Cuerpos. Introducción a números complejos. Cuerpos ordenados

Sergio A. Carrillo
sacarrillot@unal.edu.co

La noción de cuerpo

Un *cuerpo* es una tripla $(K, +, \cdot)$ donde $K \neq \emptyset$ y

$$\begin{aligned} + \ : K \times K &\to K, & \cdot \ : K \times K &\to K \\ (x, y) &\mapsto x + y, & (x, y) &\mapsto x \cdot y = xy, \end{aligned}$$

satisfacen las siguientes propiedades:

i) **Axiomas para la suma**
- $(x + y) + z = x + (y + z)$, para todo $x, y, z \in K$.
- $x + y = y + x$, para todo $x, y \in K$.
- Existe un elemento de K, denotado por 0, tal que $x + 0 = x$ para todo $x \in K$.
- Para cada $x \in K$ existe un $y \in K$ tal que $x + y = 0$. Este elemento se denota por $-x$ y se llama el *inverso aditivo de* x.

La noción de cuerpo

ii) **Axiomas para el producto**
- $(xy)z = x(yz)$, para todo $x, y, z \in K$.
- $xy = yx$, para todo $x, y \in K$.
- Existe un elemento de K, distinto de 0, que denotaremos por 1, tal que $1x = x1 = x$, para todo $x \in K$.
- Para cada $x \in K$ distinto de cero, existe un $y \in K$ tal que $xy = 1$. Este elemento se denota por $1/x$ y se llama el *recíproco de* x.

iii) **Axioma de distributividad**
- $(x + y)z = xz + yz$, para todo $x, y, z \in K$.

En el lenguaje de grupos, se requiere que $(K, +)$ y $(K^*, \cdot)$ sean grupos abelianos, además de la distributividad.

Notación: $K^* := K \setminus \{0\}$.

Ejemplos

- $\mathbb{Z}/p\mathbb{Z}$ con las operaciones de clases, donde p es un número primo.
- $\mathbb{Q}$ con las operaciones usuales.
- $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ con las operaciones usuales.
- $\mathbb{R}$ con las operaciones que veremos al construirlo.
- $\mathbb{C} = \{a + ib : a, b \in \mathbb{R}\}$ con las operaciones de suma por componentes y producto

$$(a + ib)(c + id) = (ac - bd) + i(ad + bc).$$

Construcción de $\mathbb{C}$

Se puede definir

$$\mathbb{C} := \{(a,b) \in \mathbb{R}^2 : a, b \in \mathbb{R}\}$$

con las operaciones

$$(a,b)+(c,d) = (a+c, b+d), \qquad (a,b)\cdot(c,d) = (ac-bd, ad+bc).$$

Si llamamos $i = (0,1)$, entonces $i^2 = (-1,0)$. Así podemos escribir

$$(a,b) = (a,0)\cdot(1,0) + (b,0)\cdot(0,1) = a + ib,$$

notando que

$$\iota : \mathbb{R} \to \mathbb{C}, \qquad \iota(a) = (a,0)$$

satisface que

$$\iota(a+c) = \iota(a) + \iota(c), \qquad \iota(ac) = \iota(a)\iota(c), \qquad a, c \in \mathbb{R}.$$

Conjugado, partes real e imaginaria

Dado $z = a + ib$, su conjugado se define por $\overline{z} := a - ib$. Esta aplicación satisface que

$$\overline{\overline{z}} = z, \qquad \overline{z + w} = \overline{z} + \overline{w}, \qquad \overline{zw} = \overline{z} \cdot \overline{w}, \qquad z, w \in \mathbb{C}.$$

Por tanto $\overline{\cdot} : \mathbb{C} \to \mathbb{C}$ es un morfismo de cuerpos. Además,

$$\mathrm{Re}(z) = a = \frac{z + \overline{z}}{2}, \qquad \mathrm{Im}(z) = b = \frac{z - \overline{z}}{2i}$$

son las partes reales e imaginarias de z, respectivamente.

Norma y cocientes en $\mathbb{C}$

Note además que

$$z \cdot \overline{z} = a^2 + b^2.$$

La *norma* de z se define por

$$|z| = \sqrt{a^2 + b^2} = \sqrt{z \cdot \overline{z}}, \qquad |\cdot| : \mathbb{C} \to \mathbb{R}.$$

Entonces $z = 0$ si y solo si $|z| = 0$. Además, si $z \neq 0$, entonces

$$\frac{1}{z} = \frac{\overline{z}}{|z|^2} = \frac{a}{a^2 + b^2} - i\frac{b}{a^2 + b^2} \in \mathbb{C}.$$

También $|zw| = |z| \cdot |w|$, para todo $z, w \in \mathbb{C}$.

Números algebraicos

Sea $a \in \mathbb{R}$. Decimos que a es *algebraico* sobre $\mathbb{Q}$ si existen $n+1$ elementos $c_0, c_1, \ldots, c_n \in \mathbb{Q}$ no todos nulos, tales que

$$c_n a^n + c_{n-1} a^{n-1} + \cdots + c_2 a^2 + c_1 a + c_0 = 0.$$

Decimos que a es *trascendente* si a no es algebraico.

