos de construir se llama el **cuerpo de fracciones** de A.

1.11.4. Ejemplo. El cuerpo de fracciones de $\mathbb{Z}$ es precisamente $\mathbb{Q}$. ▲

1.11.5. Ejemplo. Sea k un cuerpo. Entonces, los polinomios con coeficientes en k forman un dominio $k[X]$. El cuerpo de fracciones correspondiente viene dado por

$$k(X) := \operatorname{Frac} k[X] = \left\{ \frac{f}{g} \;\middle|\; f, g \in A[X],\ g \neq 0 \right\}.$$

Por ejemplo, tenemos en $k(X)$

$$\frac{X^n - 1}{1} \cdot \frac{1}{X - 1} = \frac{1 + X + X^2 + \cdots + X^{n-1}}{1}.$$ ▲

1.11.6. Ejemplo. Si k es un cuerpo, no es muy interesante tomar el cuerpo de fracciones $\operatorname{Frac} k$. En efecto, tendremos para toda fracción

$$\frac{a}{b} = \frac{ab^{-1}}{bb^{-1}} = \frac{ab^{-1}}{1},$$

así que en el denominador siempre se puede poner 1. De esta manera $\operatorname{Frac} k$ se identifica con el mismo k, pero las palabras "se identifica" tendrán un sentido preciso un poco más adelante. ▲

Vamos a volver a los cuerpos de fracciones más adelante, después de introducir la noción de homomorfismo e isomorfismo de anillos.

1.12 ¿Para qué sirven los anillos? (♣)

Los anillos conmutativos tienen mucha importancia en las matemáticas modernas. En muchas situaciones hay una correspondencia

Objetos geométricos ("espacios") $\longleftrightarrow$ 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 $\mathbb{Z}$, $\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{n}]$ que hemos visto arriba. A tales objetos se pueden 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 $\mathbb{Z}$, $\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{n}]$ 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 $A[X]$, la dimensión sube por 1:

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

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.

1.13 Ejercicios

Ejercicio 1.1. Demuestre las identidades trigonométricas

$$\operatorname{sen}(\phi+\psi) = \operatorname{sen}\phi\cos\psi + \cos\phi\operatorname{sen}\psi,$$
$$\cos(\phi+\psi) = \cos\phi\cos\psi - \operatorname{sen}\phi\operatorname{sen}\psi$$

usando la identidad de Euler para los números complejos.

Ejercicio 1.2. Sea $n = 2,3,4,\ldots$ un número fijo y $\zeta_n := e^{2\pi i/n}$.

1) Para un polinomio complejo $f = a_{n-1}X^{n-1} + \cdots + a_1 X + a_0$ de grado $< n$ demuestre que

$$\frac{1}{n}\sum_{0\le k\le n-1} f(\zeta_n^k) = a_0.$$

2) Demuestre que $\prod_{1\le k\le n-1}(1-\zeta_n^k) = n$.

Ejercicio 1.3. Sea X un conjunto y 2^X el conjunto de los subconjuntos de X. Demuestre que 2^X es un anillo conmutativo de característica 2 respecto a la suma $A\triangle B$ (diferencia simétrica) y producto $A\cap B$ (intersección).

Ejercicio 1.4 (Los números duales). Inmitando la definición de los números complejos, consideremos las expresiones $x+y\epsilon$, donde x, y son números reales, respecto a la suma y producto

$$(x_1+y_1\epsilon)+(x_2+y_2\epsilon) := (x_1+x_2)+(y_1+y_2)\,\epsilon,$$
$$(x_1+y_1\epsilon)\cdot(x_2+y_2\epsilon) := x_1x_2 + (x_1y_2+x_2y_1)\,\epsilon.$$

1) Demuestre que de esta manera se obtiene un anillo conmutativo.

2) Demuestre que no es un dominio.

3) Determine cuándo un elemento $x+y\epsilon$ es invertible y encuentre la fórmula para su inverso.

