1 LOS NÚMEROS REALES

(Resumen teórico)

1.1 Introducción

1.2 Relación de orden

1.3 Los naturales

1.4 Los enteros

1.5 Los racionales

1.6 Valor absoluto, intervalos, cotas

1.7 Polinomios

1.1 Introducción

El conjunto $\mathbb{R}$ de los *números reales* se construye de forma que cada punto de una línea recta corresponda a un número real, y viceversa.

Independientemente de la construcción formal, resumimos las propiedades de $\mathbb{R}$.

En $\mathbb{R}$ se define la operación suma, que asigna a cada par de número reales a, b otro número real $a+b$. Esta operación tiene las siguientes propiedades:

- (Asociativa) $a+(b+c)=(a+b)+c$ para todos $a,b,c \in \mathbb{R}$.
- (Conmutativa) $a+b=b+a$ para todos $a,b \in \mathbb{R}$.
- (Existencia de elemento neutro) Existe un número real 0 tal que $a+0=a$ para todo $a \in \mathbb{R}$.
- (Existencia de elementos opuestos) Para cada número real a, existe un número real $-a$ tal que $a+(-a)=0$.

En $\mathbb{R}$ se define una segunda operación, el producto, que asigna a cada par de número reales a, b otro número real ab. Esta operación tiene las siguientes propiedades:

- (Asociativa) $a(bc) = (ab)c$ para todos $a, b, c \in \mathbb{R}$.
- (Conmutativa) $ab = ba$ para todos $a, b \in \mathbb{R}$.
- (Existencia de elemento neutro) Existe un número real 1 tal que $a \cdot 1 = a$ para todo $a \in \mathbb{R}$.
- (Existencia de elementos inversos) Para cada $a \in \mathbb{R} \setminus \{0\}$, existe un número real a^{-1} (denotado también $1/a$) tal que $a \cdot a^{-1} = 1$.

Finalmente, la propiedad distributiva relaciona ambas operaciones:

- $a(b + c) = ab + ac$ para todos $a, b, c \in \mathbb{R}$.

Todo conjunto con dos operaciones que satisfacen todas las propiedades anteriores se denomina cuerpo. Estas propiedades justifican convenciones usuales, como no escribir paréntesis cuando hay más de dos sumandos o factores, escribir $a-b$ en lugar de $a+(-b)$, etc. De esas propiedades se deducen también otras bien conocidas, como $-(a+b) = -a-b$, las leyes de simplificación en sumas ($a+c = b+c \Leftrightarrow a = b$) y productos ($ac = bc \Leftrightarrow a = b$, si $c \neq 0$), etc.

1.2 Relación de orden

En $\mathbb{R}$ se define una relación de orden $\leq$. La notación $a < b$ significa $a \leq b$ y $a \neq b$. Esta relación es total, lo cual significa que, dados dos reales a, b, se cumple exactamente una de las tres propiedades $a < b$, $a = b$ o $a > b$.

El comportamiento de la relación de orden respecto a las operaciones es el siguiente. Para todo $a, b, c \in \mathbb{R}$,

- $a < b \Leftrightarrow a + c < b + c$.
- Si $c > 0$, entonces $a < b \Leftrightarrow ac < bc$.
- Si $c < 0$, entonces $a < b \Leftrightarrow ac > bc$.

1.3 Los naturales

El conjunto de los números naturales es el subconjunto $\mathbb{N}$ de $\mathbb{R}$ formado por los números obtenidos sumando 1 consigo mismo repetidamente: $\mathbb{N} = \{1, 2, 3, \ldots\}$.

La suma y el producto de dos naturales es un natural. Ciertamente, las propiedades válidas para todos los reales (asociativas, conmutativas, distributiva, etc.) son en particular válidas para los naturales. Observemos, sin embargo, que el neutro de la suma 0 no es natural, que el opuesto de un natural no es un natural y que el inverso de un natural tampoco es un natural, con la excepción de 1, que es su propio inverso.

Restringido al conjunto de los naturales, la relación de orden tiene al menos dos propiedades particulares relevantes. La primera es que, si A es un subconjunto no vacío de $\mathbb{N}$, entonces existe un elemento $m \in A$ tal que $m \leq a$ para todo $a \in A$; este elemento se denomina *mínimo* o *primer elemento de* A. La segunda es la siguiente.

Principio de inducción. Sea A un subconjunto no vacío de $\mathbb{N}$ y m su mínimo. Si $n \in A$ implica $n+1 \in A$, entonces $A = \{n \in \mathbb{N} : n \geq m\}$.

