PROBLEMAS RESUELTOS DE MATEMÁTICAS SUPERIORES (FASCÍCULO 4)

FERNANDO REVILLA JIMÉNEZ

Resumen. Cada fascículo de estos *Problemas resueltos de matemáticas superiores* consta de 50 problemas resueltos. Pueden considerarse como anexos a mis libros *Problemas resueltos de álgebra* y *Problemas resueltos de análisis matemático*.

Índice

151. Completación de todo espacio métrico

Sea X un espacio métrico. Se dice que el espacio métrico X^* es una *completacion* de X si X^* es completo y X es isométrico a un subespacio denso de X^*. El objetivo de éste problema es demostrar que todo espacio métrico tiene una completación y que ésta es única salvo isometrías.

1) Sea (X, d) un espacio métrico y sea $C[X]$ el conjunto de todas las sucesiones de Cauchy en X. Se define en $C[X]$ la relación

$$(x_n) \sim (y_n) \Leftrightarrow \lim d(x_n, y_n) = 0.$$

Demostrar que $\sim$ es una relación de equivalencia en $C[X]$
2) Sean (x_n) e (y_n) dos elementos de $C[X]$. Demostrar que la sucesión de números reales $d(x_n, y_n)$ es convergente.
3) Sea el conjunto cociente $X^* = C[X]/\sim$. Se define la aplicación

$$d^* : X^* \times X^* \to \mathbb{R}, \quad d^*([x_n], [y_n]) = \lim d(x_n, y_n).$$

Demostrar que está bien definida, es decir que no depende del representante elegido en cada clase.
4) Demostrar que d^* es una distancia en X^*.
5) Para todo $p \in X$ sea la sucesión constante $(p) = (p, p, p, \ldots)$. Consideremos el subconjunto de X^*: $\hat{X} = \{[(p)] : p \in X\}$. Demostrar que X es

isométrico a $\hat{X}$. 6) Demostrar que $\hat{X}$ es denso en X^*.
7) Demostrar el siguiente lema:
Sea (M,d) un espacio métrico, (b_n) una sucesión de Cauchy en M y sea (a_n) una sucesión en M tal que $d(a_n,b_n)<1/n$ para todo n natural. Entonces,
(i) (a_n) es sucesión de Cauchy en M.
(ii) $(a_n)\to p\in M \Leftrightarrow (b_n)\to p\in M$
8) Demostrar que (X^*,d^*) es completo.
9) Demostrar que si Y^* es una completación de X, entonces Y^* es isométrico a X^*.
10) ¿Cuál es la completación de $\mathbb{Q}$ con la distancia usual?

SOLUCIÓN. 1) *Reflexiva.* Para todo $(x_n)\in C[X]$ tenemos $\lim d(x_n,x_n)=\lim 0=0$, luego $(x_n)\sim(x_n)$.
Simétrica. Para todo $(x_n),(y_n)\in C[X]$ tenemos

$$(x_n)\sim(y_n)\Rightarrow \lim d(x_n,y_n)=0\Rightarrow$$

$$\lim d(y_n,x_n)=\lim d(x_n,y_n)=0\Rightarrow (y_n)\sim(x_n).$$

Transitiva. Si $(x_n)\sim(y_n)$ e $(y_n)\sim(z_n)$ se verifica $d(x_n,y_n)\to 0$ y $d(y_n,z_n)\to 0$. Por la desigualdad triangular, $0\le d(x_n,z_n)\le d(x_n,y_n)+d(y_n,z_n)$. Por el teorema del Sandwich, $d(x_n,z_n)\to 0$ luego $(x_n)\sim(z_n)$.

2) Por la desigualdad triangular

$$d(x_n,y_n)\le d(x_n,x_m)+d(x_m,y_m)+d(y_m,y_n)$$

o bien $d(x_n,y_n)-d(x_m,y_m)\le d(x_n,x_m)+d(y_m,y_n)$ con lo cual

$$|d(x_n,y_n)-d(x_m,y_m)|\le d(x_n,x_m)+d(y_m,y_n)$$

Como las sucesiones (x_n) e (y_n) son de Cauchy, para todo $\epsilon>0$ existen naturales N_x,N_y tales que $d(x_n,x_m)<\epsilon/2$ si $n,m\ge N_x$ y $d(y_n,y_m)<\epsilon/2$ si $n,m\ge N_y$. Entonces,

$$|d(x_n,y_n)-d(x_m,y_m)|<\epsilon/2+\epsilon/2=\epsilon \text{ si } N=\max\{N_x,N_y\}.$$

Esto prueba que la sucesion de números reales $d(x_n,y_n)$ es de Cauchy y por tanto convergente al ser $\mathbb{R}$ completo.

3) Supongamos que $(x_n)\sim(x'_n)$ y que $(y_n)\sim(y'_n)$. Sea $l=\lim d(x_n,y_n)$ y $l'=\lim d(x'_n,y'_n)$. Tenemos que demostrar que $l=l'$. Por la desigualdad triangular,

$$d(x_n,y_n)\le d(x_n,x'_n)+d(x'_n,y'_n)+d(y'_n,y_n).$$

Sea ahora $\epsilon>0$. Tenemos

$$\exists n_1\in\mathbb{N}: n\ge n_1\Rightarrow d(x_n,x'_n)<\epsilon/3,$$

$$\exists n_2\in\mathbb{N}: n\ge n_2\Rightarrow d(y_n,y'_n)<\epsilon/3,$$

$$\exists n_3\in\mathbb{N}: n\ge n_3\Rightarrow \left|d(x'_n,y'_n)-l'\right|<\epsilon/3.$$

Si $n\ge\max\{n_1,n_2,n_3\}$ se verifica $d(x_n,y_n)<l'+\epsilon$ y por tanto $\lim d(x_n,y_n)=l\le l'+\epsilon$ para todo ϵ luego $l\le l'$. De manera simétrica se demuestra que

$l' \leq l$ y por tanto, $l = l'$.

4) Para todo $[(x_n)], [(y_n)] \in X^*$ tenemos $d^*\left([(x_n)], [(y_n)]\right) = \lim d(x_n, y_n)$, límite que vimos que existe y que además es ≥ 0 al ser los $d(x_n, y_n) \geq 0$. Por otra parte,

$$d^*\left([(x_n)], [(y_n)]\right) = 0 \Leftrightarrow \lim d(x_n, y_n) = 0 \Leftrightarrow (x_n) \sim (y_n) \Leftrightarrow [(x_n)] = [(y_n)].$$

Para todo $[(x_n)], [(y_n)] \in X^*$:

$$d^*\left([(x_n)], [(y_n)]\right) = \lim d(x_n, y_n) = \lim d(y_n, x_n) = d^*\left([(y_n)], [(x_n)]\right),$$

Para todo $[(x_n)], [(y_n)], [(z_n)] \in X^*$:

$$d^*\left([(x_n)], [(y_n)]\right) = \lim d(x_n, y_n) \leq \lim \left[d(x_n, z_n) + d(z_n, y_n)\right]$$

$$= \lim d(x_n, z_n) + \lim d(z_n, y_n) = d^*\left([(x_n)], [(z_n)]\right) + d^*\left([(z_n)], [(y_n)]\right).$$

Concluimos pues que d^* es distancia en X^*.

5) Para todo $p \in X$ la sucesión constante (p) es convergente y por tanto de Cauchy, con lo cual $\hat{X} \subset X^*$. Definamos la aplicación $f : X \to \hat{X}$ dada por $f(p) = [(p)]$. Tenemos,

$$f(p) = f(q) \Rightarrow [(p)] = [(q)] \Rightarrow \lim (p - q) = p - q = 0 \Rightarrow p = q$$

es decir, f es inyectiva. Por otra parte para todo $[(p)] \in \hat{X}$ se verifica $[(p)] = f(p)$, luego f es sobreyectiva. Veamos ahora que la biyección f es isometría. En efecto, para todo $p, q \in X$:

$$d^*\left([(p)], [(q)]\right) = \lim\ d(p, q) = d(p, q).$$

6) Basta demostrar que todo punto de X^* es el límite de una sucesión de elementos de $\hat{X}$. Sea pues $x = [(x_n)] \in X^*$ y denotemos por $\hat{x_1}$, $\hat{x_2}$, $\hat{x_3}, \ldots$ los elementos de $\hat{X}$:

$$\hat{x_1} = [(x_1, x_1, x_1, \ldots)],\ \hat{x_2} = [(x_2, x_2, x_2, \ldots)],\ \hat{x_3} = [(x_3, x_3, x_3, \ldots)],\ \ldots$$

Dado que (x_n) es sucesión de Cauchy en X:

$$\lim_{m \to +\infty} d^*(\hat{x_m}, x) = \lim_{m \to +\infty} \left(\lim_{n \to +\infty} d(x_m, x_n) \right) = \lim_{m,\, n \to +\infty} d(x_m, x_n) = 0$$

luego $(\hat{x}_n) \to x$.

7) (i) Por la desigualdad triangular

$$d(a_m, a_n) \leq d(a_m, b_m) + (b_m, b_n) + d(b_n, a_n).$$

Para todo $\epsilon > 0$ existe n_1 natural tal que $1/n_1 < \epsilon/3$ por tanto

$$n, m \geq n_1 \Rightarrow d(a_m, a_n) \leq \epsilon/3 + (b_m, b_n) + \epsilon/3.$$

Como (b_n) es de Cauchy, existe n_2 natural tal que si $n, m \geq n_2$ entonces $d(b_m, b_n) < \epsilon/3$. Si $n_0 = \text{máx}\{n_1, n_2\}$,

$$n, m \geq n_0 \Rightarrow d(a_m.a_n)\ \ < \epsilon/3 + \epsilon/3 + \epsilon/3 = \epsilon$$

lo cual implica que (a_n) es de Cauchy.
(ii) $\Rightarrow$) Por hipótesis $(a_n) \to p$, luego $d(a_n, p) \to 0$. Por otra parte $0 \leq d(b_n, a_n) \leq 1/n$, es decir $d(b_n, a_n) \to 0$. De la desigualdad triangular $0 \leq d(b_n, p) \leq d(b_n, a_n) + d(a_n, p)$ obtenemos usando el teorema del Sandwich que $d(b_n, p) \to 0$ o de forma equivalente $(b_n) \to p$.
$\Leftarrow$) Se demuestra de manera análoga.

8) Sea (α_n) una sucesión de Cauchy en X^*. Tenemos que demostrar que converge en X^*. Como $\hat{X}$ es denso en X^*, para todo n natural existe $\hat{x_n} \in \hat{X}$ tal que $d^*(\hat{x_n}, \alpha_n) < 1/n$. Por la parte (i) del apartado anterior, la sucesión $(\hat{x_n})$ es también de Cauchy en X^* con lo cual lo será (x_n) en X por ser X y $\hat{X}$ isométricos. Por el apartado 6, $(\hat{x_n}) \to x \in X^*$ y por la parte (ii) del apartado anterior también $(\alpha_n) \to x$.

9) Sea Y^* una completación de X. Al ser X isométrico a un subespacio denso de Y^*, podemos asumir que X es subespacio de Y^*. Al ser X denso en Y^*, para todo $y \in Y^*$ existe una sucesión (x_n) de X que converge a y con lo cual (x_n) es de Cauchy. Definamos la aplicación

$$g : Y^* \to X^*, \quad g(y) = [(x_n)].$$

La aplicación está bien definida pues si (x'_n) es otra sucesión tal que $(x'_n) \to y$, entonces $d(x_n, x'_n) \to 0$ y por tanto $[(x'_n)] = [(x_n)]$. Sean ahora $y, y' \in Y^*$ con $(x_n) \to y$, $(x'_n) \to y'$. Entonces,

$$g(y) = g(y') \Rightarrow [(x_n)] = [(x'_n)] \Rightarrow \lim\, d(x_n, x'_n) = 0 \Rightarrow y = y'$$

luego g es inyectiva. También es sobreyectiva. En efecto, si $[(x_n)] \in X^*$ la sucesión (x_n) es de Cauchy en $X \subset Y^*$ por tanto (x_n) converge a un $y \in Y^*$, luego $[(x_n)] = g(y)$. Por último, para todo $y, y' \in Y^*$

$$\begin{aligned} d^*\left(f(y), f(y')\right) &= d^*\left([(x_n)], [(x'_n)]\right) = \lim d(x_n, x'_n) \\ &= d\left(\lim x_n, \lim x'_n\right) = d(y, y') \end{aligned}$$

es decir, g es isometría.

10) De la conocida construcción de los números reales vía sucesiones de Cauchy racionales, deducimos que la completación de $\mathbb{Q}$ es $\mathbb{Q}^* = \mathbb{R}$. □

152. Álgebras uniformemente densas, teorema Stone-Weierstrass

Sea X un espacio topológico compacto y $C(X)$ el espacio vectorial de las funciones reales continuas $f : X \to \mathbb{R}$ con la norma de la convergencia uniforme

$$\|f\|_\infty = \max\{|f(x)| : x \in X\}.$$

Es claro que una sucesión f_n de $C(X)$ converge uniformemente a $f \in C(X)$ si y sólo si f_n converge a f con la norma anterior. El teorema de Stone-Weierstrass asegura que si $\mathcal{F}$ es un álgebra de $C(X)$ que separa puntos y

contiene a las funciones constantes, entonces es uniformemente densa en $C(X)$ (es decir, es densa con la norma de la convergencia uniforme).
Esto, naturalmente equivale a decir que para toda función $f \in C(X)$ existe una sucesión f_n en $\mathcal{F}$ tal que $f_n \to f$ uniformemente. Se pide:

1) Demostrar que el conjunto $\mathbb{R}[x]$ de las funciones polinómicas es familia uniformemente densa en $C([a,b])$. Concluir.
2) Ídem para $K \subset \mathbb{R}^n$ compacto y la familia $\mathcal{F} = \mathbb{R}[x_1, \ldots, x_n]$ de las funciones polinómicas.
3) Demostrar que el subespacio vectorial de $C[0,1]$ generado por las funciones $\{e^{nx} : n \in \mathbb{Z}\}$ es uniformemente densa en $C[0,1]$.
4) Demostrar que el teorema de Stone-Weirstrass es aplicable al intervalo $[a,b]$ con

$$\mathcal{F} = \text{Lip } ([a,b]) = \{f : [a,b] \to \mathbb{R} \text{ con } f \text{ lipschitziana}\}.$$

SOLUCIÓN. 1) Recordamos que si A y B son conjuntos y $\mathcal{F}$ es una familia de funciones de A en B, se dice que $\mathcal{F}$ separa puntos si para cada par de elementos $x, y \in A$ con $x \neq y$ existe $f \in \mathcal{F}$ tal que $f(x) \neq f(y)$.
El intervalo $[a,b]$ es compacto, $\mathbb{R}[x]$ es un álgebra de $C([a,b])$ y contiene a las funciones constantes. Por otra parte si $\alpha, \beta \in [a,b]$ con $\alpha \neq \beta$ el polinomio $p(x) = x$ satisface $p(\alpha) \neq p(\beta)$. Por el teorema de Stone-Weierstrass $\mathbb{R}[x]$ es álgebra uniformemente densa en $C([a,b])$. Concluimos que para toda función continua f en $[a,b]$ existe una sucesión de polinomios p_n tales que $p_n \to f$ en $[a,b]$ uniformemente.
Nota. Este caso particular del teorema de Stone-Weierstrass se conoce como *Teorema de Weierstrass.*

2) De nuevo, K es compacto por hipótesis, $\mathbb{R}[x_1, \ldots, x_n]$ es un álgebra de $C(K)$ y contiene a las funciones constantes. Por otra parte si $\alpha, \beta \in K$ con

$$\alpha = (\alpha_1, \ldots, \alpha_n) \neq \beta = (\beta_1, \ldots, \beta_n),$$

existe k tal que $\alpha_k \neq \beta_k$. Eligiendo $p(x_1, \ldots, x_n) = x_k$, obtenemos $p(\alpha) \neq p(\beta)$, i.e. $\mathbb{R}[x_1, \ldots, x_n]$ es familia uniformemente densa en $C(K)$.

3) El subespacio vectorial $\mathcal{F}$ generado por $\{e^{nx} : n \in \mathbb{Z}\}$ está formado por las funciones de la forma

$$f : [0,1] \to \mathbb{R}, \quad f(x) = \lambda_1 e^{n_1 x} + \lambda_2 e^{n_2 x} + \cdots + \lambda_m e^{n_m x} \quad (\lambda_i \in \mathbb{R}, n_i \in \mathbb{Z}).$$

$\mathcal{F} \subset C[0,1]$ pues las funciones de $\mathcal{F}$ son continuas. Es fácil demostrar que forman un álgebra. Contiene a las funciones constantes pues $f(x) = C = Ce^{0x} \in \mathcal{F}$. Por último, si $\alpha, \beta \in [0,1]$ con $\alpha \neq \beta$ entonces, $f(x) = e^x = 1e^{1x} \in \mathcal{F}$ y $f(\alpha) = e^\alpha \neq e^\beta = f(\beta)$. Concluimos que $\mathcal{F}$ es uniformemente densa en $C([0,1])$.

4) (i) Lip $[a,b]$ *es subespacio vectorial de* $C[a,b]$. En efecto, sabemos que toda función lipschitziana es uniformemente continua y por tanto continua, luego Lip $[a,b] \subset C[a,b]$. La función nula es claramente lipschitziana. Además, para todo $x, y \in [a,b]$:

$$f, g \in \text{Lip } [a,b] \Rightarrow \begin{cases} \exists k_1 > 0 : |f(x) - f(y)| \leq k_1 |x-y| \\ \exists k_2 > 0 : |g(x) - g(y)| \leq k_2 |x-y| \end{cases}$$

$$\Rightarrow |(f+g)(x) - (f+g)(y)| = |f(x) + g(x) - f(y) - g(y)|$$

$$\leq |f(x) - f(y)| + |g(x) - g(y)| = (k_1 + k_2)|x-y| \Rightarrow f + g \in \text{Lip } [a,b].$$

$$\lambda \in \mathbb{R},\ f \in \text{Lip } [a,b] \Rightarrow \exists k > 0 : |f(x) - f(y)| \leq k |x-y|$$

$$\Rightarrow |(\lambda f)(x) - (\lambda f)(y)| = |\lambda f(x) - \lambda f(y)| = |\lambda|\,|f(x) - f(y)|$$

$$\leq k |\lambda| |x-y| \Rightarrow \lambda f \in \text{Lip } [a,b].$$

(ii) Lip $[a,b]$ *es subanillo de* $C[a,b]$. En efecto, $\emptyset \neq$ Lip $[a,b] \subset C[a,b]$. Además, para todo $x, y \in [a,b]$:

$$f, g \in \text{Lip } [a,b] \Rightarrow \begin{cases} \exists k_1 > 0 : |f(x) - f(y)| \leq k_1 |x-y| \\ \exists k_2 > 0 : |g(x) - g(y)| \leq k_2 |x-y| \end{cases}$$

$$\Rightarrow |(f-g)(x) - (f-g)(y)| = |f(x) - g(x) - f(y) + g(y)|$$

$$\leq |f(x) - f(y)| + |g(x) - g(y)| = (k_1 + k_2)|x-y| \Rightarrow f - g \in \text{Lip } [a,b].$$

Si f, g son lispschitzianas en $[a,b]$, son continuas en $[a,b]$ y por tanto están acotadas, es decir existe $M > 0$ tal que $|f| \leq M$ y $|g| \leq M$. Entonces,

$$f, g \in \text{Lip } [a,b] \Rightarrow |(fg)(x) - (fg)(y)| = |f(x)g(x) - f(y)g(y)|$$

$$\leq |f(x)g(x) - f(x)g(y)| + |f(x)g(y) - f(y)g(y)|$$

$$\leq M\,(|g(x) - g(y)| + |f(x) - f(y)|) \leq M(k_1 + k_2)|x-y| \Rightarrow fg \in \text{Lip } [a,b].$$

Lip $[a,b]$ es por tanto subanillo de $C[a,b]$ (además, conmutativo y unitario).

Ahora, para todo $\lambda \in \mathbb{R}$ y para todo par de funciones $f, g \in$ Lip $[a,b]$ se verifica $\lambda(fg) = (\lambda f)g = f(\lambda g)$ con lo cual podemos concluir que Lip $[a,b]$ es un álgebra. Claramente contiene a las funciones constantes y separa puntos pues $id \in$ Lip $[a,b]$ e $id(\alpha) \neq id(\beta)$ si $\alpha \neq \beta$. Esto completa la demostración de que se verifican las hipótesis del teorema de Stone-Weierstrass y en consecuencia Lip $[a,b]$ es álgebra uniformemente densa en $C[a,b]$. $\square$

153. Teorema de Wedderburn

A lo largo de éste problema la letra K designará un cuerpo finito y no necesariamente conmutativo. Si A es un conjunto, denotamos por $|A|$ al cardinal de A. Se trata de demostrar el teorema de Wedderburn i.e. que todo cuerpo finito es conmutativo.

1) Sea $k \subset K$ un subcuerpo propio y conmutativo de K.
(i) Demostrar que la dimensión de K como k-espacio vectorial es finita y mayor o igual que 2
(ii) Demostrar existe un entero $n \geq 2$ tal que $|K| = |k|^n$.
2) Sea $s \in K$. Definimos el *centralizador* de s como

$$C_s = \{x \in K : xs = sx\}$$

es decir, como el conjunto de los elementos de K que conmutan con s. Demostrar que C_s es subcuerpo de K.
3) El *centro* de K se define como

$$Z = \{a \in K : ax = xa \ \forall x \in K\}$$

es decir, es el conjunto de los elementos de K que conmutan con todos los de K. Demostrar que Z es subcuerpo conmutativo de K.
Nota. Obsérvese que el teorema de Wedderburn quedaría demostrado si demostramos que $Z = K$.
4) Sea $|Z| = q$. Demostrar que $|K| = q^n$ y que $|C_s| = q^{n_s}$ para ciertos enteros positivos n, n_s. Demostrar que si además K no es conmutativo, existe $s \in K$ tal que $n_s < n$.
5) Definimos en $K^* = K \setminus \{0\}$ la relación

$$u \sim v \Leftrightarrow u = x^{-1}vx \text{ para algún } x \in K^*.$$

Demostrar que $\sim$ es relación de equivalencia en K^* y determinar sus clases de equivalencia.
6) Demostrar que $|[s]| = 1 \Leftrightarrow s \in Z$, y que si K no es conmutativo existe al menos una clase tal que $|[s]| \geq 2$.
7) Para $s \in K^*$ denotamos $C_s^* = C_s \setminus \{0\}$ y $C_s^* x = \{zx : z \in C_s^*\}$. Se considera la aplicación

$$f_s : K^* \to [s], \quad f_s(x) = x^{-1}sx.$$

Demostrar que $f_s(x) = f_s(y)$ si y sólo si, $y \in C_s^* x$. Aplicar éste resultado para demostrar que

$$\frac{|K^*|}{|C_s^*|} = \frac{q^n - 1}{q^{n_s} - 1} = |[s]|$$

en donde q, n y n_s tienen los mismos significados que en el apartado 4.
8) Sea K no conmutativo y llamemos $Z^* = Z \setminus \{0\}$. Sean $[s_1], \ldots, [s_m]$ las clases que tienen más de un elemento (vimos que existen si K no conmutativo).