Ejercicio 1.5 (Cuaterniones). Denotemos por $u\cdot v$ y $u\times v$ el producto escalar y producto cruz sobre $\mathbb{R}^3$ respectivamente.

1) Demuestre que en general, $(u\times v)\times w \neq u\times(v\times w)$, pero se cumple la **identidad de Jacobi**

$$u\times(v\times w) + v\times(w\times u) + w\times(u\times v) = 0.$$

2) Identifiquemos los elementos de $\mathbb{R}^4$ con pares (a,u), donde $a\in\mathbb{R}$ y $u\in\mathbb{R}^3$. Demuestre que $\mathbb{R}^4$ forma un anillo no conmutativo respecto a las operaciones

$$(a,u)+(b,v) := (a+b, u+v), \quad (a,u)\cdot(b,v) := (ab - u\cdot v,\ av + bu + u\times v).$$

Este se llama el **anillo de cuaterniones** y se denota por $\mathbb{H}$.

3) Demuestre que todo elemento no nulo en $\mathbb{H}$ es invertible.
Sugerencia: defina $\overline{(a,u)} := (a,-u)$ *y calcule* $(a,u)\cdot\overline{(a,u)}$.

Ejercicio 1.6 (Enteros ciclotómicos). Para un número primo p consideremos el conjunto

$$\mathbb{Z}[\zeta_p] := \{a_0 + a_1\zeta_p + a_2\zeta_p^2 + \cdots + a_{p-2}\zeta_p^{p-2} \mid a_i\in\mathbb{Z}\} \subset \mathbb{C}.$$

1) Demuestre que $\mathbb{Z}[\zeta_p]$ es un subanillo de $\mathbb{C}$.

2) Calcule $(1+\zeta_5^3)^2$, $(1+\zeta_5^3)^3$, $(1+\zeta_5^3)^{-1}$ en $\mathbb{Z}[\zeta_5]$.

Ejercicio 1.7. Para un número fijo $n = 1,2,3,\ldots$ consideremos el conjunto de fracciones con potencias de n en el denominador:

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

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

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

Verifique que $\mathbb{Z}\Big[\frac{1}{n}\Big]$ y $\mathbb{Z}_{(p)}$ son subanillos de $\mathbb{Q}$.

Ejercicio 1.8. Sea A un anillo y $A_i \subseteq A$ una familia de subanilos. Demuestre que $\bigcap_i A_i$ es un subanillo de A.

Ejercicio 1.9 (Series formales de potencias). Sea A un anillo conmutativo. Una **serie formal de potencias** con coeficientes en A en una variable X es una suma formal

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

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

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

1) Demuestre que las series formales forman un anillo conmutativo. Este se denota por $A[[X]]$.

2) Demuestre que $A[X]$ es un subanillo de $A[[X]]$.

3) Demuestre que si A es un dominio, entonces $A[[X]]$ es también un dominio.

   Sugerencia: para dos series no nulas $f, g \in A[[X]]$, sean a_m y b_n el primer coeficiente no nulo de f y g respectivamente:

   $$f = a_m X^m + a_{m+1} X^{m+1} + \cdots, \quad g = b_n X^n + b_{n+1} X^{n+1} + \cdots$$

   Analice los coeficientes del producto fg.

4) Verifique la identidad

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

   en el anillo de series formales $A[[X]]$.

5) Verifique la identidad $\Big(\sum_{i\geq 0} \frac{X^i}{i!}\Big)^n = \sum_{i \geq 0} \frac{n^i}{i!} X^i$ en el anillo de series formales $\mathbb{Q}[[X]]$.

Ejercicio 1.10. En el anillo de matrices $M_2(A)$ encuentre dos elementos a, b tales que

$$(ab)^2 \neq a^2 b^2, \quad (a+b)^2 \neq a^2 + 2ab + b^2.$$

Ejercicio 1.11. Sea A un anillo conmutativo.