1.4 Los enteros

El conjunto $\mathbb{Z}$ de los números enteros está formado por los naturales, el 0 y los opuestos de todos los naturales: $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$. La suma y el producto de dos enteros son enteros. En los enteros, estas operaciones tienen las mismas propiedades que la suma y el producto de números reales, con la excepción de que en los enteros no es cierto que cada entero $a \neq 0$ tenga inverso entero para el producto (de hecho, sólo 1 y -1 tienen inverso). La definición de anillo conmutativo es similar a la de cuerpo, excepto que no se exige la existencia de inversos para el producto. Así, $\mathbb{Z}$, con la suma y el producto, es un anillo conmutativo.

Si a, b y c son números enteros y $a = bc$, se dice que b es un *divisor* de a o que *divide* a a y que a es un *múltiplo* de b. Un número entero *primo* es un entero $p > 1$ tal que no tiene ningún divisor positivo d tal que $1 < d < p$. Los números primos tienen la siguiente propiedad.

Teorema fundamental de la aritmética. Todo entero mayor que 1 es o bien primo o puede escribirse de manera única (salvo el orden) como producto de números primos.

Supondremos conocidos otros conceptos y propiedades relativos a los números enteros, como el máximo común divisor y el mínimo común múltiplo; enteros relativamente primos (o primos entre sí); que si p es un primo que divide a un producto ab, entonces divide a uno de los factores, etc.

1.5 Los racionales

El conjunto $\mathbb{Q}$ de los *números racionales* está formado por todos los números reales de la forma $a/b = ab^{-1}$ con $a, b \in \mathbb{Z}$ y $b \neq 0$.

Nótese que, si $a, b, c, d \in \mathbb{Z}$ y $b \neq 0 \neq d$, entonces $a/b = c/d$ si, y sólo si, $ad = bc$. Si $q = a/b \in \mathbb{Q}$, con a y b primos entre sí, se dice que la fracción a/b es irreducible. Los números reales no racionales se llaman irracionales; por ejemplo, $\sqrt{2}$ es irracional. La suma y el producto de dos racionales es un racional y, con estas operaciones, $\mathbb{Q}$ es un cuerpo.

Cada número real admite una expresión decimal. Los números racionales se caracterizan como los números reales que admiten una expresión decimal periódica, por ejemplo $108/33 = 3{,}272727\dots$

Respecto al orden, debemos señalar que

- Dados dos números reales distintos cualesquiera $a < b$, existen infinitos racionales q e infinitos irracionales r tales que $a < q < b$ y $a < r < b$. En particular, entre cada dos números racionales distintos hay infinitos números racionales.

1.6 Valor absoluto, intervalos, cotas

El valor absoluto de un número real a es el número real $|a| = \begin{cases} a & \text{si } a \geq 0, \\ -a & \text{si } a < 0. \end{cases}$

Tiene las siguientes propiedades.

Para cualesquiera $a, b, x \in \mathbb{R}$,

- $|a| \geq 0$; $\quad |a| = 0 \Leftrightarrow a = 0$;
- $|a + b| \leq |a| + |b|$;
- $|ab| = |a| \cdot |b|$;
- Si $a > 0$, entonces $|x| < a \Leftrightarrow -a < x < a$.

La distancia entre dos números reales a y b es el número $|a - b|$.

Los intervalos son subconjuntos relevantes de $\mathbb{R}$.

Sean $a, b \in \mathbb{R}$ con $a < b$.
El conjunto $[a, b] = \{x \in \mathbb{R} \mid a \leq x \leq b\}$ se llama *intervalo cerrado* de *extremos* a y b;
el conjunto $(a, b) = \{x \in \mathbb{R} \mid a < x < b\}$ se llama *intervalo abierto* de *extremos* a y b;
los conjuntos $(a, b] = \{x \in \mathbb{R} \mid a < x \leq b\}$ y $[a, b) = \{x \in \mathbb{R} \mid a \leq x < b\}$ son *intervalos semiabiertos* o *semicerrados*.
Finalmente, los conjuntos

$$\begin{aligned} (-\infty, a] &= \{x \in \mathbb{R} \mid x \leq a\}, & (-\infty, a) &= \{x \in \mathbb{R} \mid x < a\}, \\ [a, +\infty) &= \{x \in \mathbb{R} \mid x \geq a\}, & (a, +\infty) &= \{x \in \mathbb{R} \mid x > a\}, \end{aligned}$$

se llaman *intervalos no acotados*. A veces, también se escribe $\mathbb{R} = (-\infty, +\infty)$.

Sean a y $\delta > 0$ números eales. El entorno de centro a y *radio* δ es el intervalo abierto $(a-\delta, a+\delta)$. Nótese la equivalencia

$$x \in (a-\delta, a+\delta) \Leftrightarrow |x-a| < \delta.$$

Los *semientornos derecho e izquierdo* de a y radio δ son los intervalos abiertos $(a, a+\delta)$ y $(a-\delta, a)$, respectivamente.