Demostrar la fórmula

$$q^n - 1 = q - 1 + \sum_{k=1}^{m} \frac{q^n - 1}{q^{n_k} - 1} \text{ con } 1 < \frac{q^n - 1}{q^{n_k} - 1} \in \mathbb{N} \ \forall k = 1, \ldots, m.$$

9) Sea K no conmutativo. Demostrar que $n_k \mid n$ para todo $k = 1, \ldots, m$.
10) Sea $\xi = e^{2\pi i/n}$ y $U_n = \{1, \xi, \xi^2, \ldots, \xi^{n-1}\}$ el grupo cíclico multiplicativo de las raíces enésimas de la unidad. Si $\lambda \in U_n$ definimos ord λ (orden de λ) como el menor entero positivo d tal que $\lambda^d = 1$. Por el teorema de Lagrange, necesariamente $d \mid n$. Para todos los divisores positivos d de n definimos los polinomios:

$$\phi_d(x) := \prod_{\text{ord } \lambda = d} (x - \lambda) \text{ con lo cual, } x^n - 1 = \prod_{d \mid n} \phi_d(x).$$

(i) Descomponer $x^6 - 1$ como producto de los polinomios $\phi_d(x)$ con $d \mid 6$.
(ii) Demostrar que para todo n el polinomio $\phi_n(x)$ tiene coeficientes enteros (i.e. $\phi_n(x) \in \mathbb{Z}[x]$) y que su término constante es 1 0 -1.
11) Demostrar que si K no es conmutativo, entonces $\phi_n(q) \mid q - 1$.
12) Demostrar el teorema de Wedderburn: todo cuerpo finito es conmutativo.

SOLUCIÓN. 1) (i) Al ser k conmutativo, claramente K es espacio vectorial sobre el cuerpo k, y por ser K finito la dimensión de K es finita. Si $a \in K$ y $a \notin k$ el sistema $S = \{1, a\}$ es libre. En efecto, si $\lambda_1 1 + \lambda_2 a = 0$ con $\lambda_1, \lambda_2 \in k$ han de ser nulos los escalares λ_1 y λ_2. Si fuera $\lambda_2 \neq 0$, entonces

$$\lambda_1 1 + \lambda_2 a = 0 \Rightarrow \lambda_2 a = -\lambda_1 \Rightarrow a = \lambda_2^{-1}(-\lambda_1).$$

Entonces, $a = \lambda_2^{-1}(-\lambda_1)$ pertenecería a k en contradicción con la hipótesis. Necesariamente $\lambda_2 = 0$ y por ende, $\lambda_1 = -0a = 0$. Concluimos pues que $\dim K \geq 2$ y finita.
(ii) Sea $\dim K = n$, que según el apartado anterior es ≥ 2 y finita. Al ser K isomorfo a k^n, se verifica $|K| = |k^n| = |k|^n$.

2) Claramente 0 y 1 pertenecen a C_s. Por otra parte,

$$x, y \in C_s \Rightarrow (x - y)s = xs - ys = sx - sy = s(x - y) \Rightarrow x - y \in C_s,$$

$$x, y \in C_s \Rightarrow (xy)s = x(ys) = x(sy) = (xs)y = (sx)y = s(xy) \Rightarrow xy \in C_s,$$

$$0 \neq x \in C_s \Rightarrow xs = sx \Rightarrow s = x^{-1}sx \Rightarrow sx^{-1} = x^{-1}s \Rightarrow x^{-1} \in C_s$$

es decir, C_s es subcuerpo de K.

3) Tenemos que $Z = \bigcap_{s \in K} C_s$ y la intersección de subcuerpos es subcuerpo. Además, Z es conmutativo por su propia definición.

4) Dado que Z es subcuerpo conmutativo tanto de C_s como de K, podemos considerar a C_s y a K como espacios vectoriales sobre Z. Si $\dim C_s = n_s$ entonces, $n_s \geq 1$ por ser $\{1\}$ sistema libre y $C_s \cong Z^{n_s}$ es decir $|C_s| = q^{n_s}$. De manera análoga, si $\dim K = n$ entonces $|K| = q^n$ con $n \geq 1$. Nótese que

según el apartado primero, sería $n \geq 2$ si $Z \subsetneq K$.

5) Para todo $u \in K^*$ se verifica $u = 1^{-1}u1$ es decir, $u \sim u$. Si $u \sim v$ entonces $u = x^{-1}vx$ lo cual implica $v = xux^{-1} = (x^{-1})^{-1}ux^{-1}$, luego $v \sim u$. Sean ahora $u, v, w \in K^*$. Entonces

$$\begin{cases} u \sim v \\ v \sim w \end{cases} \Rightarrow \begin{cases} u = x^{-1}vx \\ v = y^{-1}wy \end{cases} \Rightarrow u = x^{-1}y^{-1}wyx = (yx)^{-1}w(yx) \Rightarrow u \sim w.$$

Concluimos que $\sim$ es relación de equivalencia en K^*. Si $s \in K^*$, la clase de equivalencia a la que pertenece s es

$$[s] = \{u \in K^* : u \sim s\} = \{u \in K^* : u = x^{-1}sx \text{ con } x \in K^*\}$$

$$= \{x^{-1}sx : x \in K^*\}.$$

6) $\Rightarrow$) Si el cardinal de $[s]$ es 1, entonces $[s] = \{s\}$ y por tanto $s = x^{-1}sx$ para todo $x \in K^*$, luego $xs = sx$ para todo $x \in K^*$ y por supuesto para todo $x \in K$ con lo cual $s \in Z$.
$\Leftarrow$) Si $s \in Z$ entonces $sx = xs$ para todo $x \in K$, por tanto

$$[s] = \{x^{-1}sx : x \in K^*\} = \{x^{-1}xs : x \in K^*\} = \{s\} \Rightarrow |[s]| = 1.$$

Si K no es conmutativo existe $s \in K$ tal que $s \notin Z$ por tanto $\emptyset \neq [s]$ no tiene cardinal 1, es decir $|[s]| \geq 2$.

7) Para todo $x, y \in K^*$ se verifica

$$f_s(x) = f_s(y) \Leftrightarrow x^{-1}sx = y^{-1}sy \Leftrightarrow \left(yx^{-1}\right)s = s\left(yx^{-1}\right)$$

$$\Leftrightarrow yx^{-1} \in C_s^* \Leftrightarrow y \in C_s^*x.$$

Claramente $|C_s^*x| = |C_s^*|$ pues x es invertible. Cada elemento $f_s(x) = x^{-1}sx$ de $[s]$ es la imagen de los $y \in K^*$ tales que $y \in C_s^*$ es decir es la imagen de $|C_s^*x| = |C_s^*|$ elementos de K^*, luego $|K^*| = |[s]|\,|C_s^*|$. Es decir

$$\frac{|K^*|}{|C_s^*|} = \frac{q^n - 1}{q^{n_s} - 1} = |[s]| \quad \forall s \in K^*.$$

8) Tenemos $|K^*| = q^n - 1$, $|Z^*| = q - 1$ y $|C_s^*| = q^{n_s} - 1$. Las clases de equivalencia de $\sim$ en K^* forman una partición de K^* y tenemos $|K^*|$ clases de equivalencia con un elemento y m clases $[s_1], \ldots, [s_m]$ con $q^{n_1}, \ldots, q^{n_m}$ elementos respectivamente, con lo cual $|K^*| = |Z^*| + \sum_{k=1}^{m} \left|C_{s_k}^*\right|$ y usando el apartado anterior queda

$$q^n - 1 = q - 1 + \sum_{k=1}^{m} \frac{q^n - 1}{q^{n_k} - 1}.$$

Por otra parte, para toda clase $[s_k]$ con $k = 1, \ldots, m$ se verifica $1 < |[s_k]| \in \mathbb{N}$ con lo cual,

$$1 < |[s_k]| = \frac{q^n - 1}{q^{n_k} - 1} \in \mathbb{N}.$$

9) Podemos escribir $n = an_k + r$ con $0 \leq r < n_k$ y para todo k se verifica $q^{n_k} - 1 \mid q^n - 1$. Entonces,

$$q^{n_k} - 1 \mid q^n - 1 \Rightarrow q^{n_k} - 1 \mid q^{an_k+r} - 1 \Rightarrow$$

$$q^{n_k} - 1 \mid \left(q^{an_k+r} - 1\right) - \left(q^{n_k} - 1\right) = q^{n_k}\left(q^{(a-1)n_k+r} - 1\right).$$

Dado que q^{n_k} y $q^{n_k} - 1$ son relativamente primos, se verifica $q^{n_k} - 1 \mid q^{(a-1)n_k+r} - 1$, y continuando de esta manera llegaríamos a que $q^{n_k} - 1 \mid q^r - 1$ con $0 \leq r < n_k$ que sólo puede ocurrir si $r = 0$, luego $n = an_k$. Es decir, $n_k \mid n$.

10) (i) Tenemos $U_6 = \{1, \xi, \xi^2, \xi^3, \xi^4, \xi^5\}$. Los mínimos exponentes positivos d que corresponden a cada raíz son

$$1^1 = 1,\ \xi^6 = 1,\ (\xi^2)^3 = 1,\ (\xi^3)^2 = 1,\ (\xi^4)^3 = 1,\ (\xi^5)^6 = 1,$$

luego los polinomios $\phi_d(x)$ son

$$\phi_1(x) = x - 1, \quad \phi_2(x) = (x - \xi^3),$$
$$\phi_3(x) = (x - \xi^2)(x - \xi^4), \quad \phi_6(x) = (x - \xi)(x - \xi^5),$$

y queda $x^6 - 1 = \phi_1(x)\phi_2(x)\phi_3(x)\phi_6(x)$.
(ii) Se verifica $\phi_1(x) = x - 1$ y procedamos por inducción. Supongamos que $\phi_d(x) \in \mathbb{Z}[x]$ para todo $d < n$ y que sus coeficientes constantes son 1 o -1. Por la descomposición $x^n - 1 = \prod_{d|n} \phi_d(x)$:

$$x^n - 1 = p(x)\phi_n(x) \ \text{ con } \ p(x) = \sum_{i=0}^{l} a_i x^i,\ \phi_n(x) = \sum_{j=0}^{n-l} b_j x^j$$

con los a_i enteros y $a_0 = 1$ o $a_0 = -1$. Dado que $-1 = a_0 b_0$, se verifica $b_0 = 1$ o $b_0 = -1$. Supongamos ahora que $b_0, b_1, \ldots, b_{k-1} \in \mathbb{Z}$. Igualando coeficientes de x^k en ambos miembros de $x^n - 1 = \prod_{d|n} \phi_d(x)$:

$$\sum_{i=0}^{k} a_i b_{k-i} = \sum_{i=1}^{k} a_i b_{k-i} + a_0 b_k \in \mathbb{Z}.$$

Por hipótesis $b_0, b_1 \ldots, b_{k-1}$ son enteros, y también lo son todos los a_i. Dado que a_0 es 1 o -1, también es entero b_k.

11) Si $n_k \mid n$ es uno de los números que aparecen en el apartado 4, se verifica:

$$x^n - 1 = \prod_{d|n} \phi_d(x) = \left(x^{n_k} - 1\right) \phi_n(x) \prod_{d|n,\ d\nmid n_k\ d\neq n} \phi_d(x).$$

En consecuencia y para $q = |K|$ se verifican las relaciones de divisibilidad en $\mathbb{Z}$:

$$\phi_n(q) \mid q^n - 1 \quad y \quad \phi_n(q) \mid \frac{q^n - 1}{q^{n_k} - 1}.$$

Por la fórmula demostrada en el apartado 8 para todo n_k:

$$q^n - 1 = q - 1 + \sum_{k=1}^{m} \frac{q^n - 1}{q^{n_k} - 1},$$

deducimos que $\phi_n(q) \mid q - 1$.

12) Supongamos que K no es conmutativo. Entonces $Z \subsetneq K$ y por el apartado 1, $n > 1$. Sabemos que $\phi_n(x) = \prod(x - \lambda)$ en donde λ recorre todas las raíces de orden n. Al ser $n > 1$, $\lambda = a + bi \neq 1$ y la parte real a de λ claramente satisface $a < 1$. Entonces,

$$|q - \lambda|^2 = |q - a - bi|^2 = (q - a)^2 + b^2 = q^2 - 2aq + a^2 + b^2$$
$$= q^2 - 2aq + 1 \underbrace{>}_{a<1} q^2 - 2q + 1 = (q - 1)^2.$$

Es decir, se verifica $|q - \lambda| > q - 1$ para toda λ de orden n. Esto implica

$$|\phi_n(q)| > \prod_{\text{ord } \lambda = n} |q - \lambda| > q - 1.$$

Pero esto contradice la relación $\phi_n(q) \mid q - 1$ demostrada en el apartado anterior. Concluimos que K ha de ser necesariamente conmutativo y queda demostrado el teorema de Wedderburn. □

154. Un espacio vectorial no usual

Sea el conjunto $H = \mathbb{R} \times \mathbb{R}_{>0}$.

1) Demostrar que $(H, \oplus)$ es grupo abeliano, estando $\oplus$ definida mediante

$$(x, y) \oplus (z, w) = (x + z - 2, yw).$$

2) Demostrar que la operación

$$\mathbb{R} \times H \to H, \quad \lambda \otimes (x, y) = (\lambda x - 2\lambda + 2, y^\lambda)$$

dota al grupo abeliano H del apartado anterior, de estructura de espacio vectorial sobre el cuerpo $\mathbb{R}$.

solución. 1) *Interna.* Dado que para todo $(x, y), (z, w) \in H$, se verifica $x, z \in \mathbb{R}$, también $x + z - 2 \in \mathbb{R}$. Al ser $y, w \in \mathbb{R}_{>0}$ también $yw \in \mathbb{R}_{>0}$ y por tanto, $(x, y) \oplus (z, w) \in H$.
Asociativa. Para todo $(x, y), (z, w), (u, v) \in H$ tenemos

$$(x, y) \oplus [(z, w) \oplus (u, v)] = (x, y) \oplus (z + u - 2, wv) = (x + z + u - 4, ywu),$$

$$[(x, y) \oplus (z, w)] \oplus (u, v) = (x + z - 2, yw) \oplus (u, v) = (x + z + u - 4, ywu).$$

Se verifica la igualdad.
Elemento neutro. El par (a, b) es elemento neutro en H si y sólo si para todo $(x, y) \in H$ se verifica

$$(x, y) \oplus (a, b) = (a, b) \oplus (x, y) = (x, y)$$

o equivalentemente $(x+a-2, yb) = (a+x-2, by) = (x, y)$. Es claro que $(a, b) = (2, 1) \in H$ y satisface la relación anterior para todo $(x, y) \in H$. Es por tanto el elemento neutro de H.
Elemento simétrico. El elemento $(x', y') \in H$ es simétrico de $(x, y) \in H$ si y sólo si se verifica

$$(x, y) \oplus (x', y') = (x', y') \oplus (x, y) = (2, 1)$$

o equivalentemente $(x + x' - 2, yy') = (x' + x - 2, y'y) = (2, 1)$. Es claro que $(x', y') = (4 - x, 1/y)$ es elemento de H y satisface la relación anterior.
Conmutativa. Para todo $(x, y), (z, w) \in H$ tenemos

$$(x, y) \oplus (z, w) = (x + z - 2, yw) = (z + x - 2, wy) = (z, w) \oplus (x, y).$$

Concluimos pues que $(H, \oplus)$ es grupo abeliano.

2) Para todo $\lambda, x \in \mathbb{R}$ se verifica $\lambda x - 2\lambda + 2 \in \mathbb{R}$ y para todo $y \in \mathbb{R}_{>0}$ existe $y^\lambda > 0$. Es decir, $\lambda \otimes (x, y) \in H$ está bien definida. Veamos ahora que se cumplen los cuatro axiomas de ley externa para espacios vectoriales.
(i) Para todo $\lambda \in \mathbb{R}$ y para todo $(x, y), (z, w) \in H$ tenemos

$$\lambda \otimes [(x, y) \oplus (z, w)] = \lambda \otimes (x + z - 2, yw) = \left(\lambda x + \lambda z - 2\lambda - 2\lambda + 2, (yw)^\lambda\right).$$

Por otra parte,

$$[\lambda \otimes (x, y)] \oplus [\lambda \otimes (z, w)] = (\lambda x - 2\lambda + 2, y^\lambda) \oplus (\lambda z - 2\lambda + 2, w^\lambda)$$

$$= (\lambda x - 2\lambda + 2 + \lambda z - 2\lambda + 2 - 2, y^\lambda w^\lambda) = \left(\lambda x + \lambda z - 4\lambda + 2, (yw)^\lambda\right).$$

Se verifica la igualdad.
(ii) Para todo $\lambda, \mu \in \mathbb{R}$ y para todo $(x, y) \in H$ tenemos

$$(\lambda + \mu) \otimes (x, y) = \left((\lambda + \mu)x - 2(\lambda + \mu) + 2, y^{\lambda+\mu}\right).$$

Por otra parte,

$$[\lambda \otimes (x, y)] \oplus [\mu \otimes (x, y)] = \left(\lambda x - 2\lambda + 2, y^\lambda)\right) \oplus (\mu x - 2\mu + 2, y^\mu)$$

$$= (\lambda x - 2\lambda + 2 + \mu x - 2\mu + 2 - 2, y^\lambda y^\mu).$$

Se verifica la igualdad.
(iii) Para todo $\lambda, \mu \in \mathbb{R}$ y para todo $(x, y) \in H$ tenemos

$$\lambda \otimes [\mu \otimes (x, y)] = \lambda \otimes (\mu x - 2\mu + 2, y^\mu) = \left(\lambda(\mu x - 2\mu + 2) - 2\lambda + 2, (y^\mu)^\lambda\right).$$

Por otra parte,

$$(\lambda\mu) \otimes (x, y) = \left((\lambda\mu)x - 2(\lambda\mu) + 2, y^{\lambda\mu}\right).$$

Se verifica la igualdad.
(iv) Para todo $(x, y) \in H$ se verifica

$$1 \otimes (x, y) = (1x - 2 \cdot 1 + 2, y^1) = (x, y).$$

Concluimos que H es espacio vectorial sobre el cuerpo $\mathbb{R}$ con las operaciones dadas. □

155. Espacio vectorial de las matrices circulantes

Sea $T : \mathbb{C}^n \to \mathbb{C}^n$ dada por $T(x_0, x_1, \ldots, x_{n-1}) = (x_{n-1}, x_0, \ldots, x_{n-2})$. Se llama matriz *circulante* de orden n determinada por $x = (x_0, x_1, \ldots, x_{n-1})$ y la representamos por $\text{circ}\{x\}$, a la matriz cuyos filas en el orden natural son $v, T(v), \ldots, T^{n-1}(x)$, es decir

$$\text{circ } \{x\} = \begin{bmatrix} x \\ T(x) \\ \vdots \\ T^{n-1}(x) \end{bmatrix}$$

1) Escribir de forma explícita una matriz circulante genérica.
2) Sea $\text{Circ}(n) = \{\text{circ}\{x\} : x \in \mathbb{C}^n\}$ el conjunto de todas las matrices circulantes de orden n. Demostrar que es subespacio vectorial de $\mathbb{C}^{n\times n}$.
3) Demostrar que la aplicación $\Phi : \mathbb{C}^n \to \text{Circ}(n)$ dada por $\Phi(x) = \text{circ}\{x\}$ es isomorfismo de espacios vectoriales.
4) Hallar la dimensión y una base de $\text{Circ}(n)$. Escribir explícitamente esta base para $n = 3$.

solución. 1) Una matriz circulante genérica es

$$\text{circ } \{x\} = \begin{bmatrix} x \\ T(x) \\ \vdots \\ T^{n-2}(x) \\ T^{n-1}(x) \end{bmatrix} = \begin{bmatrix} x_0 & x_1 & \ldots & x_{n-2} & x_{n-1} \\ x_{n-1} & x_0 & \ldots & x_{n-3} & x_{n-2} \\ \vdots & & & \vdots & \\ x_2 & x_3 & \ldots & x_0 & x_1 \\ x_1 & x_2 & \ldots & x_{n-1} & x_0 \end{bmatrix} \in \mathbb{C}^{n\times n}.$$

2) Se verifica $0 = \text{circ}\{0\} \in \text{Circ}(n)$. Por otra parte y para todo $\lambda \in \mathbb{C}$ y para todo par de matrices $\text{circ}\{x\}$, $\text{circ}\{y\}$ de $\text{Circ}(n)$:

$$\text{circ}\{x\} + \text{circ}\{y\} = \text{circ}\{x + y\} \in \text{Circ}(n), \quad \lambda\text{circ}\{x\} = \text{circ}\{\lambda x\} \in \text{Circ}(n),$$

por tanto $\text{Circ}(n)$ es subespacio de $\mathbb{C}^{n\times n}$.

3) Para todo $\lambda \in \mathbb{C}$ y para todo $x, y \in \mathbb{C}$ se verifica

$$\Phi(x + y) = \text{circ}\{x + y\} = \text{circ}\{x\} + \text{circ}\{y\} = \Phi(x) + \Phi(y),$$
$$\Phi(\lambda x) = \text{circ}\{\lambda x\} = \lambda\text{circ}\{x\} = \lambda\Phi(\lambda x).$$

Por tanto, Φ es lineal. Es inyectiva pues

$$\ker \Phi = \{x \in \mathbb{C}^n : \Phi(x) = 0\} = \{x \in \mathbb{C}^n : \text{circ}\{x\} = 0\} = \{0\}.$$

Por otra parte, Φ es sobreyectiva por su propia construcción. Concluimos que Φ es isomorfismo.