1) Si $x, y \in A$ son nilpotentes, demuestre que $x + y$ es también nilpotente.

   Sugerencia: calcule $(x+y)^n$ usando el teorema del binomio.

2) En el anillo de matrices $M_2(A)$ encuentre $a, b \in M_2(A)$ tales que a y b son nilpotentes, pero $a+b$ no es nilpotente.

Ejercicio 1.12. Sea A un anillo. Demuestre que si $x \in A$ es nilpotente, entonces $1 \pm x$ es invertible en A.
Sugerencia: revise la fórmula para la serie geométrica $\sum_{k\geq 0} x^k$.

Ejercicio 1.13. Consideremos las matrices con coeficientes en cualquier anillo conmutativo A.

1) Demuestre que las matrices de la forma

$$\begin{pmatrix} 0 & a_{12} & a_{13} \\ 0 & 0 & a_{23} \\ 0 & 0 & 0 \end{pmatrix}$$

son nilpotentes.

2) En general, demuestre que toda **matriz triangular superior estricta** de $n \times n$; es decir $a \in M_n(A)$ con $a_{ij} = 0$ para $i \geq j$ (la diagonal es también nula) es nilpotente.

Ejercicio 1.14. Sea $a \in M_n(A)$ una matriz triangular superior estricta. Demuestre que

$$(1-a)^{-1} = 1 + a + a^2 + a^3 + \cdots + a^{n-1}.$$

Ejercicio 1.15. Sea A un dominio.

1) Demuestre que para todo $a \neq 0$ la aplicación

$$\mu_a \colon A \to A, \quad x \mapsto ax$$

es inyectiva.

2) Demuestre que si A es un dominio finito, entonces la aplicación $x \mapsto ax$ es biyectiva.

3) Deduzca de lo anterior que todo dominio finito es un cuerpo.

Ejercicio 1.16. Sean L un cuerpo y $K \subseteq L$ un subcuerpo. Demuestre que L es un espacio vectorial sobre K.

Ejercicio 1.17.

1) Calcule la dimensión del espacio vectorial

   a) $\mathbb{C}$ sobre $\mathbb{R}$,

   b) $\mathbb{Q}(\sqrt{n})$ sobre $\mathbb{Q}$, donde $n \neq 1$ es libre de cuadrados.

2) Demuestre que $\mathbb{R}$ tiene dimensión infinita sobre $\mathbb{Q}$.
   Sugerencia: recuerde que $\mathbb{R}$ *no es un conjunto numerable.*

Ejercicio 1.18. Sean A un dominio y $\operatorname{Frac} A$ su cuerpo de fracciones. Demuestre explícitamente todos los axiomas de anillos (anillos conmutativos, cuerpos) para $\operatorname{Frac} A$.

Ejercicio 1.19. Volvamos al anillo de las series formales $A[[X]]$ introducido en el ejercicio 1.9.

1) En el anillo $\mathbb{Z}[[X]]$ demuestre que los siguientes elementos son invertibes y encuentre sus inversos:

$$f = X^2 - 2X + 1, \quad g = 1 - X - X^2.$$

2) Generalizando estos cálculos, demuestre que una serie formal es invertible si y solo si su término constante es invertible:

$$A[[X]]^\times = \left\{ \sum_{i\geq 0} a_i\, X^i \;\middle|\; a_0 \in A^\times \right\}.$$

Ejercicio 1.20. Sea k un cuerpo. Una **serie de Laurent** es una serie formal que puede tener un número finito de términos $a_i\, X^i$ con $i < 0$:

$$f = \sum_{i\geq -k} a_i X^i = a_{-k}X^{-k} + a_{-k+1}X^{-k+1} + \cdots + a_{-1}X^{-1} + a_0 + a_1 X + a_2 X^2 + a_3 X^3 + \cdots,$$

donde $a_i \in k$. Demuestre que las series de Laurent forman un cuerpo. Este se denota por $k((X))$.