Un *entorno de* $+\infty$ es un intervalo de la forma $(a, +\infty)$ y un *entorno de* $-\infty$ es un intervalo de la forma $(-\infty, a)$.

Sea A un subconjunto de $\mathbb{R}$. Un número k es una *cota superior* de A si $a \leq k$ para todo $a \in A$. Si A tiene cotas superiores, la menor de ellas se llama el *supremo* de A. Análogamente, k es una *cota inferior* de A si $k \leq a$ para todo $a \in A$. Si A tiene cotas inferiores, la mayor de todas ellas se llama el *ínfimo* de A. En $\mathbb{R}$ se cumple el siguiente teorema.

Teorema del extremo. Todo conjunto de números reales no vacío acotado superiormente (resp. inferiormente) tiene supremo (resp. ínfimo).
Si A tiene supremo m y m es un elemento de A, entonces m se denomina *máximo* de A y se denota $\max A$; si A tiene ínfimo m y m es un elemento de A, entonces m se denomina *mínimo* de A y se denota $\min A$.

Sea x un número real.

La parte entera inferior de x es el número entero

$$\lfloor x \rfloor = \text{máx}\{m \in \mathbb{Z} : m \leq x\}.$$

La parte entera superior de un número real x es el número entero

$$\lceil x \rceil = \text{mín}\{m \in \mathbb{Z} : m \leq x\}.$$

Si x es un entero, entonces $x = \lfloor x \rfloor = \lceil x \rceil$. Si x no es entero, entonces $\lfloor x \rfloor$ y $\lceil x \rceil$ son, respectivamente, el primer entero a la izquierda y el primer entero a la derecha de x en la representación de los números reales en una recta.

1.7 Polinomios

Un *polinomio* con coeficientes en $\mathbb{R}$ es una aplicación $f\colon \mathbb{R} \to \mathbb{R}$ de la forma

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

donde $n \geq 0$ es un natural y $a_0, \ldots, a_n$ son números reales, denominados coeficientes del polinomio. Si $a_n \neq 0$, el número n se llama grado del polinomio f y se denota $\deg f(x)$. El conjunto de todos los polinomios con coeficientes en $\mathbb{R}$ se denota $\mathbb{R}[x]$.

Notemos que, si $f(x) = a_n x^n + \cdots + a_0$ es un polinomio y $m > n$, el polinomio $f(x)$ también puede escribirse en la forma $f(x) = a_m x^m + \cdots + a_n x^n + \cdots + a_0$ simplemente tomando $a_m = a_{m-1} = \cdots = a_{n+1} = 0$.

La suma de dos polinomios $f(x) = a_n x^n + \cdots + a_0$ y $g(x) = b_n x^n + \cdots + b_0$ es el polinomio definido por

$$(f+g)(x) = f(x) + g(x) = (a_n + b_n)x^n + (a_{n-1} + b_{n-1})x^{n-1} + \cdots + (a_0 + b_0).$$

Esta suma es asociativa y conmutativa; admite elemento neutro, que es el polinomio definido por $e(x) = 0$; y cada polinomio $f(x)$ tiene opuesto, que es el polinomio $-f(x)$, que se obtiene cambiando de signo todos los coeficientes de $f(x)$.

El producto de dos polinomios $f(x) = a_n x^n + \cdots + a_0$ y $g(x) = b_m x^m + \cdots + b_0$ es el polinomio definido por

$$(f \cdot g)(x) = f(x)g(x) = c_{n+m}x^{n+m} + \cdots + c_0, \qquad \text{con} \qquad c_k = a_k b_0 + a_{k-1} b_1 + \cdots + a_0 b_k,$$

para todo $k \in \{0, \ldots, n+m\}$. Este producto es asociativo y conmutativo; admite elemento neutro, que es el polinomio definido por $u(x) = 1$; y es distributivo respecto a la suma. Así, $\mathbb{R}[x]$, con la suma y el producto, es un anillo conmutativo.

Sea $a \in \mathbb{R}$. El *polinomio constante* a es el polinomio definido por $f(x) = a$. La suma y el producto de polinomios constantes tienen las mismas propiedades que la suma y el producto de los números reales, por lo cual cada polinomio constante $f(x) = a$ se identifica con el número real a.

Con la suma y el producto que hemos definido, $\mathbb{R}[x]$ no es un cuerpo, porque no es cierto que todo polinomio tenga inverso para el producto. Los únicos polinomios que tienen inverso son los constantes distintos de cero.