4) Al ser Φ isomorfismo, $\dim \mathrm{Circ}(n) = \dim \mathbb{C}^n = n$ y como los isomorfismos transforman bases en bases, si $B_c = \{e_0, e_1, \ldots, e_{n-1}\}$ es la base canónica de $\mathbb{C}^n$ una base de $\mathrm{Circ}(n)$ es $B_{\mathrm{Circ}(n)} = \{\Phi(e_0), \Phi(e_1), \ldots, \Phi(e_{n-1})\}$. Para $n = 3$, los vectores de una base de $\mathrm{Circ}(3)$ son

$$\Phi(e_0) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \ \Phi(e_1) = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}, \ \Phi(e_2) = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}.$$

□

156. Probabilidad de la unión de n sucesos

Sea (E, Ω, p) un espacio de probabilidad. Se trata de demostrar la fórmula:

$$p\left(A_1 \cup \ldots \cup A_n\right) = \sum_{i=1}^{n} p\left(A_i\right) - \sum_{i,j=1,\, i<j}^{n} p\left(A_i \cap A_j\right) +$$

$$\sum_{i,j,k=1,\, i<j<k}^{n} p\left(A_i \cap A_j \cap A_k\right) + \ldots + (-1)^{n+1} p\left(A_1 \cap A_2 \cap \ldots \cap A_n\right),$$

para $A_1, \ldots, A_n \in \Omega$. Se pide:
1) Demostrar la fórmula para $n = 2$.
2) Demostrar la fórmula para $n = 3$.
3) Usando el método de inducción, demostrar que la fórmula es válida para todo $n \geq 2$.

solución. 1) Tenemos

$$A_1 = A_1 \cap E = A_1 \cap (A_2 \cup A_2^c) = (A_1 \cap A_2) \cup (A_1 \cap A_2^c),$$

$$A_2 = A_2 \cap E = A_2 \cap (A_1 \cup A_1^c) = (A_1 \cap A_2) \cup (A_2 \cap A_1^c).$$

Además, A_1 está expresado como unión de los sucesos incompatibles $A_1 \cap A_2$ y $A_1 \cap A_2^c$ y por tanto,

$$p\left(A_1\right) = p\left(A_1 \cap A_2\right) + p\left(A_1 \cap A_2^c\right). \qquad [1]$$

De la misma manera,

$$p\left(A_2\right) = p\left(A_1 \cap A_2\right) + p\left(A_2 \cap A_1^c\right). \qquad [2]$$

Por otra parte,

$$A_1 \cup A_2 = (A_1 \cap A_2) \cup (A_1 \cap A_2^c) \cup (A_2 \cap A_1^c)$$

está expresado como unión de tres sucesos incompatibles y por tanto,

$$p\left(A_1 \cup A_2\right) = p\left(A_1 \cap A_2\right) + p\left(A_1 \cap A_2^c\right) + p\left(A_2 \cap A_1^c\right). \qquad [3]$$

Sumando miembro a miembro [1] y [2] y pasando un $p\left(A_1 \cap A_2\right)$ al primer miembro

$$p\left(A_1\right) + p\left(A_2\right) - p\left(A_1 \cap A_2\right) = p\left(A_1 \cap A_2\right) + p\left(A_1 \cap A_2^c\right) + p\left(A_2 \cap A_1^c\right),$$

y usando la igualdad [3] queda

$$p\left(A_1 \cup A_2\right) = p\left(A_1\right) + p\left(A_2\right) - p\left(A_1 \cap A_2\right) = \sum_{i=1}^{2} p\left(A_i\right) + (-1)^{2+1} p\left(A_1 \cap A_2\right).$$

2) Usando la fórmula deducida en el apartado anterior,

$$\begin{gathered}
p\left(A_1 \cup A_2 \cup A_3\right) = p\left[A_1 \cup \left(A_2 \cup A_3\right)\right] = \\
p\left(A_1\right) + p\left(A_2 \cup A_3\right) - p\left[A_1 \cap \left(A_2 \cup A_3\right)\right] \\
= p\left(A_1\right) + p\left(A_2\right) + p\left(A_3\right) - p\left(A_2 \cap A_3\right) - p\left[\left(A_1 \cap A_2\right) \cup \left(A_1 \cap A_3\right)\right] \\
= p\left(A_1\right) + p\left(A_2\right) + p\left(A_3\right) - p\left(A_2 \cap A_3\right) \\
- \left[p\left(A_1 \cap A_2\right) + p\left(A_1 \cap A_3\right) - p\left(\left(A_1 \cap A_2\right) \cap \left(A_1 \cap A_3\right)\right)\right] \\
= p\left(A_1\right) + p\left(A_2\right) + p\left(A_3\right) - p\left(A_2 \cap A_3\right) \\
- p\left(A_1 \cap A_2\right) - p\left(A_1 \cap A_3\right) + p\left(A_1 \cap A_2 \cap A_3\right) \\
= \sum_{i=1}^{3} p\left(A_i\right) - \sum_{i,j=1,\, i<j}^{3} p\left(A_i \cap A_j\right) + (-1)^{3+1} p\left(A_1 \cap A_2 \cap A_3\right).
\end{gathered}$$

3) Sea la fórmula cierta para $n \geq 3$ y veamos que es cierta para $n+1$:

$$\begin{gathered}
p\left(A_1 \cup \ldots \cup A_n \cup A_{n+1}\right) = p\left[\left(A_1 \cup \ldots \cup A_n\right) \cup A_{n+1}\right] \\
= p\left(A_1 \cup \ldots \cup A_n\right) + p\left(A_{n+1}\right) - p\left[\left(A_1 \cup \ldots \cup A_n\right) \cap A_{n+1}\right] \\
= p\left(A_1 \cup \ldots \cup A_n\right) + p\left(A_{n+1}\right) - p\left[\left(A_1 \cap A_{n+1}\right) \cup \ldots \cup \left(A_n \cap A_{n+1}\right)\right] \\
= \sum_{i=1}^{n} p\left(A_i\right) - \sum_{i,j=1,\, i<j}^{n} p\left(A_i \cap A_j\right) + \sum_{i,j,k=1,\, i<j<k}^{n} p\left(A_i \cap A_j \cap A_k\right) \\
+ \ldots + (-1)^n p\left(A_1 \cap \ldots \cap A_n\right) + p\left(A_{n+1}\right) \\
- \sum_{i=1}^{n} p\left(A_i \cap A_{n+1}\right) + \sum_{i,j=1,\, i<j}^{n} p\left(A_i \cap A_j \cap A_{n+1}\right) \\
- \sum_{i,j,k=1,\, i<j<k}^{n} p\left(A_i \cap A_j \cap A_k \cap A_{n+1}\right) \\
+ \ldots - (-1)^{n+1} p\left(A_1 \cap \ldots \cap A_n \cap A_{n+1}\right).
\end{gathered}$$

Agrupando las probabilidades de las intersecciones de un conjunto, de dos, etc. obtenemos

$$p\left(A_1 \cup \ldots \cup A_n \cup A_{n+1}\right) = \sum_{i=1}^{n+1} p\left(A_i\right) - \sum_{i,j=1,\, i<j}^{n+1} p\left(A_i \cap A_j\right)$$

$$+ \sum_{i,j,k=1,\, i<j<k}^{n+1} p\left(A_i \cap A_j \cap A_k\right) + \ldots + (-1)^{(n+1)+1} p\left(A_1 \cap \ldots \cap A_n \cap A_{n+1}\right),$$

y la fórmula es cierta para $n+1$. □

157. Cardinal de la unión de n conjuntos

Dado un conjunto A denotamos por $|A|$ a su cardinal. Sean los n conjuntos finitos $A_1, \ldots, A_n$ que podemos suponer contenidos en un conjunto universal U finito. Se trata de demostrar la fórmula

$$|A_1 \cup \ldots \cup A_n| = \sum_{i=1}^{n} |A_i| - \sum_{i,j=1,\, i<j}^{n} |A_i \cap A_j| +$$

$$\sum_{i,j,k=1,\, i<j<k}^{n} |A_i \cap A_j \cap A_k| + \ldots + (-1)^{n+1} |A_1 \cap A_2 \cap \ldots \cap A_n| .$$

Se pide:
1) Demostrar la fórmula para $n = 2$.
2) Demostrar la fórmula para $n = 3$.
3) Usando el método de inducción, demostrar que la fórmula es válida para todo $n \geq 2$.

SOLUCIÓN. 1) Sabemos que si $B_1, \ldots, B_m$ son m conjuntos finitos y disjuntos dos a dos se verifica

$$|B_1 \cup \ldots \cup B_m| = |B_1| + \ldots + |B_m| . \qquad [1]$$

Tenemos

$$A_1 = A_1 \cap U = A_1 \cap (A_2 \cup A_2^c) = (A_1 \cap A_2) \cup (A_1 \cap A_2^c) ,$$

$$A_2 = A_2 \cap U = A_2 \cap (A_1 \cup A_1^c) = (A_1 \cap A_2) \cup (A_2 \cap A_1^c) .$$

Además, A_1 está expresado como unión de los conjuntos disjuntos $A_1 \cap A_2$ y $A_1 \cap A_2^c$ y por [1],

$$|A_1| = |A_1 \cap A_2| + |A_1 \cap A_2^c| . \qquad [2]$$

De la misma manera,

$$|A_2| = |A_1 \cap A_2| + |A_2 \cap A_1^c| . \qquad [3]$$

Por otra parte,

$$A_1 \cup A_2 = (A_1 \cap A_2) \cup (A_1 \cap A_2^c) \cup (A_2 \cap A_1^c)$$

está expresado como unión de tres conjuntos disjuntos dos a dos, y por [1],

$$|A_1 \cup A_2| = |A_1 \cap A_2| + |A_1 \cap A_2^c| + |A_2 \cap A_1^c| . \qquad [4]$$

Sumando miembro a miembro [2] y [3] y pasando un $|A_1 \cap A_2|$ al primer miembro

$$|A_1| + |A_2| - |A_1 \cap A_2| = |A_1 \cap A_2| + |A_1 \cap A_2^c| + |A_2 \cap A_1^c| ,$$

y usando la igualdad [4] queda

$$|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2| = \sum_{i=1}^{2} |A_i| + (-1)^{2+1} |A_1 \cap A_2| .$$

2) Usando la fórmula deducida en el apartado anterior,

$$|A_1 \cup A_2 \cup A_3| = |A_1 \cup (A_2 \cup A_3)| =$$

$$|A_1| + |A_2 \cup A_3| - |A_1 \cap (A_2 \cup A_3)|$$

$$= |A_1| + |A_2| + |A_3| - |A_2 \cap A_3| - |(A_1 \cap A_2) \cup (A_1 \cap A_3)|$$

$$= |A_1| + |A_2| + |A_3| - |A_2 \cap A_3|$$

$$- (|A_1 \cap A_2| + |A_1 \cap A_3| - |(A_1 \cap A_2) \cap (A_1 \cap A_3)|)$$

$$= |A_1| + |A_2| + |A_3| - |A_2 \cap A_3|$$

$$- |A_1 \cap A_2| - |A_1 \cap A_3| + |A_1 \cap A_2 \cap A_3|$$

$$= \sum_{i=1}^{3} |A_i| - \sum_{i,j=1,\, i<j}^{3} |A_i \cap A_j| + (-1)^{3+1} |A_1 \cap A_2 \cap A_3| .$$

¡/li¿¡li¿Sea la fórmula cierta para $n \geq 3$ y veamos que es cierta para $n+1$:

$$|A_1 \cup \ldots \cup A_n \cup A_{n+1}| = |(A_1 \cup \ldots \cup A_n) \cup A_{n+1}|$$

$$= |A_1 \cup \ldots \cup A_n| + |A_{n+1}| - |(A_1 \cup \ldots \cup A_n) \cap A_{n+1}|$$

$$= |A_1 \cup \ldots \cup A_n| + |A_{n+1}| - |(A_1 \cap A_{n+1}) \cup \ldots \cup (A_n \cap A_{n+1})|$$

$$= \sum_{i=1}^{n} |A_i| - \sum_{i,j=1,\, i<j}^{n} |A_i \cap A_j| + \sum_{i,j,k=1,\, i<j<k}^{n} |A_i \cap A_j \cap A_k|$$

$$+ \ldots + (-1)^n |A_1 \cap \ldots \cap A_n| + |A_{n+1}|$$

$$- \sum_{i=1}^{n} |A_i \cap A_{n+1}| + \sum_{i,j=1,\, i<j}^{n} |A_i \cap A_j \cap A_{n+1}|$$

$$- \sum_{i,j,k=1,\, i<j<k}^{n} |A_i \cap A_j \cap A_k \cap A_{n+1}|$$

$$+ \ldots - (-1)^{n+1} |A_1 \cap \ldots \cap A_n \cap A_{n+1}| .$$

Agrupando los cardinales de las intersecciones de un conjunto, de dos, etc. obtenemos

$$|A_1 \cup \ldots \cup A_n \cup A_{n+1}| = \sum_{i=1}^{n+1} |A_i| - \sum_{i,j=1,\, i<j}^{n+1} |A_i \cap A_j|$$

$$+ \sum_{i,j,k=1,\, i<j<k}^{n+1} |A_i \cap A_j \cap A_k| + \ldots + (-1)^{(n+1)+1} p\, |A_1 \cap \ldots \cap A_n \cap A_{n+1}| ,$$

y la fórmula es cierta para $n+1$. □

158. Valores propios y determinante de una matriz circulante

Recordamos que una matriz circulante es una matriz de la forma

$$A = \begin{bmatrix} a_0 & a_1 & \dots & a_{n-2} & a_{n-1} \\ a_{n-1} & a_0 & \dots & a_{n-3} & a_{n-2} \\ a_{n-2} & a_{n-1} & \dots & a_{n-4} & a_{n-3} \\ \vdots & \vdots & \dots & \vdots & \vdots \\ a_2 & a_3 & \dots & a_0 & a_1 \\ a_1 & a_2 & \dots & a_{n-1} & a_0 \end{bmatrix} \in \mathbb{C}^{n\times n},$$

es decir una matriz cuadrada compleja cuyas componentes de la primera fila son números complejos cualesquiera y cada una de las sucesivas filas se obtiene de la anterior sustituyendo la última componente por la primera y trasladando las restantes. El objetivo de este problema es hallar los valores propios, vectores propios y el determinante de cualquier matriz circulante.
1) Demostrar que $v = \left[1, \omega, \omega^2 \dots, \omega^{n-1}\right]^T$ con ω cualquier raíz enésima de la unidad, es vector propio de A. Determinar su valor propio asociado.
2) Demostrar que A tiene n vectores propios linealmente independientes.
3) Calcular $\det A$.
4) Para una matriz genérica circulante de orden 2, hallar sus valores propios, vectores propios y determinante sin usar los apartados anteriores. Verificar los resultados.

SOLUCIÓN. 1) Hallemos el vector Av, es decir

$$Av = \begin{bmatrix} a_0 & a_1 & \dots & a_{n-2} & a_{n-1} \\ a_{n-1} & a_0 & \dots & a_{n-3} & a_{n-2} \\ a_{n-2} & a_{n-1} & \dots & a_{n-4} & a_{n-3} \\ \vdots & \vdots & \dots & \vdots & \vdots \\ a_2 & a_3 & \dots & a_0 & a_1 \\ a_1 & a_2 & \dots & a_{n-1} & a_0 \end{bmatrix} \begin{bmatrix} 1 \\ \omega \\ \omega^2 \\ \vdots \\ \omega^{n-1} \end{bmatrix}.$$

Llamemos λ a la primera componente del vector Av. Entonces,

$$\lambda = a_0 + a_1\omega + a_2\omega^2 + \cdots a_{n-2}\omega^{n-2} + a_{n-1}\omega^{n-1}.$$

La segunda componente del vector Av es

$$\begin{aligned} &a_{n-1} + a_0\omega + \cdots + a_{n-3}\omega^{n-2} + a_{n-2}\omega^{n-1} \\ &= \omega\left(a_{n-1}\omega^{n-1} + a_0 + \cdots + a_{n-3}\omega^{n-3} + a_{n-2}\omega^{n-2}\right) \\ &= \omega\left(a_0 + \cdots + a_{n-3}\omega^{n-3} + a_{n-2}\omega^{n-2} + a_{n-1}\omega^{n-1}\right) = \lambda\omega. \end{aligned}$$

La i-ésima componente es

$$\begin{aligned} &a_{n-i+1} + a_{n-i+2}\omega + \cdots + a_{n-i}\omega^{n-1} \\ &= \omega^{i-1}\left(a_{n-i+1}\omega^{n-i+1} + a_{n-i+2}\omega^{n-i+2} + \cdots + a_{n-i}\omega^{n-i}\right) = \lambda\omega^{i-1}. \end{aligned}$$

En consecuencia

$$Av = \begin{bmatrix} \lambda \\ \lambda\omega \\ \lambda\omega^2 \\ \vdots \\ \lambda\omega^{n-1} \end{bmatrix} = \lambda \begin{bmatrix} 1 \\ \omega \\ \omega^2 \\ \vdots \\ \omega^{n-1} \end{bmatrix} = \lambda v.$$

Concluimos que $v = \left[1, \omega, \omega^2 \ldots, \omega^{n-1}\right]^T \neq 0$ es vector propio asociado al valor propio $\lambda = a_0 + a_1\omega + a_2\omega^2 + \cdots a_{n-2}\omega^{n-2} + a_{n-1}\omega^{n-1}$, y esto para todo ω raíz n-ésima de la unidad.

2) El razonamiento del apartado anterior es válido para toda raíz enésima de la unidad. Si $\zeta = e^{2\pi i}$ entonces, las n raíces enésimas de la unidad son $\omega = \zeta^k$ con $k = 0, 1, \ldots, n-1$. Esto significa que para todo $k = 0, 1, \ldots, n-1$ el vector

$$v_k = \left[1, \zeta^k, \zeta^{2k} \ldots, \zeta^{k(n-1)}\right]^T$$

es vector propio de A asociado al valor propio

$$\lambda_k = a_0 + a_1\zeta^k + a_2\zeta^{2k} + \cdots a_{n-2}\zeta^{k(n-2)} + a_{n-1}\zeta^{k(n-1)}.$$

Para demostrar que los vectores v_k $(k = 0, 1, \ldots, n-1)$ son linealmente independientes formamos la matriz:

$$P = \left[v_0, v_1, v_2 \ldots, v_{n-1}\right] =$$

$$\begin{bmatrix} 1 & 1 & 1 & \ldots & 1 & 1 \\ 1 & \zeta & \zeta^2 & \ldots & \zeta^{n-2} & \zeta^{n-1} \\ 1 & \zeta^2 & \zeta^4 & \ldots & \zeta^{2(n-2)} & \zeta^{2(n-1)} \\ 1 & \zeta^3 & \zeta^6 & \ldots & \zeta^{3(n-2)} & \zeta^{3(n-1)} \\ \vdots & \vdots & \vdots & \ldots & \vdots & \vdots \\ 1 & \zeta^{n-1} & \zeta^{2(n-1)} & \ldots & \zeta^{(n-1)(n-2)} & \zeta^{(n-1)(n-1)} \end{bmatrix}.$$

La matriz P es una matriz de Vandermonde y su determinante es

$$\det P = \prod_{0 \leq i < j \leq n-1} (\zeta^j - \zeta^i) \neq 0.$$

Es decir, rg $(P) = n$ lo cual implica que sus columnas son linealmente independientes. Nótese que hemos demostrado también que toda matriz circulante es diagonalizable.

3) El determinante de A es el producto de sus valores propios, en consecuencia

$$\det A = \prod_{k=0}^{n-1} \left(a_0 + a_1\zeta^k + a_2\zeta^{2k} + \cdots + a_{n-1}\zeta^{k(n-1)}\right), \quad \zeta = e^{2\pi i/n}.$$

4) Hallemos los valores propios de una matriz circulante genérica A de orden dos:

$$A = \begin{bmatrix} a_0 & a_1 \\ a_1 & a_0 \end{bmatrix} \in \mathbb{C}^{2\times 2}, \quad \chi(\lambda) = \lambda^2 - 2a_0\lambda + a_0^2 - a_1^2 = 0$$

$$\Leftrightarrow \lambda = \frac{2a_0 \pm \sqrt{4a_0^2 - 4a_0^2 + 4a_1^2}}{2} = a_0 \pm a_1.$$

Llamemos $\lambda_0 = a_0 + a_1$ y $\lambda_1 = a_0 - a_1$. Se verifica $\lambda_0 = \lambda_1$ si y sólo si $a_1 = 0$. Entonces para $a_1 \neq 0$ tenemos dos valores propios simples y los subespacios propios y una base de cada uno de ellos son:

$$V_{\lambda_0} : \begin{cases} -a_1x_1 + a_1x_2 = 0 \\ a_1x_1 - a_1x_2 = 0, \end{cases} \quad B_{V_{\lambda_0}} = \{v_0 = (1,1)^T\}.$$

$$V_{\lambda_1} : \begin{cases} a_1x_1 + a_1x_2 = 0 \\ a_1x_1 + a_1x_2 = 0, \end{cases} \quad B_{V_{\lambda_1}} = \{v_1 = (1,-1)^T\}.$$

Para $a_1 = 0$ tenemos

$$Av_0 = \begin{bmatrix} a_0 & 0 \\ 0 & a_0 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \end{bmatrix} = a_0 \begin{bmatrix} 1 \\ 1 \end{bmatrix}, \; Av_1 = \begin{bmatrix} a_0 & 0 \\ 0 & a_0 \end{bmatrix} \begin{bmatrix} 1 \\ -1 \end{bmatrix} = a_0 \begin{bmatrix} 1 \\ -1 \end{bmatrix}$$

y por tanto v_0 y v_1 son también vectores propios asociados al valor propio doble $\lambda_0 = \lambda_1 = a_0$. Verificamos todo esto con lo demostrado en los apartados anteriores. Sea $\zeta = -1$. Las raíces cuadradas de la unidad son $\zeta^0 = 1$ y $\zeta^1 = -1$. Los valores propios son:

$$\lambda_0 = a_0 + a_1 = a_0 + a_1\zeta^0, \quad \lambda_1 = a_0 - a_1 = a_0 + a_1\zeta^1,$$

y los respectivos vectores propios

$$v_0 = \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ \zeta^0 \end{bmatrix}, \quad v_1 = \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ \zeta^1 \end{bmatrix}.$$

Por último,

$$\det A = a_0^2 - a_1^2 = (a_0 + a_1)(a_0 - a_1) = \left(a_0 + a_1\zeta^0\right)\left(a_0 + a_1\zeta^1\right)$$

$$= \prod_{k=0}^{2-1} \left(a_0 + a_1\zeta^k\right), \quad \zeta = e^{2\pi i/2} = -1.$$

□

159. Teorema de reordenación de Riemann

Por simplicidad, denotaremos $\sum a_n = \sum_{n=1}^{\infty} a_n$.
1) Demostrar que si la serie real $\sum a_n$ es condicionalmente convergente, entonces existen infinitos términos positivos e infinitos negativos.
2) Para todo n descomponemos $a_n = a_n^+ + a_n^-$ con $a_n^+ \geq 0$ y $a_n^- \leq 0$ de la siguiente manera:

$$a_n^+ = \frac{a_n + |a_n|}{2}, \quad a_n^- = \frac{a_n - |a_n|}{2}.$$

Describir tal descomposición según los casos a_n positivo, negativo o nulo.
3) Demostrar que $\sum a_n^+ = +\infty$ y que $\sum a_n^- = -\infty$.
4) Dada una serie real condicionalmente convergente y dado cualquier número real x, demostrar que existe una reordenación de la serie cuya suma es x.
5) Dada una serie real condicionalmente convergente demostrar que existe

una reordenación de la serie cuya suma es $+\infty$ y otra cuya suma es $-\infty$ (esto completará la demostración del teorema).