- Si $p, q \in \mathbb{Z}$, $q \neq 0$, $qx - p = 0$ tiene como solución a $x = p/q$. Luego todo racional es algebraico.
- $\sqrt{2}$ es algebraico al ser solución de $x^2 - 2 = 0$. Lo mismo es válido para $\sqrt{3}, \sqrt{5}, \sqrt{6}, \ldots$, y en general para $\sqrt{p/q}$, donde $p, q \in \mathbb{Q}_{>0}$.

Más ejemplos

- $\sqrt[2]{2}$ es algebraico al ser solución de $x^3 - 2 = 0$.
- $\varphi = \frac{1+\sqrt{5}}{2}$ (número áureo) es algebraico al ser raíz de $x^2 - x - 1 = 0$.
- e y π son números trascendentes (Hermite y von Lindemann, respectivamente).

Teorema

Sea $\mathfrak{A} \subseteq \mathbb{R}$ el conjunto de números algebraicos reales. Entonces $\mathfrak{A}$ es un cuerpo con las operaciones de los reales y $\mathbb{Q} \subset \mathfrak{A}$.

Números construirles con regla y compás

Un número $\alpha \in \mathbb{R}$ es *construible con regla y compás* si puede obtenerse como longitud de un segmento construido a partir de un segmento inicial de longitud 1, usando solo:

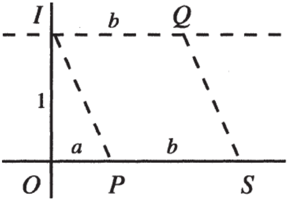
- Una regla no graduada (para trazar rectas entre puntos).
- Un compás (para trazar círculos con centro y radio dados).

Teorema

Sea $\mathfrak{C} \subseteq \mathbb{R}$ el conjunto de números construibles reales. Entonces $\mathfrak{C}$ es un cuerpo con las operaciones de los reales y $\mathbb{Q} \subset \mathfrak{C}$.

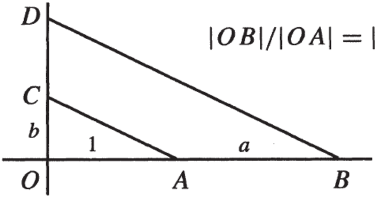
Por ejemplo, $1, \sqrt{2}, \frac{1+\sqrt{5}}{2} \in \mathfrak{C}$.

Suma y productos construibles



$I = (0, 1)$ $\quad Q = (b, 1)$

$P = (a, 0)$ $\quad S = (a + b, 0)$



$|OB|/|OA| = |OD|/|OC|$

$B = (1 + a, 0)$ $\quad C = (0, b)$

$A = (1, 0)$

Propiedades

Sea K un cuerpo.

1. Si $x, y \in K$ y $xy = 0$, entonces $x = 0$ o $y = 0$.
2. Si $x, y, z \in K$, $z \neq 0$ y $xz = yz$, entonces $x = y$.
3. Considere $\iota : \mathbb{N} \to K, \iota(n) = n \cdot 1 = \underbrace{1 + \cdots + 1}_{n \text{ veces}}$.

   En general, ι no es inyectiva. Cuando lo es, K contiene una copia de $\mathbb{N}$ ($\iota(\mathbb{N})$). Además, K también contiene una copia de $\mathbb{Z}$ y de $\mathbb{Q}$.

Notación: $n = n \cdot 1$.

Cuerpos ordenados

Una pareja $(X, <)$ es un *conjunto ordenado* si $X \neq \emptyset$ y $<$ es una relación binaria que satisface:

- (orden total) Si $x, y \in X$, entonces $x < y$, $x = y$ o $y < x$.
- (transitividad) Si $x < y$ e $y < z$, entonces $x < z$.

Notación: $y > x$ si $x < y$; $x \leq y$ si $x < y$ o $x = y$.

Un *cuerpo ordenado* es una cuádrupla $(K, +, \cdot, <)$ donde $(K, +, \cdot)$ es un cuerpo, $(K, <)$ es un conjunto ordenado y además

- Si $x < y$, entonces $x + z < y + z$, para todo $z \in K$.
- Si $x < y$ y $z > 0$, entonces $xz < yz$.

Propiedades de cuerpos ordenados

Proposición

Sea $(K, +, \cdot, <)$ *un cuerpo ordenado. Entonces:*

1. *Si* $x > 0$, *entonces* $-x < 0$.
2. *Si* $x > 0$ *e* $y > 0$, *entonces* $xy > 0$.
3. *Si* $x \neq 0$, *entonces* $x^2 > 0$. *En particular,* $1 > 0$.
4. *Si* $x > 0$, *entonces* $1/x > 0$.
5. *Si* $0 < x < y$, *entonces* $0 < 1/y < 1/x$.

Ejemplos: Los ejemplos habituales son $\mathbb{Q}$ y $\mathbb{R}$. Note que $\mathbb{C}$ y $\mathbb{Z}/p\mathbb{Z}$ no pueden ser cuerpos ordenados.