Teorema de la división. Sean $f(x), g(x) \in \mathbb{R}[x]$, con $g(x) \neq 0$. Entonces existen polinomios $q(x), r(x) \in \mathbb{R}[x]$ únicos tales que

$$f(x) = g(x)q(x) + r(x), \quad \text{y} \quad r = 0 \quad \text{o} \quad \deg r(x) < \deg g(x).$$

Los polinomios $q(x)$ y $r(x)$ se denominan, respectivamente, *cociente* y *resto* de la divición de $f(x)$ por $g(x)$.
Si $r(x) = 0$, se dice que $f(x)$ es *divisible* por $g(x)$ y que $f(x)$ se *descompone* en producto de los dos *factores* $g(x)$ y $q(x)$.
Teorema del resto. Sea $f(x)$ un polinomio y $a \in \mathbb{R}$. El valor $f(a)$ es el resto de la división de $f(x)$ por $x - a$.
Con frecuencia se denomina también *regla de Ruffini* a un algoritmo bien conocido (que no detallamos aquí) para dividir un polinomio $f(x)$ por un polinomio de la forma $x - a$.

Una raíz de un polinomio $p(x)$ es un número a tal que $p(a) = 0$. Un número real a es una raíz de un polinomio $f(x)$ si, y sólo si, $f(x)$ es divisible por $x - a$.

- Si $f(x) = a_n x^n + \cdots + a_0$ es un polinomio con todos los coeficientes enteros y $a \in \mathbb{Z}$ es una raíz de $f(x)$, entonces a es un divisor de a_0.

Polinomios de segundo grado

Consideremos los polinomios de segundo grado $p(x) = ax^2 + bx + c \in \mathbb{R}[x]$, $a \neq 0$.

El número real $\Delta = b^2 - 4ac$ se denomina discriminante.

Si $\Delta > 0$, entonces $p(x)$ tiene las dos raíces reales distintas

$$x_1 = \frac{-b + \sqrt{\Delta}}{2a}, \quad x_2 = \frac{-b - \sqrt{\Delta}}{2a}$$

y $p(x)$ factoriza como $p(x) = a(x - x_1)(x - x_2)$.

Si $\Delta = 0$, entonces $p(x)$ tiene una única raíz $x_0 = -b/(2a)$, y $p(x) = a(x - x_0)^2$.

Finalmente, si $\Delta < 0$, entonces $p(x)$ no tiene raíces reales y no admite ninguna factorización como producto de polinomios con coeficientes reales de grado 1.

La factorización de polinomios

Se tiene las siguiente propiedad:

- Todo polinomio $f(x)$ con coeficientes reales es producto de polinomios con coeficientes reales de grado 1 y de grado 2 con discriminante negativo.

Además de la división de polinomios y la factorización de los de segundo grado, hay algunas fórmulas útiles para factorizar polinomios que son consecuencias de la fórmula del Binomio de Newton.

Definimos el factorial de un entero no negativo n, denotado $n!$, como $0! = 1$, $1! = 1$ y $n! = n(n-1)\cdots 2 \cdot 1$ si $n \geq 2$.

Si n y k son enteros no negativos, el número binomial n sobre k se define como

$$\binom{n}{k} = \begin{cases} 0 & \text{si } k > n, \\ \dfrac{n!}{k!(n-k)!} & \text{si } k \leq n. \end{cases}$$

Observemos que, en el caso $k \leq n$, simplificando $(n-k)!$ en la fracción se obtiene

$$\binom{n}{k} = \frac{n(n-1)(n-2)\cdots(n-k+1)}{k!}.$$

Se cumplen las siguientes propiedades:

- $\binom{n}{0} = \binom{n}{n} = 1, \quad (n \geq 0).$
- $\binom{n}{1} = \binom{n}{n-1} = n, \quad (n \geq 1).$

- $\binom{n}{k} = \binom{n}{n-k}, \quad (0 \leq k \leq n).$
- $\binom{n-1}{k-1} + \binom{n-1}{k} = \binom{n}{k}, \quad (1 \leq k \leq n).$

Los números binomiales aparecen en la fórmula del binomio de Newton. Aunque esta fórmula será aplicada esencialmente a polinomios, hay que remarcar que es válida en todo anillo conmutativo. Si $n \geq 0$ es un natural, y a y b son elementos de un anillo conmutativo (por ejemplo, polinomios), entonces

$$\boxed{(a+b)^n = \binom{n}{0}a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \cdots + \binom{n}{n-1}ab^{n-1} + \binom{n}{n}b^n.}$$

En el caso de los polinomios, esta fórmula puede interpretarse como una factorización del término de la derecha. Otras factorizaciones a menudo útiles son las siguientes:

- $a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + \cdots ab^{n-1} + b^{n-1}).$
- Si n es impar, $a^n + b^n = (a+b)(a^{n-1} - a^{n-2}b + \cdots - ab^{n-2} + b^{n-1}).$

Como casos particulares:

- $a^2 - b^2 = (a+b)(a-b).$
- $a^n - 1 = (a-1)(a^{n-1} + a^{n-2} + \cdots + a + 1).$
- Si n es impar, $a^n + 1 = (a+1)(a^{n-1} - a^{n-2} + \cdots - a + 1).$