SOLUCIÓN. 1) Supongamos que existiera sólo un número finito de términos positivos y sea a_m el último de ellos. Entonces, al ser $\sum a_n$ convergente, lo sería $\sum_{n>m} a_n = -\sum_{n>m} |a_n|$ con lo cual lo sería $\sum_{n>m} |a_n|$ y por ende $\sum |a_n|$. Llegaríamos al absurdo de que $\sum a_n$ sería absolutamente convergente. Análogo razonamiento si existiera sólo un número finito de términos negativos.
2) De acuerdo con las definiciones de a_n^+ y a_n^-:

$$a_n = \begin{cases} a_n^+ + a_n^- = a_n + 0 & \text{si} \quad a_n > 0 \\ a_n^+ + a_n^- = 0 + a_n & \text{si} \quad a_n < 0 \\ a_n^+ + a_n^- = 0 + 0 & \text{si} \quad a_n = 0. \end{cases}$$

3) Si ambas series fueran convergentes:

$$\begin{cases} \sum a_n^+ = S \in \mathbb{R} \\ \sum a_n^- = T \in \mathbb{R} \end{cases} \Rightarrow \begin{cases} \sum a_n^+ = S \\ \sum |a_n^-| = -T \end{cases}$$

$$\Rightarrow \sum |a_n| = \sum \left(a_n^+ + \left|a_n^-\right|\right) = \sum a_n^+ + \sum \left|a_n^-\right| = S - T \in \mathbb{R}$$

y la serie $\sum a_n$ sería absolutamente convergente (contradicción). Si una de las series $\sum a_n^+$, $\sum a_n^-$ fuera convergente y otra divergente, la serie suma $\sum (a_n^+ + a_n^-)$ (que es la serie $\sum a_n$), sería divergente, en contradicción con la hipótesis de ser $\sum a_n$ condicionalmente convergente. Concluimos que necesariamente las series $\sum a_n^+$ y $\sum a_n^-$ son ambas divergentes. Ademas, al ser $\sum a_n^+$ serie de términos positivos y $\sum a_n^-$ de negativos, ha de ser

$$\sum a_n^+ = +\infty, \quad \sum a_n^- = -\infty.$$

4) Podemos suponer sin pérdida de generalidad que todos los términos de la serie condicionalmente convergente $\sum a_n$ son no nulos. Sea p_n el n-ésimo término positivo de $\sum a_n$ y sea $-q_n$ su n-ésimo negativo. Según el apartado anterior, $\sum p_n = +\infty$ y $\sum -q_n = -\infty$. Elijamos términos positivos $p_1, \ldots, p_{n_1}$ hasta el primer p_{n_1} que verifique

$$S_{n_1} = p_1 + \ldots + p_{n_1} > x$$

con lo cual, $S_{n_1} - x < p_{n_1}$. Elijamos términos negativos $-q_1, \ldots, -q_{n_2}$ hasta el primer $-q_{n_2}$ que verifique

$$S_{n_1+n_2} = p_1 + \ldots + p_{n_1} - q_1 - \ldots - q_{n_2} < x$$

con lo cual, $x - S_{n_1+n_2} < q_{n_2}$. Además, $S_{n_1} > S_{n_1+1} > \ldots > S_{n_1+n_2}$, luego

$$x - S_n < q_{n_2} \quad \forall n = n_1, n_2 + 1, \ldots, n_1 + n_2.$$

Nótese que estamos reordenado la serie $\sum a_n$. De nuevo, elijamos los términos positivos $p_{n_1+1}, \ldots, p_{n_3}$ hasta el primer p_{n_3} que verifique

$$S_{n_1+n_2+n_3} = p_1 + \ldots + p_{n_1} - q_1 - \ldots - q_{n_2} + p_{n_1+1} + \ldots + p_{n_3} > x$$

con lo cual, $S_{n_1+n_2+n_3} - x < p_{n_3}$. Además, $S_{n_1+n_2} < S_{n_1+n_2+1} < \ldots < S_{n_1+n_2+n_3}$, luego

$$S_n - x < p_{n_3} \quad \forall n = n_1 + n_2, n_1 + n_2 + 1, \ldots, n_1 + n_2 + n_3.$$

Procediendo de esta manera llegamos a una reordenación de la serie $\sum a_n$ de tal manera que sus sumas parciales satisfacen

$$S_{n_1} - x < p_{n_1}, \quad x - S_{n_1+n_2} < q_{n_2}, \quad S_{n_1+n_2+n_3} - x < p_{n_3}, \quad \ldots$$

así como las sumas parciales intermedias S_n. Por la condición necesaria de la convergencia de $\sum a_n$ tenemos que $p_n \to 0$ y $q_n \to 0$, por tanto las sumas parciales de la serie reordenada tienen límite x.
5) De nuevo y sin pérdida de generalidad suponemos que todos los términos de la serie $\sum a_n$ son no nulos. Sea $p_1 < p_2 < p_3 < \cdots$ la sucesión de índices tales que a_{p_i} es término positivo de la serie y $n_1 < n_2 < n_3 < \cdots$ la de los que a_{n_i} es negativo. Cada número natural aparece pues una y sólo una vez en alguna de las sucesiones (p_i) o (n_i). Recordemos que según se ha demostrado, $\sum_{i=1}^{\infty} a_{p_i} = +\infty$. Entonces, sea k_1 el menor número natural tal que

$$\sum_{i=1}^{k_1} a_{p_i} \geq |a_{n_1}| + 1,$$

k_2 el menor número natural tal que

$$\sum_{i=k_1+1}^{k_2} a_{p_i} \geq |a_{n_2}| + 1,$$

y así sucesivamente. Esto define la reordenación de la serie

$$a_{p_1} + a_{p_2} + \cdots + a_{p_{k_1}} + a_{n_1} + a_{p_{k_1+1}} + a_{p_{k_1+2}} + a_{p_{k_2}} + a_{n_2} + \cdots$$

Veamos que la serie reordenada de esta manera tiene suma $+\infty$. Efectivamente, por construcción, la suma de los $k_1 + 1$ primeros términos de la reordenación es ≥ 1 y ninguna suma parcial de entre esos términos es < 0. De manera análoga, la suma de los siguientes $k_2 - k_1 + 1$ términos es ≥ 1 y ninguna suma parcial de entre esos términos es < 0. Reiterando, concluimos que la suma de la reordenación es $+\infty$. La demostración de que existe una reordenación cuya suma es $-\infty$ es similar. □

160. Derivada aritmética natural

La función *derivada aritmética* es una función $n' : \mathbb{N} \to \mathbb{N}$ definida recursivamente por
(1) $p' = 1$ para todo p primo
(2) $(ab)' = a'b + ab'$ para todo $a, b \in \mathbb{N}$ (Regla de Leibniz).
1) Calcular $1'$, $0'$, $6'$ y $9''$.
2) Calcular las derivadas de los 11 primeros números naturales.

3) Demostrar que si existe la función derivada aritmética, es única.
4) Demostrar que la función derivada aritmética existe y es

$$n' = \begin{cases} 0 & \text{si} \quad n = 0 \ \vee \ n = 1 \\ n \displaystyle\sum_{i=1}^{m} \frac{n_i}{p_i} & \text{si} \qquad n \geq 2 \end{cases}$$

en donde $n = \prod_{i=1}^{m} p_i^{n_i} \geq 2$ es la factorización de n en producto de factores primos.
5) Usando el teorema anterior, hallar $120'$.

SOLUCIÓN. 1) Tenemos $1' = (1 \cdot 1)' = 1' \cdot 1 + 1 \cdot 1' = 2 \cdot 1' \Rightarrow 1' = 0$.
$0' = (2 \cdot 0)' = 2' \cdot 0 + 2 \cdot 0' = 1 \cdot 0 + 2 \cdot 0' = 2 \cdot 0' \Rightarrow 0' = 0$.
$6' = (2 \cdot 3)' = 2' \cdot 3 + 2 \cdot 3' = 1 \cdot 3 + 2 \cdot 1 = 5$.
$9'' = (9')' = 6' = 5$. 2) Fácilmente podemos verificar las derivadas de los 11 primeros números naturales:

n	0	1	2	3	4	5	6	7	8	9	10
n'	0	0	1	1	4	1	5	1	12	6	7

3) Si existe la derivada aritmética vimos que necesariamente $0' = 1' = 0$ y por definición, $p' = 1$ para todo p primo. Sea $n \geq 2$ y $n = \prod_{i=1}^{m} p_i$ la descomposición de n en factores primos (repetidos o no). Procedamos por inducción sobre m. Para $m = 1$ tenemos $n' = (p_1)' = 1$. Supongamos determinada unívocamente la derivada aritmética para todos los naturales de la forma $\prod_{i=1}^{m} p_i$, Entonces,

$$\left(\prod_{i=1}^{m+1} p_i\right)' = \left(\left(\prod_{i=1}^{m} p_i\right) \cdot p_{m+1}\right)' = \left(\prod_{i=1}^{m} p_i\right)' \cdot p_{m+1} + \left(\prod_{i=1}^{m} p_i\right),$$

y al estar determinado $(\prod_{i=1}^{m} p_i)'$, lo está $\left(\prod_{i=1}^{m+1} p_i\right)'$.
4) Es claro que para $n \geq 2$ la fórmula dada es válida incluso si alguno de los exponente n_i es nulo, por tanto si a, b son dos números mayores o iguales que 2 se pueden expresar en la forma $a = \prod_{i=1}^{k} p_i^{\alpha_i}$, $b = \prod_{i=1}^{k} p_i^{\beta_i}$. Entonces,

$$(ab)' = \left(\prod_{i=1}^{k} p_i^{\alpha_i + \beta_i}\right)' = ab \sum_{i=1}^{k} \frac{\alpha_i + \beta_i}{p_i}$$

$$= \left(a \sum_{i=1}^{k} \frac{\alpha_i}{p_i}\right) b + a \left(b \sum_{i=1}^{k} \frac{\beta_i}{p_i}\right) = a'b + ab'.$$

Si alguno de los a, b es 0 o 1, la comprobación de la regla de Leibniz es inmediata.
5) Tenemos $120' = \left(2^3 \cdot 3 \cdot 5\right)' = 120 \left(\frac{3}{2} + \frac{1}{3} + \frac{1}{5}\right) = 244$. □

161. Propiedades de la derivada aritmética natural

1) Demostrar que para k, n enteros positivos se verifica $(n^k)' = kn^{k-1}n'$.
2) Demostrar la fórmula de Leibniz para la derivada k-ésima del producto de dos números: $(ab)^{(k)} = \sum_{i=0}^{k} \binom{k}{i} a^{(k-i)}b^{(i)}$.
3) Demostrar que la aditividad de la derivada $(a+b)' = a' + b'$ se cumple en algunos casos y en otros no.
4) Demostrar que
   (1) $(a+b)' = a' + b' \Rightarrow (ka+kb)' = (ka)' + (kb)' \quad \forall k \in \mathbb{N}$.
   (2) $(a+b)' \geq a' + b' \Rightarrow (ka+kb)' \geq (ka)' + (kb)' \quad \forall k \in \mathbb{N}$.
   (3) $(a+b)' \leq a' + b' \Rightarrow (ka+kb)' \leq (ka)' + (kb)' \quad \forall k \in \mathbb{N}$.
5) Demostrar que para todo $k > 1$ número natural se verifica

$$n' \geq n \geq 1 \Rightarrow (kn)' > kn \qquad \forall n \geq 1.$$

SOLUCIÓN. 1) Para $k = 1$, $(n^1)' = n' = 1n^{1-1}n'$ y la fórmula se verifica. Para $k = 2$, $(n^2)' = (n \cdot n)' = n'n + nn' = 2nn'$, y también se cumple. Si se cumple para k,

$$\left(n^{k+1}\right)' = \left(n^k n\right)' = \left(n^k\right)' n + n^k n' = kn^{k-1}n'n + n^k n' = (k+1)n^k n',$$

y la fórmula es cierta para $k+1$.
2) La fórmula es cierta para $k = 1$, en efecto

$$(ab)^{(1)} = (ab)' = a'b + ab'$$

$$= \binom{1}{0} a^{(1)}b^{(0)} + \binom{1}{1} a^{(0)}b^{(1)} = \sum_{i=0}^{1} \binom{1}{i} a^{(1-i)}b^{(i)}.$$

Supongamos que la fórmula es cierta para k. Entonces,

$$(ab)^{(k+1)} = \left(\sum_{i=0}^{k} \binom{k}{i} a^{(k-i)}b^{(i)}\right)' = \sum_{i=0}^{k} \left(\binom{k}{i} a^{(k-i)}b^{(i)}\right)'$$

$$= \sum_{i=0}^{k} \binom{k}{i} \left(a^{(k-i+1)}b^{(i)} + a^{(k-i)}b^{(i+1)}\right)$$

$$= \sum_{i=0}^{k} \binom{k}{i} a^{(k-i+1)}b^{(i)} + \sum_{i=0}^{k} \binom{k}{i} a^{(k-i)}b^{(i+1)}.$$

Haciendo un cambio de índices y usando las conocidas fórmulas combinatorias $\binom{k}{i} + \binom{k}{i-1} = \binom{k+1}{i}$, $\binom{k}{0} = 1 = \binom{k+1}{0}$, $\binom{k}{k} = 1 = \binom{k+1}{k+1}$ podemos escribir

$$(ab)^{(k+1)} = \sum_{i=0}^{k} \binom{k}{i} a^{(k-i+1)}b^{(i)} + \sum_{i=1}^{k+1} \binom{k}{i-1} a^{(k-i+1)}b^{(i)}$$

$$= \binom{k}{0} a^{(k+1)}b^{(0)} + \sum_{i=1}^{k} \binom{k}{i} a^{(k-i+1)}b^{(i)}$$

$$+\sum_{i=1}^{k}\binom{k}{i-1}a^{(k-i+1)}b^{(i)}+\binom{k}{k}a^{(0)}b^{(k+1)}$$

$$=\binom{k+1}{0}a^{(k+1)}b^{(0)}+\sum_{i=1}^{k}\binom{k+1}{i}a^{(k+1-i)}b^{(i)}+\binom{k+1}{k+1}a^{(0)}b^{(k+1)}$$

$$=\sum_{i=0}^{k+1}\binom{k+1}{i}a^{(k+1-i)}b^{(i)},$$

lo cual implica que la fórmula es cierta para $k+1$.
3) Por ejemplo

$$(1+2)'=3'=1=0+1=1'+2',$$
$$(3+5)'=8'=12,\ 3'+5'=1+1=2\Rightarrow(3+5)'\neq 3'+5'.$$

4) Tenemos
(1) $(ka+kb)'=(k(a+b))'=k'(a+b)+k(a+b)'=k'a+k'b+k(a'+b')$ $=(k'a+ka')+(k'b+kb')=(ka)'+(kb)'$.
(2) $(ka+kb)'=(k(a+b))'=k'(a+b)+k(a+b)'\geq k'a+k'b+k(a'+b')$ $=(k'a+ka')+(k'b+kb')=(ka)'+(kb)'$.
(3) Análogo razonamiento.
5) Si $k>1$ entonces $k'\geq 1$ con lo cual $k'n\geq 1$. Entonces, $(kn)'=k'n+kn'>kn'\geq kn$. □

162. Cotas para la derivada aritmética natural

1) Demostrar que para todo entero positivo n se verifica $n'\leq\dfrac{n\log_2 n}{2}$.
2) Demostrar que si $n=2^k$ la cota es exacta
3) Demostrar que si n es el producto de k factores, cada uno de ellos mayor que 1, se verifica $n'\geq kn^{\frac{k-1}{k}}$.
4) Demostrar que si $n=2^k$ la cota es exacta.
5) Demostrar que si $n>1$ no es primo, entonces $n'\geq 2\sqrt{n}$.

solución. 1) Si $n=1$ se verifica la desigualdad trivialmente. Si $n\geq 2$, sea $n=\prod_{i=1}^{k}p_i^{n_i}$ su descomposición en factores primos. Entonces,

$$n\geq\prod_{i=1}^{k}2^{n_i}\Rightarrow\log_2 n\geq\log_2\prod_{i=1}^{k}2^{n_i}=\sum_{i=1}^{k}n_i.$$

$$\Rightarrow n'=n\sum_{i=1}^{k}\frac{n_i}{p_i}\leq n\sum_{i=1}^{k}\frac{n_i}{2}=\frac{n}{2}\sum_{i=1}^{k}n_i\leq\frac{n\log_2 n}{2}.$$

2) Tenemos $n'=n\cdot\dfrac{k}{2}=\dfrac{n\log_2 2^k}{2}=\dfrac{n\log_2 n}{2}$.
3) Sea $n=n_1n_2n_3\cdots n_k$ con $n_i\geq 2$ para todo $i=1,\ldots,k$. Aplicando la regla de Leibniz y que $n_i'\geq 1$ para todo i,

$$n'=n_1'n_2n_3\cdots n_k+n_1n_2'n_3\cdots n_k+\ldots+n_1n_2n_3\cdots n_k'$$

$$\geq n_2n_3\cdots n_k + n_1n_3\cdots n_k + \ldots + n_1n_2n_3\cdots n_{k-1}$$
$$= n\left(\frac{1}{n_1}+\frac{1}{n_2}+\ldots+\frac{1}{n_k}\right).$$

Usando que la media aritmética es mayor o igual que la geométrica,

$$n' \geq nk\left(\frac{1}{n_1}\cdot\frac{1}{n_2}\cdot\ldots\cdot\frac{1}{n_k}\right)^{1/k} = knn^{-1/k} = kn^{\frac{k-1}{k}}.$$

4) Tenemos $n' = 2^k\dfrac{k}{2} = k2^{k-1} = k\left(2^k\right)^{\frac{k-1}{k}} = kn^{\frac{k-1}{k}}$.
5) Si $n > 1$ no es primo, es el producto de $k \geq 2$ factores mayores que 1, por tanto $n' \geq kn^{\frac{k-1}{k}} \geq 2n^{\frac{2-1}{2}} = 2\sqrt{n}$. □

163. Primeras ecuaciones diferenciales aritméticas

Es natural plantear el problema de encontrar todos los números naturales que satisfacen a la ecuación diferencial aritmética

$$a_kn^{(k)} + a_{k-1}n^{(k-1)} + \cdots + a_2n'' + a_1n' + a_0n = b$$

con los a_i y b, números naturales. Vemos algunos ejemplos sencillos.
1) Demostrar que el único entero positivo que satisface $n' = 0$ es $n = 1$.
2) Demostrar que los únicos números naturales n que verifican $n' = 1$ son los primos.
3) Demostrar que si $a - 2$ es primo, la ecuación $n' = a$ tiene al menos la solución $n = 2(a-2)$.
4) Demostrar que $n = p^p$ con p primo es solución de la ecuación $n' = n$

solución. 1) Sabemos que $1' = 0$ y si $n \geq 2$, entonces n contiene algún factor primo con lo cual $n' > 0$.
2) Si n es primo, entonces $n' = 1$ y si $n \geq 2$ no es primo, contiene al menos un par de primos p_1, p_2 en su factorización, es decir $n = p_1p_2\ldots$ y $n' = n\left(\frac{1}{p_1}+\frac{1}{p_2}+\ldots\right) > 1$.
3) En efecto, $(2(a-2))' = 2'(a-2) + 2(a-2)' = a - 2 + 2 = a$.
4) Tenemos $(p^p)' = pp^{p-1}p' = p^p$. □

164. Conjetura de Goldbach y derivada aritmética

La conjetura de Goldbach, no resuelta a día de hoy se enuncia como *todo número par mayor que dos es la suma de dos primos.* Proporcionamos una condición necesaria para que la conjetura sea cierta en términos de una ecuación diferencial aritmética.

Demostrar que si la conjetura de Goldbach es cierta, entonces la ecuación diferencial aritmética $n' = 2a$ tiene solución para todo $a \geq 2$.

solución. Si la conjetura de Goldbach es cierta, entonces para todo $a \geq 2$ existen primos p_1, p_2 con $2a = p_1 + p_2$. Si $n = p_1p_2$, tenemos $n' = (p_1p_2)' = p_1'p_2 + p_1p_2' = p_2 + p_1 = 2a$, por tanto $n = p_1p_2$ es solución de $n' = 2a$. □

165. Conjetura de los primos gemelos y derivada aritmética

La conjetura de los primos gemelos, no resuelta a día de hoy se enuncia como *existen infinitos pares de números gemelos*, es decir infinitos pares $(p, p+2)$ con p y $p+2$ primos. Proporcionamos una condición necesaria para que la conjetura sea cierta en términos de una ecuación diferencial aritmética.

Demostrar que si la conjetura de la infinitud de los primos gemelos es cierta, entonces la ecuación diferencial aritmética $n'' = 1$ tiene infinitas soluciones.

solución. Si la conjetura de los primos gemelos es cierta, entonces existen infinitos pares de primos de la forma $p, p+2$. Si $n = 2p$, tenemos $n' = (2p)' = 2'p + 2p' = p + 2$. Pero al ser $p+2$ primo, $n'' = (p+2)' = 1$. □

166. Conjetura de Sophie Germain y derivada aritmética

Un número primo p se dice que es un primo de Sophie Germain si $2p+1$ es también primo. Por ejemplo, 2 es primo de Sophie Germain, y 7 no lo es. Se ha conjeturado que existen infinitos primos de Sophie Germain, pero a día de hoy, esta conjetura ni se ha demostrado ni refutado.

1) Demostrar que si p es primo, entonces $(2^4 p)' = 2^4(2p+1)$.
2) Demostrar que para todo entero positivo m se verifica la desigualdad $(2^4 m)'' \geq 2^4(4m+3)$, con igualdad si y sólo si m es un primo de Sophie Germain.
3) Demostrar que la conjetura de Sophie Germain es cierta si y sólo si la ecuación diferencial aritmética $n'' = 4n + 48$ tiene infinitas soluciones de la forma $n = 2^4 p$ con p primo.

solución. 1) Tenemos $(2^4 p)' = (2^4)'p + 2^4 p' = 4 \cdot 2^3 \cdot 2' \cdot p + 2^4 \cdot 1 = 2^4(2p+1)$.
2) Analicemos los casos m primo y no primo. Si m no es primo,

$$\left(2^4 m\right)' = 4 \cdot 2^3 m + 2^4 m' = 2^4(2m + m'),$$

$$\begin{aligned}\left(2^4 m\right)'' &= \left(2^4(2m+m')\right)' = 4 \cdot 2^3(2m+m') + 2^4(2m+m')' \\ &= 2^4\left(4m + 2m' + (2m+m')'\right) > 2^4(4m+3).\end{aligned}$$

Si m es primo,

$$\left(2^4 m\right)' = 4 \cdot 2^3 m + 2^4 m' = 2^4(2m+m') = 2^4(2m+1),$$

$$\begin{aligned}\left(2^4 m\right)'' &= \left(2^4(2m+1)\right)' = 4 \cdot 2^3(2m+1) + 2^4(2m+1)' \\ &= 2^4\left(4m + 2 + (2m+1)'\right) \geq 2^4(4m+3),\end{aligned}$$

verificándose la igualdad si y sólo si $2m+1$ es también primo, es decir si y sólo si m es un primo de Sophie Germain.
3) Si la conjetura de Sophie Germain es cierta, segun el apartado anterior existen infinitos primos p tales que $(2^4 p)' = 2^4(4p+3)$ y llamando $n = 2^4 p$ queda la ecuación $n'' = 4n + 48$. Recíprocamente, si la ecuación $n'' = 4n + 48$

tiene infinitas soluciones de la forma $n = 2^4 p$, entonces $(2^4 p)' = 2^4(4p+3)$ y sgún el apartado anterior, p es primo de Sophie Germain. □

167. La ecuación diferencial aritmética $n' = n$

1) Demostrar que si $n = p^p m$ con p primo y $m > 1$ natural, entonces $n' = p^p(m + m')$ y $\lim_{k\to\infty} n^{(k)} = \infty$.
2) Sea n número natural y p^k la mayor potencia del primo p tal que $p^k \mid n$. Si $0 < k < p$, demostrar que p^{k-1} es la mayor potencia de p tal que $p^{k-1} \mid n'$ y que todas las derivadas n', n'', $\ldots$, $n^{(k)}$ son distintas.
3) Demostrar que si $n = p^{pk} m$ para algún primo p y enteros $k, m > 1$, entonces $n' = p^{pk}(km + m')$.
4) Sea $n \geq 2$ entero. Demostrar que: n está libre de cuadrados $\Leftrightarrow (n, n') = 1$.
5) Demostrar que todas las soluciones de la ecuación $n' = n$ son $n = 0$ y $n = p^p$ con p primo.

solución. 1) Tenemos $n' = (p^p m)' = (p^p)' m + p^p m' = p^p \cdot \frac{p}{p} \cdot m + p^p m' = p^p(m + m')$. Dado que $(p^p)^{(i)} = p^p$ para todo $i \geq 0$ y usando la fórmula de la derivada k-ésima del producto,

$$(p^p m)^{(k)} = \sum_{i=0}^{k} \binom{k}{i} (p^p)^{(k-i)} m^{(i)} = p^p \left(m + km' + \cdots\right)$$

$$\geq p^p m + k p^p m' \geq p^p m + k = n + k \Rightarrow \lim_{k\to\infty} n^{(k)} = \infty.$$

2) Como $p^k \mid n$, podemos escribir $n = p^k m$. Derivando, $n' = kp^{k-1} m + p^k m' = p^{k-1}(km + pm')$, es decir $p^{k-1} \mid n'$. No puede ocurrir $p^k \mid n'$ pues si así fuera,

$$p^k \mid n' \Rightarrow p^k \mid p^{k-1}(km + pm') \Rightarrow p \mid km + pm',$$

lo cual es absurdo pues $k < p$ y m no contiene el factor p. Deducimos además que n'' sólo puede ser divisible por p^{k-2}, etc. Esto asegura que las derivadas n', n'', $\ldots$, $n^{(k)}$ son distintas.
3) Tenemos $(p^{pk} m)' = pkp^{pk-1} m + p^{pk} m' = p^{pk}(km + m')$.
4) $\Rightarrow$) Si $(n, n') \neq 1$, existe primo p tal que $p \mid n$ y $p \mid n'$ y según el apartado 2, $p^2 \mid n$ (absurdo).
$\Leftarrow$) Si existe primo p tal que $p^2 | n$, por el apartado 2, $p \mid n'$ con lo cual $(n, n') \neq 1$ (absurdo).
5) Se verifica $0' = 0$ y $(p^p)' = pp^{p-1} p' = p^p$, luego 0 y p^p son soluciones de la ecuación.
Sea $n \neq 0$ y $n' = n$, con lo cual ha de ser $n \geq 2$. Sea p alguno de los factores primos que aparecen en la factorización de n. Entonces, $p \mid n$ y veamos que al menos $p^p \mid n$. En efecto si p^k con $0 < k < p$ fuera la mayor potencia que divide a n, entonces y según el apartado 2, p^{k-1} sería la mayor potencia que divide a $n' = n$ lo cual es absurdo. Pero si $p^p \mid n$ tenemos $n = p^p m$ con $m \geq 1$. Si fuera $m > 1$ y por el apartado 1, $n' = p^p (m + m') = p^p m$ implica

$m' = 0$ y por tanto $m = 1$, lo cual es es una contradicción. Ha de ser pues $m = 1$ con lo cual necesariamente $n = p^p$. □

168. Derivada aritmética entera

Se llama función *derivada aritmética* en los enteros $\mathbb{Z}$ a la función $n' : \mathbb{Z} \to \mathbb{Z}$ dada por
(1) $0' = 1' = (-1)' =: 0$.
(2) Si $n = up_1p_2 \cdots p_k$ con $u = \pm 1$ y los p_i son primos (alguno de ellos puede estar repetido), entonces $n' := u \sum_{i=1}^{k} p_1 \cdots p_{i-1}p_{i+1} \cdots p_k$.
Nótese que si p es primo, entonces $k = 1$ y el producto anterior es vacío, por tanto $p' = 1$.

1) Demostrar que esta definición generaliza la derivada aritmética en $\mathbb{N}$.
2) Demostrar que $(-n)' = -n'$ para todo $n \in \mathbb{Z}$, y que se verifica la regla de Leibniz.
3) Calcular $(-60)'$.

solución. 1) En efecto, para $n = 0$ y $n = 1$ coinciden y para $n \geq 2$ con descomposición $n = \prod_{i=1}^{m} P_i^{n_i} = 1p_1p_2 \cdots p_k$ tenemos

$$n' = n \sum_{i=1}^{m} \frac{n_i}{P_i} = p_1p_2 \cdots p_k \left(\frac{1}{p_1} + \frac{1}{p_2} + \cdots + \frac{1}{p_k} \right)$$

$$= p_2p_3 \cdots p_k + p_1p_3 \cdots p_k + \ldots + p_1p_2 \cdots p_{k-1} = 1 \sum_{i=1}^{k} p_1 \cdots p_{i-1}p_{i+1} \cdots p_k.$$

2) Son consecuencia inmediatas de la definición.
3) $(-60)' = -(60)' = -\left(2^2 \cdot 3 \cdot 5\right)' = -60 \left(\frac{2}{2} + \frac{1}{3} + \frac{1}{5} \right) = -92$. □

169. Derivada aritmética racional

1) Demostrar que la función $(a/b)' : \mathbb{Q} \to \mathbb{Q}$ definida mediante

$$\left(\frac{a}{b} \right)' := \frac{a'b - b'a}{b^2},$$

es una extensión de la derivada aritmética en $\mathbb{Z}$ y cumple la regla de Leibniz.
2) Demostrar que es la única extensión que la cumple.
3) Completar la tabla

a	1	2	4	5	6	7	9
b	3	3	5	5	7	8	10
$(a/b)'$							

solución. 1) Veamos que $(a/b)'$ está bien definida, es decir que no depende del representante de cada número racional. En efecto, si $0 \neq k \in \mathbb{Z}$,

$$\left(\frac{ka}{kb} \right)' = \frac{(ka)'(kb) - (kb)'(ka)}{(kb)^2} = \frac{(k'a + ka')(kb) - (k'b + kb')(ka)}{(kb)^2}$$

$$= \frac{k^2(a'b - b'a)}{k^2b^2} = \frac{a'b - b'a}{b^2} = \left(\frac{a}{b}\right)'.$$

Es una extensión de la derivada aritmética en los enteros pues

$$\left(\frac{a}{1}\right)' = \frac{a'1 - 1'a}{1^2} = a'.$$

Cumple la regla de Leibniz:

$$\left(\frac{a}{b}\right)'\left(\frac{c}{d}\right) + \left(\frac{a}{b}\right)\left(\frac{c}{d}\right)' = \frac{a'b - b'a}{b^2} \cdot \frac{c}{d} + \frac{a}{b} \cdot \frac{c'd - d'c}{b^2}$$

$$= \frac{(a'c + ac')(bd) - (ac)(b'd + bd')}{b^2d^2} = \frac{(ac)'(bd) - (bd)'(ac)}{(bc)^2}$$

$$= \left(\frac{ac}{bd}\right)' = \left(\frac{a}{b} \cdot \frac{c}{d}\right)'.$$

2) No existe otra función de $\mathbb{Q}$ en $\mathbb{Q}$ que extienda a la derivada aritmética en $\mathbb{Z}$ y que cumpla la regla de Leibniz. En efecto, tal derivada ha de cumplir $1' = 0$ y se cumplen las equivalencias

$$1' = 0 \Leftrightarrow \left(n \cdot \frac{1}{n}\right)' = 0 \Leftrightarrow n' \cdot \frac{1}{n} + n \cdot \left(\frac{1}{n}\right)' = 0 \Leftrightarrow \left(\frac{1}{n}\right)' = -\frac{n'}{n^2}.$$

Es decir, necesariamente ha de ser $(1/n)' = -n'/n^2$ y de aquí se deduce que

$$\left(\frac{a}{b}\right)' = \left(a \cdot \frac{1}{b}\right)' = a' \cdot \frac{1}{b} + a \cdot \left(\frac{1}{b}\right)' = \frac{a'}{b} + a \cdot \frac{-b'}{b^2} = \frac{a'b - b'a}{b^2}.$$

3) Fácilmente verificamos:

a	1	2	4	5	6	7	9
b	3	3	5	5	7	8	10
$(a/b)'$	$-\frac{1}{9}$	$\frac{1}{9}$	$\frac{16}{25}$	0	$\frac{29}{49}$	$-\frac{19}{16}$	$-\frac{1}{10}$

□

170. Derivada aritmética en dominios de factorización única

Sea D un dominio de factorización única y elijamos en D los elementos irreducibles que son *positivos*, es decir elijamos un conjunto $\mathcal{P}$ de elementos irreducibles tales que cada elemento irreducible de D está asociado a uno y sólo un elemento de $\mathcal{P}$. Llamemos a $\mathcal{P}$ el conjunto de los *átomos positivos* y sea $\mathcal{U}$ el conjunto de las unidades de D. Para todo $a \in D$ definimos la derivada a' de a como sigue:

(1) Si $a = 0$ o $a \in \mathcal{U}$ entonces $a' = 0$.

(2) En otro caso, existen $u \in \mathcal{U}$, $p_1, \ldots, p_k \in \mathcal{P}$ (únicos salvo el orden y tal vez alguno repetido) tales que $a = up_1 \cdots p_k$. Entonces

$$a' := u \sum_{i=1}^{k} p_1 \cdots p_{i-1}p_{i+1} \cdots p_k.$$

Nota. Si $a = p \in \mathcal{P}$ entonces $k = 1$ y tenemos un producto vacío, con lo cual $a' = 1$. La función a' depende por supuesto de la elección de $\mathcal{P}$, en consecuencia se debería escribir $a'_{\mathcal{P}}$. No obstante y por simplicidad de notación, escribiremos a' cuando el conjunto de átomos positivos se sobreentienda.

1) Demostrar que la derivada $a'_{\mathcal{P}}$ definida en un dominio de factorización única D, satisface la regla de Leibniz.
2) En $D = \mathbb{Z}$, se consideran los conjuntos de átomos positivos

$$\mathcal{P}_1 = \{2, 3, 5, 7, \ldots\}, \quad \mathcal{P}_2 = \{2, -3, 5, -7, \ldots\}.$$

Calcular $(6)'_{\mathcal{P}_1}$ y $(6)'_{\mathcal{P}_2}$.
3) Si $D = \mathbb{R}[x]$, el conjunto de la unidades es $\mathcal{U} = \mathbb{R} \setminus \{0\}$. Elijamos como conjunto $\mathcal{P}$ de átomos positivos, el conjunto de los polinomios mónicos de primer grado unión el de los mónicos de segundo grado con discriminante menor que 0 y sea $f(x) = -x^4 + 2x^3 - 3x^2$. Calcular $(f(x))'_{\mathcal{P}}$.
4) *Nota.* Para todo dominio de factorización única D que no es un cuerpo y con la derivada aritmética $a'_{\mathcal{P}}$, se puede definir una derivada aritmética en su cuerpo de fracciones K que es extensión de $a'_{\mathcal{P}}$, de la misma manera que se hizo en $\mathbb{Q}$:

$$\left(\frac{a}{b}\right)'_{\mathcal{P}} = \frac{a'_{\mathcal{P}} b - b'_{\mathcal{P}} a}{b^2},$$

y la demostración es análoga.
Sea $\mathbb{R}[x]$ con los átomos positivos del apartado anterior. Calcular

$$\left(\frac{(x-1)^2}{x^2+1}\right)'.$$

SOLUCIÓN. 1) Denotemos a $a'_{\mathcal{P}}$ simplemente por a'. Tenemos que demostrar que para todo $a, b \in D$ se verifica $(ab)' = a'b + ab'$. Supongamos que tanto a como b no son nulos ni unidades, caso contrario el resultado es evidente. Sean $a = up_1 \cdots p_k$ y $b = vp_{k+1} \cdots p_m$ con u, v unidades y los $p_i \in \mathcal{P}$, entonces

$$\begin{aligned} a'b + ab' &= \left(u \sum_{i=1}^{k} p_1 \cdots p_{i-1} p_{i+1} \cdots p_k\right) (vp_{k+1} \cdots p_m) \\ &\quad + (up_1 \cdots p_k) \left(v \sum_{i=k+1}^{m} p_{k+1} \cdots p_{i-1} p_{i+1} \cdots p_m\right) \\ &= uv \sum_{i=1}^{k} p_1 \cdots p_{i-1} p_{i+1} \cdots p_k p_{k+1} \cdots p_m \\ &\quad + uv \sum_{i=k+1}^{m} p_1 \cdots p_k p_{k+1} \cdots p_{i-1} p_{i+1} \cdots p_m \\ &= (uv) \sum_{i=1}^{m} p_1 \cdots p_{i-1} p_{i+1} \cdots p_m = (ab)'. \end{aligned}$$

2) El conjunto de la unidades es $\mathcal{U} = \{1, -1\}$. Entonces,

$$(6)'_{\mathcal{P}_1} = (1 \cdot 2 \cdot 3)' = 1(3+2) = 5,$$
$$(6)'_{\mathcal{P}_2} = ((-1) \cdot 2 \cdot (-3))' = (-1)(-3+2) = 1.$$

Nótese que la derivada en $\mathbb{Z}$ que se definió en el problema 168 es la que corresponde a $\mathcal{P}_1$.
3) La descomposición de $f(x)$ en producto de irreducibles es $(-1) \cdot x \cdot x \cdot (x^2 - 2x + 3)$ y por tanto,

$$(f(x))'_{\mathcal{P}} = (-1)\left[x \cdot (x^2 - 2x + 3) + x \cdot (x^2 - 2x + 3) + x \cdot x\right]$$
$$= -2x^3 + 3x^2 - 6x.$$

4) Tenemos

$$\left((x-1)^2\right)' = x - 1 + x - 1 = 2x - 2, \quad (x^2+1)' = 1$$
$$\Rightarrow \left(\frac{(x-1)^2}{x^2+1}\right)' = \frac{(2x-2)(x^2+1) - 1 \cdot (x-1)^2}{(x^2+1)^2} = \frac{2x^3 - 3x^2 + 4x - 3}{(x^2+1)^2}.$$

□

171. Derivada aritmética y anillo $\mathbb{Z}[\sqrt{5}i]$

1) Demostrar que $\mathbb{Z}[\sqrt{5}i] = \{a + b\sqrt{5}i : a, b \in \mathbb{Z}\}$ es dominio de integridad con las operaciones habituales suma y producto de complejos pero que no es dominio de factorización única.
2) Demostrar que en $\mathbb{Z}[\sqrt{5}i]$ no se puede definir una derivada aritmética. Para ello, elegir diferentes conjuntos de átomos positivos.

solución. 1) Como $\mathbb{Z}[\sqrt{5}i] \subset \mathbb{C}$ bastará demostrar que $\mathbb{Z}[\sqrt{5}i]$ es subanillo de $\mathbb{C}$. Usamos el conocido teorema de caracterización de subanillos. Claramente, $\mathbb{Z}[\sqrt{5}i] \neq \emptyset$. Para cada par de elementos $a + b\sqrt{5}i$ y $c + d\sqrt{5}i$ de $\mathbb{Z}[\sqrt{5}i]$,

$$(a + b\sqrt{5}i) - (c + d\sqrt{5}i) = (a - c) + (b - d)\sqrt{5}i \in \mathbb{Z}[\sqrt{5}i],$$
$$(a + b\sqrt{5}i)(c + d\sqrt{5}i) = (ac - 5bd) + (ad + bc)\sqrt{5}i \in \mathbb{Z}[\sqrt{5}i].$$

Hemos demostrado pues que $\mathbb{Z}[\sqrt{5}i]$ es anillo. Dado que $\mathbb{C}$ es conmutativo, también lo es $\mathbb{Z}[\sqrt{5}i]$. Por otra parte $1 = 1 + 0i \in \mathbb{Z}[\sqrt{5}i]$, luego es unitario. Al ser $(\mathbb{C}, +, \cdot)$ es dominio de integridad, también lo es $\mathbb{Z}[\sqrt{5}i]$
Un elemento $a + b\sqrt{5}i \in \mathbb{Z}[\sqrt{5}i]$ no nulo es unidad si y sólo si existe un $a' + b'\sqrt{5}i \in \mathbb{Z}[\sqrt{5}i]$ no nulo tal que $(a + b\sqrt{5}i)(a' + b'\sqrt{5}i) = 1$. Tomando módulos al cuadrado, obtenemos $(a^2 + 5b^2)(a'^2 + 5b'^2) = 1$. Como los dos factores anteriores son enteros positivos, ha de ser necesariamente $a^2 + 5b^2 = 1$ o equivalentemente $a = \pm 1 \wedge b = 0$. Es decir, las únicas posibles unidades de $\mathbb{Z}[\sqrt{5}i]$ son $1, -1$. Pero estos elementos son efectivamente unidades al cumplirse $1 \cdot 1 = 1$, $(-1) \cdot (-1) = 1$. Concluimos que $\mathcal{U} = \{1, -1\}$. Expresemos

$6 = (a + b\sqrt{5}i)(c + d\sqrt{5}i)$ como producto de dos factores no nulos. Esto equivale a

$$\begin{cases} ac - 5bd = 6 \\ bc + ad = 0 \end{cases}$$

Resolviendo en las incógnitas c, d obtenemos

$$c = \frac{\begin{vmatrix} 6 & -5b \\ 0 & a \end{vmatrix}}{\begin{vmatrix} a & -5b \\ b & a \end{vmatrix}} = \frac{6a}{a^2 + 5b^2}\ ,\ d = \frac{\begin{vmatrix} a & 6 \\ b & 0 \end{vmatrix}}{\begin{vmatrix} a & -5b \\ b & a \end{vmatrix}} = \frac{-6b}{a^2 + 5b^2}.$$

Dando los valores $a = 1, b = 1$ obtenemos $c = 1, d = -1$ y por tanto

$$6 = (1 + \sqrt{5}i)(1 - \sqrt{5}i). \quad (1)$$

Por otra parte tenemos la factorización

$$6 = 2 \cdot 3 = (2 + 0\sqrt{5}i)(3 + 0\sqrt{5}i). \quad (2)$$

Veamos que los elementos $1 + \sqrt{5}i, 1 - \sqrt{5}i, 2, 3$ son irreducibles. En efecto, si $x + y\sqrt{5}i \in \mathbb{Z}[\sqrt{5}i]$ divide a $1 + \sqrt{5}i$, existe $u + v\sqrt{5}i \in \mathbb{Z}[\sqrt{5}i]$ tal que $1 + \sqrt{5}i = (x + y\sqrt{5}i)(u + v\sqrt{5}i)$. Tomando módulos al cuadrado queda $6 = (x^2 + 5y^2)(u + 5v^2)$ lo cual implica que $x^2 + 5y^2$ ha de dividir a 6. Esto ocurre en los casos $x = \pm 1, y = 0$ o $x = \pm 1, y = \pm 1$ es decir, los posibles divisores de $1 + \sqrt{5}i$ son ± 1, $\pm(1 + \sqrt{5}i)$, $\pm(1 - \sqrt{5}i)$. Los elementos ± 1 y $\pm(1 + \sqrt{5}i)$ claramente dividen a $1 + \sqrt{5}i$ pero los primeros son unidades y los segundos sus asociados. Por otra parte, $\pm(1 - \sqrt{5}i)$ no dividen a $1 + \sqrt{5}i$ pues

$$\frac{1 + \sqrt{5}i}{\pm(1 - \sqrt{5}i)} = \pm\frac{(1 + \sqrt{5}i)(1 + \sqrt{5}i)}{(1 - \sqrt{5}i)(1 + \sqrt{5}i)} = \pm\left(-\frac{2}{3} + \frac{\sqrt{5}}{3}i\right) \notin \mathbb{Z}[\sqrt{5}i].$$

Hemos demostrado que $1 + \sqrt{5}i$ es irreducible. De manera análoga podemos demostrar que $1 - \sqrt{5}i, 2, 3$ también lo son. Debido a las factorizaciones (1) y (2), concluimos que $\mathbb{Z}[\sqrt{5}i]$ no es dominio de factorización única.

2) Veamos que para cualquier elección $\mathcal{P}$ de los átomos positivos, no se puede construir una derivada aritmética en $\mathbb{Z}[\sqrt{5}i]$.

Caso 1. Elijamos un conjunto $\mathcal{P}$ de átomos positivos que contiene a los elementos irreducibles $2, 3, 1 + \sqrt{5}i, 1 - \sqrt{5}i$. Entonces,

$$6 = 2 \cdot 3 \Rightarrow 6' = 2 + 3 = 5,$$
$$6 = (1 + \sqrt{5}i)(1 - \sqrt{5}i) \Rightarrow 6' = (1 + \sqrt{5}i) + (1 - \sqrt{5}i) = 2.$$

Caso 2. Si $\mathcal{P}$ contiene a los elementos irreducibles $-2, 3, 1 + \sqrt{5}i, 1 - \sqrt{5}i$,

$$6 = (-1) \cdot (-2) \cdot 3 \Rightarrow 6' = (-1)\left((-2) + 3\right) = -1,$$
$$6 = (1 + \sqrt{5}i)(1 - \sqrt{5}i) \Rightarrow 6' = (1 + \sqrt{5}i) + (1 - \sqrt{5}i) = 2.$$

Caso 3. Si $\mathcal{P}$ contiene a los elementos irreducibles $2, -3, 1+\sqrt{5}i, 1-\sqrt{5}i$,

$$6 = (-1)\cdot 2\cdot(-3) \Rightarrow 6' = (-1)\,(2+(-3)) = 1,$$
$$6 = (1+\sqrt{5}i)(1-\sqrt{5}i) \Rightarrow 6' = (1+\sqrt{5}i)+(1-\sqrt{5}i) = 2.$$

Caso 4. Si $\mathcal{P}$ contiene a los elementos irreducibles $-2, -3, 1+\sqrt{5}i, 1-\sqrt{5}i$,

$$6 = (-2)\cdot(-3) \Rightarrow 6' = (-2)+(-3) = -5,$$
$$6 = (1+\sqrt{5}i)(1-\sqrt{5}i) \Rightarrow 6' = (1+\sqrt{5}i)+(1-\sqrt{5}i) = 2.$$

Caso 5. Si $\mathcal{P}$ contiene a los elementos irreducibles $-2, -3, 1+\sqrt{5}i, -1+\sqrt{5}i$,

$$6 = 2\cdot 3 \Rightarrow 6' = 2+3 = 5,$$
$$6 = (-1)\cdot(1+\sqrt{5}i)(-1+\sqrt{5}i) \Rightarrow$$
$$6' = (-1)\left((1+\sqrt{5}i)+(-1+\sqrt{5}i)\right) = -2\sqrt{5}i.$$

En todos los casos anteriores la derivada no está bien definida, y de manera análoga podemos verificar los restantes casos. □

172. Ecuación diofántica lineal en dos incógnitas

Una ecuación *diofántica* lineal en dos incógnitas es una ecuación de la

$$ax + by = c, \quad (a, b, c \in \mathbb{Z}, a \neq 0, b \neq 0). \qquad (E)$$

Se llama solución de la ecuación anterior a todo par de enteros (x, y) que la satisface.

1) Sea $d = \text{m.c.d.}\,(a, b)$. Demostrar que la ecuación (E) tiene alguna solución $\Leftrightarrow d \mid c$.

2) Hallar, si es posible, una solución particular de la ecuación diofántica $97x + 35y = 13$.

3) Hallar, si es posible, una solución particular de la ecuación diofántica $14x + 21y = 11$.

4) Sea la ecuación diofántica $ax + by = c$ con $d = \text{m.c.d.}\,(a, b) \mid c$. Demostrar que la solución general (i.e. todas las soluciones) de la ecuación es

$$\begin{cases} x = x_0 + k\frac{b}{d} \\ y = y_0 - k\frac{a}{d} \end{cases} \quad (k \in \mathbb{Z})$$

siendo (x_0, y_0) una solución particular.

5) Hallar la solución general de la ecuación diofántica $97x + 35y = 13$.

SOLUCIÓN. 1) $\Rightarrow$) Si la ecuación (E) tiene una solución entera (x_0, y_0), entonces $ax_0 + by_0 = c$. Como $d \mid a$ y $d \mid b$, se verifica $d \mid ax_0 + by_0 = c$. $\Leftarrow$) Tenemos

$$\text{m.c.d.}\left(\frac{a}{d}, \frac{b}{d}\right) = 1 \underbrace{\Rightarrow}_{\text{Id. Bezout}} \exists p, q \in \mathbb{Z} : p\frac{a}{d} + q\frac{b}{d} = 1$$
$$\Rightarrow a\frac{pc}{d} + b\frac{qc}{d} = c.$$

Por hipótesis $d \mid c$ con lo cual $(x_0, y_0) = \left(\frac{pc}{d}, \frac{qc}{d}\right)$ es solución de (E). Nótese, que esto proporciona un método para hallar una solución particular de la ecuación diofántica (E).
2) Usando el algortitmo de Euclides:

	2	1	3	2	1	2
97	35	27	8	3	2	1
27	8	3	2	1	0	

con lo cual $d = \text{m.c.d.}\,(97, 35) = 1 \mid 13$ y la ecuación tiene soluciones. Tenemos las relaciones:

$$\begin{aligned} 3 &= 1 \cdot 2 + 1 \\ 8 &= 3 \cdot 2 + 2 \\ 27 &= 8 \cdot 3 + 2 \\ 35 &= 1 \cdot 27 + 8 \\ 97 &= 2 \cdot 35 + 27. \end{aligned}$$

Expresemos $d = 1$ como combinación lineal de 97 y 35. Tenemos

$$1 = 3 - 2 = 3 - (8 - 3 \cdot 2) = 3 \cdot 3 - 8 = 3 \cdot (27 - 3 \cdot 8) - 8$$

$$= 3 \cdot 27 - 10 \cdot 8 = 3 \cdot 27 - 10 \cdot (35 - 27) = 13 \cdot 27 - 10 \cdot 35$$

$$= 13 \cdot (97 - 2 \cdot 35) - 10 \cdot 35 = \underbrace{13}_{p} \cdot 97 + \underbrace{(-36)}_{q} \cdot 35.$$

Según el apartado anterior, una solución particular de la ecuación diofántica es

$$(x_0, y_0) = \left(\frac{pc}{d}, \frac{qc}{d}\right) = (13 \cdot 13, (-36) \cdot 13) = (169, -468).$$

3) Tenemos $d = \text{m.c.d.}\,(14, 21) = 7$, que no divide a 11, por tanto la ecuación no tiene soluciones.
4) Como $d \mid c$, del apartado 1 deducimos que existe una solución particular (x_0, y_0). Sea (x_1, y_1) cualquier solución de la ecuación, entonces

$$\begin{cases} \frac{a}{d}x_1 + \frac{b}{d}y_1 = \frac{c}{d} \\ \frac{a}{d}x_0 + \frac{b}{d}y_0 = \frac{c}{d} \end{cases} \Rightarrow \frac{a}{d}(x_1 - x_0) + \frac{b}{d}(y_1 - y_0) = 0$$

$$\Rightarrow \frac{a}{d}(x_1 - x_0) = \frac{b}{d}(y_0 - y_1) \Rightarrow \frac{b}{d} \mid \frac{a}{d}(x_1 - x_0).$$

Pero a/d y b/d son primos entre si, por tanto $\frac{b}{d} \mid (x_1 - x_0)$, con lo cual existe $k \in \mathbb{Z}$ tal que $x_1 - x_0 = k\frac{b}{d}$, luego $x_1 = x_0 + k\frac{b}{d}$. Sustituyendo en

$$\frac{a}{d}(x_1 - x_0) + \frac{b}{d}(y_1 - y_0) = 0,$$

$$\frac{a}{d} \cdot k \cdot \frac{b}{d} + \frac{b}{d}(y_1 - y_0) = 0 \Rightarrow \frac{a}{d} \cdot k + y_1 - y_0 = 0 \Rightarrow y_1 = y_0 - k\frac{a}{d}.$$

Hemos demostrado que cualquier solución (x_1, y_1) de la ecuación diofántica es necesariamente de la forma dada. Falta demostrar que son efectivamente soluciones. Pero,

$$ax_1 + by_1 = a\left(x_0 + k\frac{b}{d}\right) + b\left(y_0 - k\frac{a}{d}\right)$$

$$= ax_0 + ak\frac{b}{d} + by_0 - bk\frac{a}{d} = ax_0 + by_0 = c.$$

5) En el apartado 2 vimos que $d = 1$ y que una solución particular es $(169, -468)$. Usando el teorema anterior, obtenemos la solución general:

$$\begin{aligned} x &= 169 + 35k \\ y &= -468 - 97k \end{aligned} \quad (k \in \mathbb{Z}).$$

□

173. Teorema del valor medio escalar

1) Demostrar el teorema del valor medio escalar:
Sea E un espacio nornado, $A \subset E$ abierto y $f : A \to \mathbb{R}$ diferenciable. Sean $a, b \in A$ con $a \neq b$ tales que el segmento $[a, b] \subset A$. Entonces, existe $c \in (a, b)$ tal que

$$f(b) - f(a) = Df(c)(b - a).$$

2) Verificar la validez del teorema del valor medio escalar para la función $f : \mathbb{R}^2 \to \mathbb{R}$ dada for $f(x, y) = x^2 + 2y^2$ en el intervalo $[a, b]$ con $a = (0, 0)$, $b = (1, 1)$.
3) Demostrar que el teorema del valor medio escalar no se puede extender a campos no escalares. Para ello, considerar $f : E = \mathbb{R} \to \mathbb{R}^2$ dada por

$$f(t) = (\cos t, \sin t)^T \quad \forall t \in \mathbb{R}$$

y cualquier intervalo cerrado de $\mathbb{R}$ de amplitud 2π.

solución. 1) Consideremos la función $\varphi : [0, 1] \to \mathbb{R}$ dada por $\varphi(t) = f((1 - t)a + tb)$. Ésta función es continua en $[0, 1]$ y por la regla de la cadena,

$$\varphi'(t) = Df((1 - t)a + tb)(b - a) \quad \forall t \in (0, 1).$$

Aplicando a φ el teorema del valor medio para funciones reales de variable real, existe $t_0 \in (0, 1)$ tal que

$$f(b) - f(a) = \varphi(1) - \varphi(0) = \varphi'(t_0) = Df((1 - t_0)a + t_0 b)(b - a).$$

Basta ahora elegir $c = (1 - t_0)a + t_0 b$.
2) Las parciales de f son $\frac{\partial f}{\partial x} = 2x$, $\frac{\partial f}{\partial y} = 4y$, que son continuas en $\mathbb{R}^2$ y por tanto f es diferenciable en $\mathbb{R}^2$. El segmento (a, b) es

$$(a, b) = \{(1 - t)(0, 0) + t(1, 1) : 0 < t < 1\} = \{(t, t) : 0 < t < 1\}.$$

Cualquier $c \in (a,b)$ es por tanto de la forma $c = (t,t)$ con $0 < t < 1$. Entonces,

$$f(b) - f(a) = Df(c)(b-a) \Leftrightarrow 3 - 0 = \nabla f(t,t) \cdot (1,1)$$

$$\Leftrightarrow 3 = (2t, 6t) \cdot (1,1) \Leftrightarrow 3 = 8t \Leftrightarrow t = 3/8,$$

y $c = (3/8, 3/8) \in (a,b)$.
3) Las funciones componentes de f son $f_1(t) = \cos t$ y $f_2(t) = \sin t$ y

$$\frac{\partial f_1}{\partial t} = -\sin t, \quad \frac{\partial f_2}{\partial t} = \cos t$$

que son continuas en todo $\mathbb{R}$, y por tanto f es diferenciable en $\mathbb{R}$. Si consideramos el intervalo cerrado $[a,b] = [a, a+2\pi]$ y $c \in (a,b)$, entonces,

$$Df(c)(b-a) = \begin{pmatrix} -\sin c \\ \cos c \end{pmatrix} (2\pi).$$

Por otra parte,

$$f(b) - f(a) = \begin{pmatrix} \cos(a+2\pi) \\ \sin(a+2\pi) \end{pmatrix} - \begin{pmatrix} \cos a \\ \sin a \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

Pero $Df(c)(b-a) \neq (0,0)^T$ para todo c, con lo cual no se verifica $f(b) - f(a) = Df(c)(b-a)$. □ □

174. El número e es trascendente

Demostrar que el número real e es trascendente sobre $\mathbb{Q}$, es decir que no existe $p \in \mathbb{Q}[x]$ no nulo tal que $p(e) = 0$.

solución. Sea $f \in \mathbb{R}[x]$ de grado r y sea

$$F(x) = f(x) + f'(x) + f''(x) + \cdots + f^{(r)}(x).$$

Hallemos la derivada de $h(x) = e^{-x}F(x)$:

$$\frac{d}{dx}\left(e^{-x}F(x)\right) = -e^{-x}\left(f(x) + f'(x) + f''(x) + \cdots + f^{(r)}(x)\right)$$

$$+e^{-x}\left(f'(x) + f''(x) + \cdots + f^{(r)}(x) + f^{(r+1)}(x)\right) \underbrace{=}_{f^{(r+1)}(x)=0} e^{-x}f(x).$$

La función h satisface las hipótesis del valor medio de Lagrange en todo intervalo de la forma $[0,k]$ con $k > 0$ es decir, existe $\xi_k \in (0,k)$ tal que

$$h'(\xi_k) = \frac{h(k) - h(0)}{k - 0} = \frac{e^{-k}F(k) - F(0)}{k}.$$

Dado que $\xi_k = \theta_k k$ con $0 < \theta_k < 1$, y que $h'(\xi_k) = -e^{-\xi_k} f(\xi_k)$ podemos escribir $e^{-k}F(k) - F(0) = -e^{-\theta_k k} f(\theta_k k)\, k$ con $0 < \theta_k < 1$. Multiplicando

pr e^k obtenemos $F(k) - e^k F(0) = -e^{(1-\theta_k)k} f(\theta_k k)\, k$ con $0 < \theta_k < 1$. Para $k = 1, 2, \ldots n$ obtenemos

$$\begin{aligned} &F(1) - eF(0) = -e^{(1-\theta_1)} f(\theta_1) = \epsilon_1 \\ &F(2) - e^2 F(0) = -2e^{2(1-\theta_2)} f(2\theta_k) = \epsilon_2 \\ &\ldots \\ &F(n) - e^n F(0) = -ne^{n(1-\theta_n)} f(n\theta_n) = \epsilon_n. \end{aligned} \qquad (1)$$

Supongamos que e no es trascendente sobre $\mathbb{Q}$, entonces se satisface una relación de la forma $b_n e^n + b_{n-1} e^{n-1} + \cdots + b_1 e + b_0 = 0$ con los $b_j \in \mathbb{Q}$ no todos nulos. Podemos suponer sin pérdida de generalidad que se satisface una relación de la forma

$$c_n e^n + c_{n-1} e^{n-1} + \cdots + c_1 e + c_0 = 0 \qquad (2)$$

con los $c_j \in \mathbb{Z}$ y $c_0 > 0$. En las relaciones (1) multipliquemos la primera igualdad por c_1, la segunda por c_2, etc. Sumando obtenemos

$$\begin{aligned} c_1 F(1) + c_2 F(2) + \cdots + c_n F(n) - F(0)\left(c_1 e + c_2 e^2 + \ldots + c_n e^n\right) \\ = c_1\epsilon_1 + c_2\epsilon_2 + \ldots + c_n\epsilon_n. \end{aligned}$$

Usando (2) queda

$$c_0 F(0) + c_1 F(1) + c_2 F(2) + \cdots + c_n F(n) = c_1\epsilon_1 + c_2\epsilon_2 + \ldots + c_n\epsilon_n. \qquad (3)$$

Todo el anterior desarrollo es válido para cualquier polinomio $f(x)$. Ahora, vamos a elegir en concreto el polinomio

$$f(x) = \frac{1}{(p-1)!} x^{p-1}(1-x)^p (2-x)^p \cdots (n-x)^p$$

en donde p es un número primo con $p > n$ y $p > c_0$. Al desarrollar, obtenemos un polinomio de la forma

$$f(x) = \frac{(n!)^p}{(p-1)!} x^{p-1} + \frac{a_0}{(p-1)!} x^p + \frac{a_1}{(p-1)!} x^{p+1} + \cdots$$

con $a_1, a_2 \ldots$, enteros. Demostremos que si $i \geq p$ la derivada i-ésima $f^{(i)}(x)$ es un polinomio con coeficientes enteros y todos múltiplos de p. En efecto el primer sumando es un monomio de grado $p-1$ y por tanto, su derivada i-ésima es 0 si $i \geq p$. Los demás monomios son de la forma $m_k(x) = \frac{a_k}{(p-1)!} x^{p+k}$ con $k \geq 0$. Hallemos sus derivadas sucesivas.

$$\begin{aligned} m_k(x) &= \frac{a_k}{(p-1)!} x^{p+k}, \\ m_k'(x) &= \frac{a_k}{(p-1)!} (p+k) x^{p+k-1}, \\ m_k''(x) &= \frac{a_k}{(p-1)!} (p+k)(p+k-1) x^{p+k-2}, \\ &\ldots \\ m_k^{(p)}(x) &= \frac{a_k}{(p-1)!} (p+k)(p+k-1)\ldots(p+k-(p-1)) x^{p+k-p} \end{aligned}$$

$$= \frac{a_k}{(p-1)!}(p+k)(p+k-1)\dots(k+1)x^k = \frac{a_k}{(p-1)!}\cdot\frac{(p+k)!}{k!}x^k$$
$$= \frac{a_k(p)!}{(p-1)!}\cdot\frac{(p+k)!}{(p!)(k!)}x^k = pa_k\binom{p+k}{k}x^k.$$

El coeficiente del monomio $m_k^{(p)}(x)$ es por tanto entero y múltiplo de p y obviamente de la misma manera será el coeficiente de $m_k^{(i)}(x)$ para $i \geq p$. Como consecuencia, para todo entero j se verifica $f^{(i)}(j)$ es entero y múltiplo de p si $i \geq p$.

Por su propia construcción, $f(x)$ tiene a $x = 1, 2, \dots, n$ como raíces de multiplicidad p. Entonces, para $j = 1, 2, \dots, n$ se verifica $f(j) = 0$, $f'(j) = 0$, $\dots$, $f^{(p-1)}(j) = 0$ y por tanto

$$F(j) = f(j) + f'(j) + \cdots + f^{(p-1)}(j) + f^{(p)}(j) + \cdots + f^{(r)}(j)$$

y por lo demostrado anteriormente $F(j)$ es entero y múltiplo de p para todo $j = 1, 2, \dots, n$. Como $x = 0$ es raíz de multiplicidad $p-1$ de $f(x)$, se verifica $f(0) = f'(0) = \dots = f^{(p-2)}(0) = 0$. Para $i \geq p$, $f^{(i)}(0)$ es entero y múltiplo de p y $f^{(p-1)}(0) = (n!)^p$. Al ser p primo y $p > n$, $p \not| (n!)^p$ es decir $f^{(p-1)}(0)$ no es divisible por p. Al ser

$$F(0) = f(0) + f'(0) + \dots + f^{(p-2)}(0) + f^{(p-1)}(0) + f^{(p)}(0) + \dots + f^{(r)}(0)$$
$$= f^{(p-1)}(0) + f^{(p)}(0) + \dots + f^{(r)}(0)$$

se cumple que $F(0)$ es entero y no divisible por p. Al ser

$$c_0 > 0,\ p > c_0,\ p \not| F(0),\ p \mid F(1),\ p \mid F(2)\ , \dots,\ p \mid F(n)$$

podemos asegurar que $c_0F(0)+c_1F(1)+\dots+c_nF(n)$ es entero y no divisible por p.

Las relaciones (1) expresan $-ie^{i(1-\theta_i)}f(i\theta_i) = \epsilon_i$ para todo $i = 1, \dots, n$ por tanto,

$$\epsilon_i = \frac{-ie^{i(1-\theta_i)}(i\theta_i)^{p-1}(1-i\theta_i)^p\dots(n-i\theta_i)^p}{(p-1)!} \quad (0 < \theta_i < 1).$$

Acotemos los ϵ_i en valor absoluto:

$$|\epsilon_i| \leq \frac{e^n n^p (n!)^p}{(p-1)!}.$$

Hallemos el límite de los ϵ_i cuando $p \to +\infty$. Tenemos

$$0 \leq |\epsilon_i| = e^n(n\cdot n!)\cdot\frac{(n\cdot n!)^{p-1}}{(p-1)!} \underbrace{\to}_{\text{si } p\to+\infty} 0$$

pues la exponencial es un infinito de orden menor que el factorial. Es decir, $\epsilon_i \to 0$ cuando $p \to +\infty$.

Podemos elegir un primo mayor que n y que c_0 que sea suficientemente grande para que ocurra $|c_1\epsilon_1 + \dots + c_n\epsilon_n| < 1$. Pero por (3), $c_1\epsilon_1 + \dots + c_n\epsilon_n = c_0F(0)+\dots+c_nF(n)$ y por tanto ha de ser entero. Dado que en valor

absoluto es menor que 1, la única opción es que $c_0F(0)+\ldots+c_nF(n)=0$. Pero habíamos visto que $p \not| c_0F(0)+\ldots+c_nF(n)$ y sin embargo $p \mid 0$ lo cual es una contradicción. Es decir, de suponer que e no es trascendente llagamos a una contradicción. Concluimos pues que e es trascendente. □

175. Desigualdad de Jensen

El teorema de la desigualdad de Jensen, se expresa en los siguientes términos: Sea $(\Omega, \mathscr{M}, \mu)$ un espacio de medida con $\mu(\Omega)=1$. Sea $f:\Omega\to\mathbb{R}$ tal que:
a) $f\in L^1(\mu)$.
b) $a<f(x)<b$ para todo $x\in(a,b)$.
c) $\varphi:(a,b)\to\mathbb{R}$ es convexa.
Entonces, se verifica la desigualdad de Jenssen

$$\varphi\left(\int_\Omega f d\mu\right)\leq\int_\Omega(\varphi\circ f)\,d\mu.$$

Sean $y_1,\ldots,y_n$ números positivos. Aplicar la desigualdad de Jensen para demostrar que

$$\sqrt[n]{y_1\ldots y_n}\leq\frac{y_1+\ldots+y_n}{n}$$

es decir, que la media geométrica es menor o igual que la media aritmética.

solución. Consideremos el espacio de medida $(\Omega,\mathscr{M},\mu)$ con $\Omega=\{p_1,\ldots,p_n\}$ un conjunto finito, $\mathscr{M}=\mathscr{P}(\Omega)$ y la medida μ determinada por $\mu(p_i)=1/n$ para todo $i=1,\ldots,n$. Se verifica

$$\mu(\Omega)=\mu(p_1)+\ldots+\mu(p_n)=1/n+\ldots+1/n=1.$$

Consideremos ahora la función $f:\Omega\to\mathbb{R}$ dada por $f(p_i)=x_i$ para $x_i\in\mathbb{R}$ genéricos. La función f es claramente simple y medible y $\int|f|\,d\mu=\sum_{i=1}^n|x_i|\,\mu(p_i)<+\infty$ es decir, $f\in L^1(\mu)$. Por otra parte, $a<f(x)<b$ para

$$a<\text{mín}\{x_1,\ldots,x_n\},\quad \text{máx}\{x_1,\ldots,x_n\}<b.$$

Elijamos la función convexa en (a,b) dada por $\varphi(x)=e^x$. Tenemos,

$$\varphi\left(\int_\Omega f d\mu\right)=e^{\int_\Omega f d\mu}=e^{x_1(1/n)+\ldots+x_n(1/n)}=\sqrt[n]{e^{x_1}\ldots e^{x_n}},$$

$$\int_\Omega(\varphi\circ f)\,d\mu=\int_\Omega e^f d\mu=e^{x_1}\cdot\frac{1}{n}+\ldots+e^{x_n}\cdot\frac{1}{n}.$$

Por la desigualdad de Jensen,

$$\sqrt[n]{e^{x_1}\ldots e^{x_n}}\leq\frac{e^{x_1}+\ldots+e^{x_n}}{n}.$$

Dados los números positivos $y_1,\ldots,y_n$ y eligiendo $x_1,\ldots,x_n$ tales que $y_i=e^{x_i}$ para todo $i=1,\ldots,n$ queda

$$\sqrt[n]{y_1\ldots y_n}\leq\frac{y_1+\ldots+y_n}{n}.$$

□ □

176. Topología final

Sea $f_i : (X, T_i) \to Y, i \in I$ una familia de aplicaciones de los espacios topológicos (X_i, T_i) en el conjunto Y.

1) Demostrar que $T_F = \{V \subset Y : f_i^{-1}(V) \in T_i \ \ \forall i \in T_i\}$ es una topología en Y. A la topología T_F se la llama topología *final* determinada por las aplicaciones f_i.
2) Demostrar que la topología final T_F es la mayor topología en Y de entre todas las que hacen a las f_i continuas.
3) Sea $f_i : (X, T_i) \to Y, i \in I$ una familia de aplicaciones de los espacios topológicos (X_i, T_i) en el conjunto Y. Sea (Z, T) un espacio topológico. Demostrar que una aplicación $g : (Y, T_F) \to (Z, T)$ es continua si y sólo si todas las composiciones $g \circ f_i$ son continuas.
4) Recíprocamente, demostrar que si una topología T' en Y cumple

$$g : (Y, T') \to (Z, T) \text{ es continua} \Leftrightarrow g \circ f_i \text{ es continua para todo } i \in I$$

entonces, T' es la topología final T_F.

solución. 1) Se verifican los tres axiomas de topología:
(i) $f_i^{-1}(\emptyset) = \emptyset \in T_i$ para todo $i \in I$ luego $\emptyset \in T_F$. Por orta parte, $f_i^{-1}(Y) = \emptyset \in T_i$ para todo $i \in I$ y por tanto $T \in T_F$.
(ii) Si $\{V_j : j \in J\}$ es una colección de elementos de T_F, para todo $i \in I$ se verifica

$$f_i^{-1}\left(\bigcup_{j\in J} V_j\right) = \bigcup_{j\in J} \underbrace{f_i^{-1}(V_j)}_{\in T_i} \in T_i,$$

lo cual implica que $\cup_{j\in J} V_j \in T_F$.
(iii) Si V_1, V_2 son elementos de T_F, para todo $i \in I$ se verifica

$$f_i^{-1}(V_1 \cap V_2) = \underbrace{f_i^{-1}(V_1)}_{\in T_i} \cap \underbrace{f_i^{-1}(V_2)}_{\in T_i} \in T_i$$

lo cual implica que $V_1 \cap V_2 \in T_F$.
2) En efecto, sea T una topología en Y tal que todas las f_i son continuas. Si $V \in T$, entonces $f_i^{-1}(V) \in T_i$ para todo $i \in V$ y por tanto $V \in T_F$. Es decir, $T \subset T_F$.
3) La aplicaciones $f_i : (X_i, T_i) \to (Y, T_F)$ son continuas, por tanto si $g : (Y, T_F) \to (Z, T)$ es continua las $g \circ f_i$ también lo son (composición de continuas). Supongamos ahora que las aplicaciones $g \circ f_i$ son continuas. Si $W \in T$,

$$f_i^{-1}(g^{-1}(W)) = (g \circ f_i)^{-1}(W) \in T_i \text{ para todo } i,$$

con lo cual $g^{-1}(W) \in T_F$ y por tanto g es continua.
4) Consideremos las composiciones

$$f_i : (X, T_i) \xrightarrow{f_i} (Y, T') \xrightarrow{I_1} (Y, T_F),$$
$$f_i : (X, T_i) \xrightarrow{f_i} (Y, T_F) \xrightarrow{I_2} (Y, T'),$$

en donde tanto I_1 como I_2 representan la aplicación identidad en Y. Por el apartado anterior, la continuidad de las aplicaciones $f_i = I_1 \circ f_i$ para todo i implica que I_1 es continua, por tanto si $V \in T_F$ entonces $I_1^{-1}(V) = V \in T'$, es decir $T_F \subset T'$. Por hipótesis, la continuidad de las aplicaciones $f_i = I_2 \circ f_i$ para todo i implica que I_2 es continua, por tanto si $V \in T'$ entonces $I_2^{-1}(V) = V \in T_F$, es decir $T' \subset T_F$. Concluimos que T' es la topología final T_F. □

177. Operador de Sturm-Liouville

Sea $C[a, b]$ el espacio vectorial de las funciones reales continuas en $[a, b]$ y $p \in C[a, b]$ fijo. Sea $C^2[a, b]$ el espacio vectorial de las funciones reales de clase 2 en $[a, b]$. Se define el conjunto:

$$E = \{f \in C^2[a, b] : p(a)f(a) = 0 \ \wedge \ p(b)f(b) = 0\}.$$

1) Demostrar que E es un subespacio vectorial de $C[a, b]$.
2) Si $q \in C[a, b]$ fijo se define la aplicación $T : E \to C[a, b]$ de la forma

$$T(f) = \left(pf'\right)' + qf.$$

Demostrar que T es lineal (se la llama operador de *Sturm-Liouville*).
3) Se considera en $C[a, b]$ el producto escalar $\langle h_1, h_2\rangle = \int_a^b h_1 h_2 dx$. Demostrar que

$$\langle T(f), g\rangle = \langle f, T(g)\rangle \quad \forall f, g \in E$$

es decir, el operador de Sturm-Liouville es simétrico.
4) Sean λ y μ autovalores de T con correspondientes autofunciones f y g. Demostrar que si $\lambda \neq \mu$, las autofunciones f y g son ortogonales.

solución. 1) Claramente $E \subset C[a, b]$. La función nula 0 es de clase 2 y satisface $p(a) \cdot 0(a) = p(b) \cdot 0(b) = 0$, luego $0 \in E$. Si $\alpha_1, \alpha_2 \in \mathbb{R}$ y $f_1, f_2 \in E$ entonces $\alpha_1 f_1 + \alpha_2 f_2$ es de clase dos en $[a, b]$ y

$$p(a)\left(\alpha_1 f_1 + \alpha_2 f_2\right)(a) = p(a)\left(\alpha_1 f_1(a) + \alpha_2 f_2(a)\right)$$
$$= \alpha_1 p(a) f_1(a) + \alpha_2 p(a) f_2(a) = \alpha_1 \cdot 0 + \alpha_2 \cdot 0 = 0$$

y análogamente cambiando b por a, luego $\alpha_1 f_1 + \alpha_2 f_2 \in E$, y E es subespacio de $C[a, b]$.
2) La aplicación está bien definida pues para todo $f \in E$, la aplicación $T(f)$ es continua en $[a, b]$. Si $\alpha_1, \alpha_2 \in \mathbb{R}$ y $f_1, f_2 \in E$ entonces

$$T\left(\alpha_1 f_1 + \alpha_2 f_2\right) = \left(p\left(\alpha_1 f_1 + \alpha_2 f_2\right)'\right)' + q\left(\alpha_1 f_1 + \alpha_2 f_2\right)$$
$$= \left(p\left(\alpha_1 f_1' + \alpha_2 f_2'\right)\right)' + \alpha_1(q f_1) + \alpha_2(q f_2)$$

$$\begin{aligned}
&= \left(\alpha_1 \left(pf_1'\right) + \alpha_2 \left(pf_2'\right)\right)' + \alpha_1(qf_1) + \alpha_2(qf_2) \\
&= \alpha_1 \left(pf_1'\right)' + \alpha_2 \left(pf_2'\right)' + \alpha_1(qf_1) + \alpha_2(qf_2) \\
&= \alpha_1 \left(\left(pf_1'\right)' + qf_1\right) + \alpha_2 \left(\left(pf_2'\right)' + qf_2\right) \\
&= \alpha_1 T(f_1) + \alpha_2 T(f_2)
\end{aligned}$$

luego T es lineal.
3) Tenemos por una parte

$$\begin{aligned}
\langle T(f), g\rangle &= \int_a^b T(f)g\, dx = \int_a^b \left(\left(pf'\right)' + qf\right) g\, dx \\
&= \int_a^b \left(pf'\right)' g\, dx + \int_a^b qfg\, dx.
\end{aligned}$$

Aplicando integración por partes a la primera integral con $u = g$, $dv = (pf')'$ obtenemos $du = g'dx$ y $v = pf'$, con lo cual

$$\langle T(f), g\rangle = \left[gpf'\right]_a^b - \int_a^b pf'g'dx + \int_a^b qfg\, dx.$$

Procediendo de la misma manera obtenemos

$$\langle f, T(g)\rangle = \left[fpg'\right]_a^b - \int_a^b pg'f'dx + \int_a^b fqg\, dx.$$

Queda entonces $\langle T(f), g\rangle - \langle f, T(g)\rangle = [gpf' - fpg']_a^b$. Pero al ser f y g funciones de E se verifica $p(a)f(a) = p(b)f(b) = p(a)g(a) = p(b)g(b) = 0$ con lo cual $\langle T(f), g\rangle - \langle f, T(g)\rangle = 0$ y la propiedad queda demostrada.
4) Dado que el operador de Sturm-Liouville T satisface $\langle T(f), g\rangle = \langle f, T(g)\rangle$, tenemos $\langle \lambda f, g\rangle = \langle f, \mu g\rangle$ o bien $\lambda\langle f, g\rangle = \mu\langle f, g\rangle$ o bien $(\lambda - \mu)\langle f, g\rangle = 0$. Al ser $\lambda - \mu \neq 0$, queda $\langle f, g\rangle = 0$. □

178. Ecuación de Legendre

Se llama *ecuación de Legendre* a la ecuación diferencial

$$(1 - x^2)y'' - 2xy' + \alpha(\alpha + 1)y = 0 \qquad (L)$$

con α real.
1) Demostrar que la ecuación de Legendre se puede escribir en la forma

$$\left((x^2 - 1)y'\right)' = \alpha(\alpha + 1)y.$$

2) Demostrar que la ecuación de Legendre se puede escribir en la forma $T(y) = \lambda y$ con $\lambda = \alpha(\alpha + 1)$ y T un operador de Sturm-Liouville.
3) Demostrar que la ecuación de Legendre tiene dos soluciones analíticas en el intervalo $(-1, 1)$ y que son linealmente independientes.
4) Demostrar que $y = \sum_{n\geq 0} a_n x^n$ es solución de la ecuación de Legendre si y sólo si se verifica

$$a_{n+2} = -\frac{(\alpha - n)(n + \alpha + 1)}{(n + 2)(n + 1)} a_n \quad \forall n \geq 0. \qquad (*)$$

5) Determinar a_n en función de a_0 para n par y en función de a_1 para n impar.
6) Determinar dos soluciones linealmente independientes de (L) en el intervalo $(-1,1)$ y deducir la solución general.

SOLUCIÓN. 1) Tenemos las equivalencias

$$\left((x^2-1)y'\right)' = \alpha(\alpha+1)y \Leftrightarrow 2xy' + (x^2-1)y'' = \alpha(\alpha+1)y$$
$$\Leftrightarrow (1-x^2)y'' - 2xy' + \alpha(\alpha+1)y = 0.$$

2) Recordamos que dadas dos funciones fijas $p, q \in C[a,b]$ un operador de Sturm-Liouville es una aplicación lineal de la forma

$$T : E = \{f \in C^2[a,b] : p(a)f(a) = 0 \ \wedge \ p(b)f(b) = 0\} \to C[a,b]$$

dado por $T(f) = (pf')' + qf$. Si elegimos $p = x^2 - 1$ y $q = 0$ tenemos que $p(1) = p(-1) = 0$ y el correspondiente operador de Sturm-Liouville es

$$T : E = \{f \in C^2[-1,1] : p(-1)f(-1) = p(1)f(1) = 0\} \to C[-1,1]$$

dado por $T(y) = \left((x^2-1)y'\right)'$. Pero $T(y) = \lambda y$ equivale a $\left((x^2-1)y'\right)' = \alpha(\alpha+1)y$, que según el apartado anterior es la ecuación de Legendre.
3) Recordamos que una ecuación diferencial homogénea de segundo orden $y'' + P(x)y' + Q(x)y = 0$ con coeficientes analíticos $P(x)$ y $Q(x)$ en un intervalo $(x_0 - r, x_0 + r)$ tiene dos soluciones analíticas y linealmente independientes en el mismo intervalo. Para $x \in (-1,1)$ la ecuación de Legendre se puede escribir en la forma

$$y'' \underbrace{-\frac{2x}{1-x^2}}_{P(x)} y' + \underbrace{\frac{\alpha(\alpha+1)}{1-x^2}}_{Q(x)} y = 0.$$

Ahora bien, para $x \in (-1,1)$ se verifica $1/(1-x^2) = \sum_{n\geq 0} x^{2n}$ con lo cual, $P(x)$ y $Q(x)$ son analíticas en $(-1,1)$.
4) Tenemos

$$y = \sum_{n\geq 0} a_n x^n, \quad y' = \sum_{n\geq 1} n a_n x^{n-1}, \quad y'' = \sum_{n\geq 2} n(n-1)a_n x^{n-2}$$
$$2xy' = \sum_{n\geq 1} 2n a_n x^n = \sum_{n\geq 0} 2n a_n x^n$$
$$(1-x^2)y'' = \sum_{n\geq 2} n(n-1)a_n x^{n-2} - \sum_{n\geq 2} n(n-1)a_n x^n$$
$$= \sum_{n\geq 0} (n+2)(n+1)a_{n+2} x^n - \sum_{n\geq 0} n(n-1)a_n x^n$$
$$= \sum_{n\geq 0} \left[(n+2)(n+1)a_{n+2} - n(n-1)a_n\right] x^n.$$

Sustituyendo en (L) la ecuación se satisface si y sólo si se cumple la relación

$$(n+2)(n+1)a_{n+2} - n(n-1)a_n - 2na_n + \alpha(\alpha+1) = 0$$

para todo $n \geq 0$. Operando, podemos escribir la relación anterior en la forma

$$a_{n+2} = -\frac{(\alpha - n)(n + \alpha + 1)}{(n+2)(n+1)} a_n.$$

5) Para los coeficientes con índice par tenemos

$$a_2 = -\frac{\alpha(\alpha+1)}{1 \cdot 2} a_0,$$

$$a_4 = -\frac{(\alpha-2)(\alpha+3)}{3 \cdot 4} a_2 = (-1)^2 \frac{\alpha(\alpha-2)(\alpha+1)(\alpha+3)}{4!} a_0,$$

y fácilmente se demuestra por inducción que

$$a_{2n} = (-1)^n \frac{\alpha(\alpha-2)\cdots(\alpha-2n+2)(\alpha+1)(\alpha+3)\cdots(\alpha+2n-1)}{(2n)!} a_0.$$

Procediendo de manera análoga obtendríamos para los coeficientes con índice impar

$$a_{2n+1} = (-1)^n \frac{(\alpha-1)(\alpha-3)\cdots(\alpha-2n+1)(\alpha+2)(\alpha+4)\cdots(\alpha+2n)}{(2n)!} a_1.$$

6) Consideremos las funciones $y_1, y_2 : (-1,1) \to \mathbb{R}$ definidas por:

$$y_1(x) = \sum_{n \geq 0} a_{2n} x^{2n} =$$

$$1 + \sum_{n \geq 1} (-1)^n \frac{\alpha(\alpha-2)\cdots(\alpha-2n+2)(\alpha+1)(\alpha+3)\cdots(\alpha+2n-1)}{(2n)!} x^{2n}$$

$$y_2(x) = \sum_{n \geq 0} a_{2n+1} x^{2n+1} =$$

$$x + \sum_{n \geq 1} (-1)^n \frac{(\alpha-1)(\alpha-3)\cdots(\alpha-2n+1)(\alpha+2)(\alpha+4)\cdots(\alpha+2n)}{(2n)!} x^{2n+1}$$

funciones que están bien definidas pues las series que las determinan son convergentes en $(-1,1)$ (criterio del cociente). Las funciones y_1 e y_2 son soluciones de la ecuación de Lagrange pues los coeficientes de cada una de las series satisfacen las relaciones $(*)$. Las funciones y_1, y_2 son linealmente independientes. Efectivamente, tenemos

$$y_1(x) = 1 + a_2 x^2 + a_4 x^4 + \ldots, \quad y_2(x) = x + a_3 x^3 + a_5 x^5 + \ldots$$

con lo cual $y_1(0) = 1$, $y_1'(0) = 0$, $y_2(0) = 0$, $y_2'(0) = 1$. Si $\lambda_1 y_1(x) + \lambda_2 y_2(x) = 0$ entonces $\lambda_1 y_1'(x) + \lambda_2 y_2'(x) = 0$ y sustituyendo $x = 0$ en las dos igualdades anteriores, obtenemos $\lambda_1 = \lambda_2 = 0$. La solución general de la ecuación de Legendre es por tanto:

$$y(x) = a_0 y_1(x) + a_1 y_2(x), \quad a_0, a_1 \in \mathbb{R}.$$

Nota. Obsérvese que por la forma de los coeficientes de las funciones $y_1(x)$ e $y_2(x)$, si $\alpha = 2k$ con $k \geq 0$ entero entonces $y_1(x)$ es un polinomio de grado $2k$ que sólo contiene potencias pares de x. Si $\alpha = 2k+1$ con $k \geq 0$ entero

entonces $y_2(x)$ es un polinomio de grado $2k+1$ que sólo contiene potencias impares de x. □

179. Iteración de punto fijo

Sea una función $g : D \subset \mathbb{R} \to \mathbb{R}$. Se dice que $p \in D$ es *punto fijo* de g si se verifica $g(p) = p$.
1) Sea una función $f : D \subset \mathbb{R} \to \mathbb{R}$ y $p \in D$. Demostrar que

$$p \text{ es cero o raíz de } f \Leftrightarrow p \text{ es punto fijo de } g(x) = x - f(x).$$

2) Sea $g \in C[a,b]$ tal que $g(x) \in [a,b]$ para todo $x \in [a,b]$. Demostrar que
i) g tiene un punto fijo en $[a,b]$.
ii) Si además, g es derivable en (a,b) y existe constante k con $0 < k < 1$ tal que $|g'(x)| \leq k$ para todo $x \in (a,b)$, el punto fijo de g es único.
3) Demostrar el *Teorema del punto fijo*:
Sea $g \in C[a,b]$ tal que $g(x) \in [a,b]$ para todo $x \in [a,b]$. Supongamos además además, g es derivable en (a,b) y que existe constante k con $0 < k < 1$ tal que $|g'(x)| \leq k$ para todo $x \in (a,b)$. Entonces, la sucesión

$$p_n = g\left(p_{n-1}\right), \quad n \geq 1$$

converge al único punto fijo p en $[a,b]$ (método de *iteración de punto fijo*).
4) Demostrar que en las hipótesis del teorema del punto fijo, se verifican para todo $n \geq 1$ las acotaciones de la sucesión de iteración de punto fijo:

$$(a) \quad |p_n - p| \leq k^n \cdot \text{máx}\{p_0 - a, b - p_0\}.$$

$$(b) \quad |p_n - p| \leq \frac{k^n}{1-k} |p_1 - p_0|.$$

5) *Aplicación.* Se considera la función $g : [-1,1] \to \mathbb{R}$ dada por $g(x) = (x^2 - 1)/3$.
a) Demostrar que g satisface las hipótesis del teorema del punto fijo.
b) Calcular el p_3 de la iteración de punto fijo con $p_0 = -1$.
c) Determinar a partir de qué n la iteración de punto fijo proporciona p con tres cifras decimales exactas.
d) Demostrar que la iteración de punto fijo proporciona en el caso presente una sucesión convergente a la única solución de la ecuación $x^2 - 3x - 1 = 0$ en $[-1,1]$. Dar una fórmula cerrada para esta solución.

SOLUCIÓN. 1) $\Rightarrow$) Si p es cero o raíz de f entonces $g(p) = p - f(p) = p - 0 = p$ es decir, p es punto fijo de g.
$\Leftarrow$) Si p es punto fijo de g entonces $f(p) = p - g(p) = p - p = 0$ es decir, p es raíz de f.
2) *i*) Si $g(a) = 0$ o $g(b) = 0$, un punto fijo es $p = a$ o $p = b$. En caso contrario se verifica $g(a) > a$ y $g(b) < b$. La función $h(x) = g(x) - x$ es continua en $[a,b]$ y verifica $h(a) > 0$ y $h(b) < 0$. Por el teorema de Bolzano, existe $p \in (a,b)$ tal que $0 = h(p) = g(p) - p$, con lo cual $g(p) = p$ y p es por tanto punto fijo de g.
ii) Supongamos que existieran dos puntos fijos p, q distintos con $p < q$.

Aplicando el teorema del valor medio de Lagrange a la función g en el intervalo $[p,q]$:

$$\exists \xi \in (p,q) : g'(\xi) = \frac{g(q)-g(p)}{q-p} \Rightarrow |q-p|$$

$$= |g(q)-g(p)| = \left|g'(\xi)\right| |q-p| \leq k\,|q-p| < |q-p|$$

lo cual es absurdo por tanto, el punto fijo es único.
3) Por el apartado anterior, existe un único punto fijo p. Como $g([a,b]) \subset [a,b]$, la sucesión p_n está bien definida. Dado que $|g'(x)| \leq k$ para todo $x \in (a,b)$ y por el teorema del valor medio de Lagrange,

$$|p_n - p| = |g(p_{n-1}) - g(p)| = \left|g'(\xi_n)\right| |p_{n-1} - p| \leq k\,|p_{n-1} - p|$$

en donde $\xi_n \in (a,b)$. Reiterando obtenemos

$$|p_n - p| \leq k\,|p_{n-1} - p| \leq k^2\,|p_{n-2} - p| \leq \ldots \leq k^n\,|p_0 - p|\,.$$

Al ser $0 < k < 1$ se verifica $\lim_{n\to+\infty} |p_n - p| \leq \lim_{n\to+\infty} k^n\,|p_0 - p| = 0$, y por tanto la sucesión p_n converge a p.
4) (a) En la demostración del teorema del punto fijo se probó que $|p_n - p| \leq k^n\,|p_0 - p|$, pero se verifica $|p_0 - p| \leq \max\{p_0 - a, b - p_0\}$.
(b) Tenemos las desigualdades

$$|p_{n+1} - p_n| = |g(p_n) - g(p_{n-1})| \leq k\,|p_n - p_{n-1}| \leq \ldots \leq k^n\,|p_1 - p_0|\,.$$

Entonces, para $m > n \geq 1$,

$$\begin{aligned} |p_m - p_n| &= |p_m - p_{m-1} + p_{m-1} - \cdots + p_{n+1} - p_n| \\ &\leq |p_m - p_{m-1}| + |p_{m-1} - p_{m-2}| + \cdots + |p_{n+1} - p_n| \\ &\leq k^{m-1}\,|p_1 - p_0| + k^{m-2}\,|p_1 - p_0| + \cdots + k^n\,|p_1 - p_0| \\ &= k^n(1 + k + k^2 + \cdots + k^{m-n-1})\,|p_1 - p_0|\,. \end{aligned}$$

Se verifica $\lim_{n\to+\infty} p_n = p$, por tanto

$$|p - p_n| = \lim_{m\to+\infty} |p_m - p_n| \leq k^n\,|p_1 - p_0| \sum_{j=0}^{m-n-1} k^j$$

$$\leq k^n\,|p_1 - p_0| \sum_{j=0}^{+\infty} k^j = \frac{k^n}{1-k}\,|p_1 - p_0|\,.$$

5) $a)$ La función g es polinómica y por tanto continua en $[-1,1]$. Es derivable en $(-1,1)$ con derivada $g'(x) = 2x/3$. El único punto crítico de g es $x = 0$. Tenemos $g(0) = -1/3$, $g(-1) = g(1) = 0$, por tanto el mínimo absoluto de g en $[-1,1]$ es $-1/3$ y el máximo absoluto 0. Esto demuestra que $g([-1,1]) \subset [-1,1]$. Además, se verifica

$$\left|g'(x)\right| = \left|\frac{2x}{3}\right| \leq \frac{2}{3} \text{ para todo } x \in (-1,1),$$

lo cual demuestra que se verifican las hipótesis del teorema del punto fijo.
b) Para $p_0 = -1$ tenemos

$$p_1 = g(p_0) = g(-1) = -\frac{1}{3},$$
$$p_2 = g(p_1) = g(-1/3) = \frac{1/9 - 1}{3} = -\frac{8}{27},$$
$$p_3 = g(p_2) = g(-8/27) = \frac{64/729 - 1}{3} = -\frac{665}{2187}.$$

c) Usando la acotación $|p_n - p| \leq k^n \cdot \text{máx}\{p_0 - a, b - p_0\}$, tenemos en nuestro caso $|p_n - p| \leq (2/3)^n \cdot \text{máx}\{0, 2\} = 2(2/3)^n$. Entonces,

$$|p_n - p| \leq 2\left(\frac{2}{3}\right)^n < 10^{-3} \Leftrightarrow \left(\frac{2}{3}\right)^n < \frac{10^{-3}}{2} \Leftrightarrow n \log_{10}\frac{2}{3} < -3 - \log_{10} 2$$
$$\underbrace{\Leftrightarrow}_{log_{10}(2/3)<0} \quad n > \frac{-3 - \log_{10} 2}{\log_{10}\frac{2}{3}} = 20{,}97\ldots,$$

con lo cual $n = 21$.
d) Sabemos que p es punto fijo de g si y sólo si p es raíz de $f(x) = x - g(x)$. En nuestro caso,

$$f(x) = 0 \Leftrightarrow x - g(x) = 0 \Leftrightarrow x - \frac{x^2 - 1}{3} = 0 \Leftrightarrow \frac{3x - x^2 + 1}{3} = 0,$$

lo cual equivale a $x^2 - 3x - 1 = 0$. Las soluciones de esta ecuación son $(3 \pm \sqrt{13})/2$ y sólo $(3 - \sqrt{13})/2 \in [-1, 1]$. Por tanto, el límite de la iteración de punto fijo es $p = (3 - \sqrt{13})/2$ □

180. Polinomios de Bernstein

El teorema de Weierstrass asegura que toda función continua $f : [a, b] \to \mathbb{R}$ puede ser aproximada uniformemente por polinomios. Construiremos de manera explícita una de tales sucesiones.

1) Sea $f : [a, b] \to \mathbb{R}$ una función continua. Se define el n-ésimo polinomio de *Bernstein* asociado a f como el polinomio:

$$B_n(f)(x) := \sum_{k=0}^{n} f\left(a + \frac{k(b-a)}{n}\right)\binom{n}{k}(x-a)^k(b-x)^{n-k}.$$

Determinar los polinomios de Bernstein asociados a las funciones $f_0(x) = 1$, $f_1(x) = x$ en el intervalo $[0, 1]$.
2) Ídem para la función $f_2(x) = x^2$ en el intervalo $[0, 1]$.
3) Demostrar que la sucesión de polinomios de Bernstein $B_n(f_i)(x)$ converge a f_i uniformemente en el intervalo $[0, 1]$ para cada $i = 0, 1, 2$.
4) Sea ahora $f : [0, 1] \to \mathbb{R}$ una función continua cualquiera. Demostrar que la sucesión de sus polinomios de Bernstein convergen uniformemente a f en $[0, 1]$.

5) Sea ahora $f : [a, b] \to \mathbb{R}$ una función continua cualquiera. Demostrar que la sucesión de sus polinomios de Bernstein convergen uniformemente a f en $[a, b]$.

SOLUCIÓN. 1) Para una función continua $f : [0, 1] \to \mathbb{R}$ los polinomios de Bernstein son

$$B_n(f)(x) = \sum_{k=0}^{n} f\left(\frac{k}{n}\right) \binom{n}{k} x^k (1-x)^{n-k}.$$

Tenemos para f_0 :

$$B_n(f_0)(x) = \sum_{k=0}^{n} 1 \cdot \binom{n}{k} x^k (1-x)^{n-k} = (x + (1-x))^n = 1.$$

Para f_1,

$$B_n(f_1)(x) = \sum_{k=1}^{n} \frac{k}{n} \binom{n}{k} x^k (1-x)^{n-k}.$$

Se verifican las implicaciones

$$\frac{k}{n}\binom{n}{k} = \frac{k}{n}\frac{n!}{k!(n-k)!} = \frac{(n-1)!}{(k-1)![(n-1)-(k-1)]!} = \binom{n-1}{k-1}$$

$$\Rightarrow B_n(f_1)(x) = x \sum_{k=1}^{n} \binom{n-1}{k-1} x^{k-1}(1-x)^{(n-1)-(k-1)}$$

$$= x \sum_{k=0}^{n-1} \binom{n-1}{k} x^k (1-x)^{(n-1)-k} = x(x + (1-x))^{n-1} = x.$$

Es decir, $B_n(f_0)(x) = 1$ y $B_n(f_1)(x) = x$.

2) Usando la relación $\frac{k}{n}\binom{n}{k} = \binom{n-1}{k-1}$ demostrada en el apartado anterior,

$$B_n(f_2)(x) = \sum_{k=0}^{n} \frac{k^2}{n^2} \binom{n}{k} x^k (1-x)^{n-k} = \frac{x}{n} \sum_{k=1}^{n} \frac{k^2}{n} \binom{n}{k} x^{k-1}(1-x)^{n-k}$$

$$= \frac{x}{n} \sum_{k=1}^{n} k \binom{n-1}{k-1} x^{k-1}(1-x)^{n-k} = \frac{x}{n} \sum_{k=0}^{n-1} (k+1) \binom{n-1}{k} x^k (1-x)^{n-1-k}$$

$$= \frac{n-1}{n} x \sum_{k=0}^{n-1} \frac{k+1}{n-1} \binom{n-1}{k} x^k (1-x)^{n-1-k}$$

$$= \frac{n-1}{n} x \sum_{k=0}^{n-1} \frac{k}{n-1} \binom{n-1}{k} x^k (1-x)^{n-1-k}$$

$$+ \frac{x}{n} \sum_{k=0}^{n-1} \binom{n-1}{k} x^k (1-x)^{n-1-k}$$

$$= \frac{n-1}{n} x \cdot x + \frac{x}{n}(x + (1-x))^{n-1} = \frac{n-1}{n} x^2 + \frac{1}{n} x.$$

3) Para $i = 0$ tenemos la sucesión constante $B_n(f_0)(x) = 1$ que de manera trivial converge uniformemente a $f_0(x) = 1$ en $[0, 1]$. Para $i = 1$, también $B_n(f_1)(x) = x$ es constante y converge trivialmente a $f_1(x) = x$ en $[0, 1]$. Para $i = 2$ tenemos $B_n(f_2)(x) = ((n-1)/n)x^2 + (1/n)x$ y $\lim_{n\to+\infty} B_n(f_2)(x) = x^2 = f_2(x)$ en $[0, 1]$. Veamos que la convergencia es uniforme.

$$|B_n(f_2)(x) - f_2(x)| = \left| \frac{n-1}{n} x^2 + \frac{1}{n} x - x^2 \right| = \left| \frac{-1}{n} x^2 + \frac{1}{n} x \right|$$

$$= \frac{1}{n} \left| -x^2 + x \right| \leq \frac{1}{n} \left(\left| -x^2 \right| + |x| \right) \leq \frac{1}{n} (1 + 1) = \frac{2}{n}.$$

Sea $\epsilon > 0$. Entonces $2/n < \epsilon$ equivale a $n > 2/\epsilon$. Si $n_0 = \lfloor 2/\epsilon \rfloor + 1$ se verifica $|B_n(f_2)(x) - f_2(x)| < \epsilon$ si $n \geq n_0$ y para todo $x \in [0, 1]$. La convergencia es por tanto uniforme.

4) Tenemos que demostrar que para todo $\epsilon > 0$ existe un número natural n_0 tal que si $n \geq n_0$, entonces $|f(x) - B_n(f)(x)| < \epsilon$ para todo $x \in [0, 1]$. Llamemos $p_k(x) = \binom{n}{k} x^k (1-x)^{n-k}$, entonces podemos escribir $B_n(f)(x) = \sum_{k=0}^{n} f(k/n) p_k(x)$ y dado que

$$\sum_{k=0}^{n} p_k(x) = \sum_{k=0}^{n} \binom{n}{k} x^k (1-x)^{n-k} = (x + (1-x))^n = 1,$$

bastará demostrar que para todo $\epsilon > 0$ existe un número natural n_0 tal que si $n \geq n_0$,

$$\left| \sum_{k=0}^{n} \left(f(x) - f\left(k/n\right) \right) p_k(x) \right| < \epsilon \quad \forall x \in [0, 1].$$

Al ser f continua en el cerrado $[0, 1]$, por el teorema de Heine f es uniformemente continua en $[0, 1]$, es decir, dado $\epsilon > 0$ existe $\delta > 0$ tal que $|f(x) - f(y)| < \epsilon/3$ si $|x - y| < \delta$. Para $x \in [0, 1]$ y n natural definimos los conjuntos

$$A_1 = \{k : 0 \leq k \leq n \text{ y } |x - k/n| \leq \delta\},$$
$$A_2 = \{k : 0 \leq k \leq n \text{ y } |x - k/n| > \delta\}.$$

Usando que $0 \leq p_k(x) \leq 1$ para todo $x \in [0, 1]$,

$$\left| \sum_{k=0}^{n} \left(f(x) - f\left(k/n\right) \right) p_k(x) \right|$$

$$\leq \sum_{k \in A_1} \left| f(x) - f\left(k/n\right) \right| p_k(x) + \sum_{k \in A_2} \left| f(x) - f\left(k/n\right) \right| p_k(x)$$

$$\leq \frac{\epsilon}{3} + \sum_{k \in A_2} \left| f(x) - f\left(k/n\right) \right| p_k(x).$$

Si $k \in A_2$ se verifica $(x-k/n)^2 > \delta^2$, luego $1 < (x-k/n)^2/\delta^2$. Al ser f continua en un intervalo cerrado, está acotada. Sea K una cota superior de f. Entonces,

$$\sum_{k\in A_2} |f(x) - f\left(k/n\right)| p_k(x) \leq \sum_{k\in A_2} \left(|f(x)| + |f\left(k/n\right)|\right) p_k(x)$$

$$\leq 2K \sum_{k\in A_2} p_k(x) \leq 2K \sum_{k\in A_2} \frac{(x-k/n)^2}{\delta^2} p_k(x) = \frac{2K}{\delta^2} \sum_{k\in A_2} (x-k/n)^2 p_k(x)$$

$$\leq \frac{2K}{\delta^2} \sum_{k=0}^{n} (x-k/n)^2 p_k(x)$$

$$= \frac{2K}{\delta^2} \left(x^2 \sum_{k=0}^{n} p_k(x) - 2x \sum_{k=0}^{n} (k/n) p_k(x) + \sum_{k=0}^{n} (k/n)^2 p_k(x) \right)$$

$$\underbrace{=}_{\text{Por los apartados 1 y 2}} \frac{2K}{\delta^2} \left(x^2 - 2x^2 + \frac{n-1}{n} x^2 + \frac{1}{n} x \right)$$

$$= \frac{2K}{\delta^2 n} x(1-x) \leq \frac{2K}{\delta^2 n}.$$

Como $\lim_{n\to+\infty} 2K/(\delta^2 n) = 0$, dado $\epsilon > 0$ existe n_0 natural tal que $2K/\delta^2 n < \epsilon/3$ si $n \geq n_0$ con lo cual,

$$\left| \sum_{k=0}^{n} \left(f(x) - f\left(k/n\right)\right) p_k(x) \right| \leq \frac{\epsilon}{3} + \frac{\epsilon}{3} = \frac{2\epsilon}{3} < \epsilon \text{ si } n \geq n_0$$

y por tanto, $B_n(f)(x) \to f(x)$ uniformemente en $[0,1]$.

5) Consideremos la función continua y biyectiva $\phi : [0,1] \to [a,b]$, $\phi(x) = (b-a)x + a$. Su inversa $\phi^{-1}(x) = (x-a)/(b-a)$ es continua. La función $g := f \circ \phi : [0,1] \to \mathbb{R}$ es continua, y por el apartado anterior $B_n(g) \to g$ uniformemente en $[0,1]$. Pero $f = g \circ \phi^{-1}$ con lo cual $B_n(g) \circ \varphi^{-1} \to f$ en $[a,b]$ uniformemente. Ahora bien,

$$B_n(g)[\varphi^{-1}(x)] = B_n(g)\left(\frac{x-a}{b-a}\right)$$

$$= \sum_{k=0}^{n} g\left(\frac{k}{n}\right) \binom{n}{k} \left(\frac{x-a}{b-a}\right)^k \left(1 - \frac{x-a}{b-a}\right)^{n-k}$$

$$= \frac{1}{(b-a)^n} \sum_{k=0}^{n} f\left(\varphi\left(\frac{k}{n}\right)\right) (x-a)^n (b-x)^n$$

$$= \frac{1}{(b-a)^n} \sum_{k=0}^{n} f\left(a + \frac{k(b-a)}{n}\right) \binom{n}{k} (x-a)^k (b-x)^{n-k}$$

que son los polinomios de Bernstein $B_n(f)$ en $[a,b]$. □

181. Espacios l_p

Designamos por $\mathbb{K}$ al cuerpo de los números reales o complejos indistintamente. Sabemos que en el espacio vectorial $\mathbb{K}^n$ y para todo $p \in [1, +\infty)$ se definen la normas

$$\|x\|_p = \left(\sum_{k=1}^{n} |x_k|^p \right)^{1/p}, \forall x = (x_1, \ldots, x_n) \in \mathbb{K}^n,$$

y también la norma $\|x\|_\infty = \max \{|x_1|, \ldots, |x_n|\}$. Generalizaremos estos conceptos a $\mathbb{K}^{\mathbb{N}}$

1) Sea $\mathbb{K}^{\mathbb{N}}$ el espacio vectorial de las sucesiones en $\mathbb{K}$ con las operaciones habituales. Para cada $p \in [1, +\infty)$ se define el subconjunto de $\mathbb{K}^{\mathbb{N}}$:

$$l_p := \{x = (x_k) \in \mathbb{K}^{\mathbb{N}} : \sum_{k=1}^{+\infty} |x_k|^p \ < +\infty\}.$$

Demostrar que l_p es subespacio vectorial de $\mathbb{K}^{\mathbb{N}}$ y que $\|x\|_p = \left(\sum_{k=1}^{+\infty} |x_k|^p\right)^{1/p}$ es una norma en l_p.
2) Demostrar que l_p es espacio de Banach para todo $p \in [1, +\infty)$.
3) Demostrar que para todo $p \in [1, +\infty)$ la dimensión de l_p es infinita.
4) Demostrar que para $1 \leq p < q < +\infty$ se verifica $l_p \subset l_q$ con $l_p \neq l_q$. Es decir l_p se agranda de manera estricta al aumentar p.
5) Se define el subconjunto de $\mathbb{K}^{\mathbb{N}}$:

$$l_\infty := \left\{ x = (x_k) \in \mathbb{K}^{\mathbb{N}} : \sup\{|x_k| : k \in \mathbb{N}\} < +\infty \right\}$$

es decir, l_∞ está formado por las sucesiones en $\mathbb{K}$ acotadas. Demostrar que l_∞ es subespacio vectorial de $\mathbb{K}^{\mathbb{N}}$ de dimensión infinita y que $\|x\|_\infty = \sup\{|x_k| : k \in \mathbb{N}\}$ es una norma en l_∞.
6) Demostrar que $l_p \subset l_\infty$ con $l_p \neq l_\infty$ para todo $p \in [1, +\infty)$.
7) Demostrar que l_∞ es espacio de Banach.

solución. 1) La sucesión nula $0 = (0)$ claramente pertenece a l_p. Si $x = (x_k)$ e $y = (y_k)$ pertenecen a l_p entonces $\sum_{k=1}^{+\infty} |x_k|^p \ < +\infty$ y $\sum_{k=1}^{+\infty} |y_k|^p \ < +\infty$. Usando la desigualdad de Minkowski,

$$\left(\sum_{k=1}^{n} |x_k + y_k|^p \right)^{1/p} \leq \left(\sum_{k=1}^{n} (|x_k| + |y_k|)^p \right)^{1/p}$$
$$\leq \left(\sum_{k=1}^{n} |x_k|^p \right)^{1/p} + \left(\sum_{k=1}^{n} |y_k|^p \right)^{1/p}.$$

Tomando límites cuando $n \to +\infty$,

$$\left(\sum_{k=1}^{+\infty} |x_k + y_k|^p \right)^{1/p} \leq \left(\sum_{k=1}^{+\infty} |x_k|^p \right)^{1/p} + \left(\sum_{k=1}^{+\infty} |y_k|^p \right)^{1/p} < +\infty, \qquad (1)$$

con lo cual $x+y \in l_p$. Si $\lambda \in \mathbb{K}$ y $x \in l_p$ entonces,

$$\sum_{k=1}^{+\infty} |\lambda x_k|^p = |\lambda|^p \sum_{k=1}^{+\infty} |x_k|^p < +\infty, \qquad (2)$$

con lo cual $\lambda x \in l_p$ y l_p es subespacio vectorial de $\mathbb{K}^{\mathbb{N}}$. Es claro que $\|x\|_p = 0$ si y sólo si $x = 0$ y las relaciones $\|\lambda x\|_p = |\lambda| \, \|x\|_p$ y $\|x+y\|_p \leq \|x\|_p + \|y\|_p$ se deducen inmediatamente de las relaciones (2) y (1) respectivamente. Por tanto, $\| \ \|_p$ es norma en l_p.

2) Sea $X_n = (x_{nk})$ una sucesión de Cauchy de elementos de l_p. Para todo par de números naturales m, n se verifica $|x_{nk} - x_{mk}| = (|x_{nk} - x_{mk}|^p)^{1/p} \leq \|X_n - X_m\|_p$. Como X_n es sucesión de Cauchy, también lo es x_{nk} para todo k y al ser $\mathbb{K}$ completo, podemos definir $x_k := \lim_{n\to+\infty} x_{nk}$. Veamos que la sucesión $X = (x_k)$ pertenece a l_p y que $X_n \to X$ con lo cual estará demostrado que l_p es completo. Al ser X_n de Cauchy en l_p, para todo $\epsilon > 0$ existe n_0 natural tal que para $m, n \geq n_0$ se verifica $\|X_n - X_m\|_p < \epsilon$. Para todo N natural tenemos

$$\sum_{k=1}^{N} |x_{nk} - x_{mk}|^p \leq \left(\|X_n - X_m\|_p \right)^p \leq \epsilon^p.$$

Tomando límites cuando $m \to +\infty$

$$\sum_{k=1}^{N} |x_{nk} - x_k|^p = \lim_{m\to+\infty} \sum_{k=1}^{N} |x_{nk} - x_{mk}|^p \leq \epsilon^p,$$

y al ser N cualquiera, $\sum_{k=1}^{+\infty} |x_{nk} - x_k|^p \leq \epsilon^p$ y por tanto $X_n - X \in l_p$. Ahora bien $X = X_n - (X_n - X)$ con lo cual $X \in l_p$. Por la última desigualdad $\|X_n - X\|_p < \epsilon$ para $n \geq n_0$ es decir, X_n converge a X.

3) Consideremos para cada n natural los elementos de $\mathbb{K}^{\mathbb{N}}$ dados por $e_n = (x_k)$ con $x_k = 1$ si $k = n$ y $x_k = 0$ si $k \neq n$. Es claro que el sistema $\{e_n : n \in \mathbb{N}\}$ es libre, tiene infinitos elementos y está contenido en l_p para todo $p \in [1, +\infty)$, luego la dimensión de l_p es infinita.

4) Si $x = (x_k) \in l_p$ entonces $\sum_{k=1}^{+\infty} |x_k|^p$ es convergente luego $\lim_{k\to+\infty} x_k = 0$ con lo cual $|x_k|^q \leq |x_k|^p$ para k suficientemente grande. Por el teorema de comparación para series de términos positivos, la serie $\sum_{k=1}^{+\infty} |x_k|^q$ converge, por tanto $x \in l_q$.
El contenido $l_p \subset l_q$ es estricto. En efecto, consideremos la sucesión $y = (k^{-1/p})$. Entonces,

$$\sum_{k=1}^{+\infty} |y_k|^p = \sum_{k=1}^{+\infty} \frac{1}{k} \text{ (divergente)}, \quad \sum_{k=1}^{+\infty} |y_k|^q = \sum_{k=1}^{+\infty} \frac{1}{k^{q/p}} \text{ (convergente)},$$

es decir $y \notin l_p$ e $y \in l_q$.

5) Es claro que la sucesión nula está acotada, que la suma de dos acotadas está acotada y que el producto de un escalar por una acotada está acotada, por tanto l_∞ es subespacio vectorial de $\mathbb{K}^{\mathbb{N}}$. La familia $\{e_n = (x_k) : n \in \mathbb{N}\}$ con $x_k = 1$ si $k = n$ y $x_k = 0$ si $k \neq n$ es libre y está contenida en l_∞, por tanto l_∞ tiene dimensión infinita. Veamos que $\| \ \|_\infty$ es norma en l_∞.

$$\|x\|_\infty = 0 \Leftrightarrow \sup\{|x_k| : k \in \mathbb{N}\} = 0 \Leftrightarrow |x_k| = 0 \ \forall k \in \mathbb{N}$$

$$\Leftrightarrow x_k = 0 \ \forall k \in \mathbb{N} \Leftrightarrow x = (0).$$

Para $\lambda \in \mathbb{K}$ y $x = (x_k) \in l_\infty$,

$$\|\lambda x\|_\infty = \sup\{|\lambda x_k| : k \in \mathbb{N}\} = \sup\{|\lambda||x_k| : k \in \mathbb{N}\}$$

$$= |\lambda| \sup\{|x_k| : k \in \mathbb{N}\} = |\lambda| \, \|x\|_\infty .$$

Por último, para $x = (x_k)$ e $y = (y_k)$ elementos de l_∞,

$$\|x + y\|_\infty = \sup\{|x_k + y_k| : k \in \mathbb{N}\} \leq \sup\{|x_k| + |y_k| : k \in \mathbb{N}\}$$

$$\leq \sup\{|x_k| : k \in \mathbb{N}\} + \sup\{|y_k| : k \in \mathbb{N}\} = \|x\|_\infty + \|y\|_\infty .$$

6) Si $x = (x_k) \in l_p$ entonces, $\sum_{k=1}^{+\infty} |x_k|^p$ es convergente y por tanto $x_k \to 0$ lo cual implica que $x = (x_k)$ está acotada. Por otra parte, la sucesión constante $x = (1)$ pertenece a l_∞ pero no a l_p.

7) Sea $X_n = (x_{nk})$ una sucesión de Cauchy de elementos de l_∞. Para todo par de números naturales m, n se verifica $|x_{nk} - x_{mk}| \leq \sup\{|x_{nk} - x_{mk}| : k \in \mathbb{N}\} \leq \|X_n - X_m\|_\infty$. Como X_n es sucesión de Cauchy, también lo es x_{nk} para todo k y al ser $\mathbb{K}$ completo, podemos definir $x_k := \lim_{n\to+\infty} x_{nk}$. Veamos que la sucesión $X = (x_k)$ pertenece a l_∞ y que $X_n \to X$ con lo cual estará demostrado que l_∞ es completo.
Si $\epsilon > 0$ existe n_0 natural tal que $|x_{nk} - x_{mk}| < \epsilon/2$ para todo k y para todo $m, n \geq n_0$. Haciendo $m \to +\infty$ obtenemos $|x_{nk} - x_k| \leq \epsilon/2$ y tomando supremos sobre k,

$$\sup\{|x_{nk} - x_k| : k \in \mathbb{N}\} \leq \epsilon/2$$

para todo $n \geq n_0$, es decir $\|X_n - X\|_\infty < \epsilon$ si $n \geq n_0$ lo cual prueba que $X_n \to X$. Por otra parte, es claro que X está acotada, luego $X \in l_\infty$. □

182. Concepto de aplicación multilineal

Sean $V_1, \ldots, V_n, V$ espacios vectoriales sobre el cuerpo K y sea

$$\phi : V_1 \times \ldots \times V_n \to V$$

una aplicación. Se dice que ϕ es *multilineal* si $\forall i = 1, \ldots, n$ se verifica

(a) $\phi(v_1, \ldots, v_i + v_i', \ldots, v_n) = \phi(v_1, \ldots, v_i, \ldots, v_n) + \phi(v_1, \ldots, v_i', \ldots, v_n)$,

(b) $\phi(v_1, \ldots, \alpha v_i, \ldots, v_n) = \alpha\phi(v_1, \ldots, v_i, \ldots, v_n)$,

en donde $v_i, v_i' \in V_i$, $v_j \in V_j$ si $j \neq i$ y $\alpha \in K$.

Nótese que el que ϕ es multilineal equivale a decir que la aplicación de V_i en V dada por $\phi(v_1, \ldots, v_{i-1}, \bullet, v_{i+1}, \ldots, v_n)$ es lineal $\forall i = 1, \ldots, n$. Si $n = 2$, decimos que ϕ es una aplicación *bilineal*. Si $V = K$ decimos que ϕ es *forma* multilineal.

1) Si $n = 1$, demostrar que $\phi : V_1 \to V$ es multilineal si y sólo si es lineal.
2) Demostrar que la aplicación $\phi : V \times V^* \to K$ dada por $\phi(x, T) = T(x)$ es forma bilineal.
3) Sea $\phi : (K^n)^n = K^n \times \ldots K^n \to K$ dada por $\phi(v_1, \ldots, v_n) = \det A$ siendo $A = [v_1 \ldots v_n]$ matriz con columnas $v_1 \ldots v_n$. Demostrar que ϕ es multilineal.
4) Sea A un álgebra sobre K. Definimos

$$\phi : A^n \to A, \quad \phi(v_1, v_2, \ldots, v_n) = v_1 v_2 \cdots v_n.$$

Demostrar que ϕ es multilineal.
Nota. Como casos particulares tenemos las álgebras: $K^{n\times n}$ (matrices cuadradas), $K[x]$ (polinomios), $C^k(I)$, $k = 0, 1, 2, \ldots, \infty$ (funciones reales de clase k en un intervalo cerrado $I = [a, b]$).
5) Sea $\phi : V_1 \times \ldots \times V_n \to V$ multilineal y $T : V \to W$ lineal. Demostrar que $T \circ \phi$ es multilineal.
6) Demostrar que $\phi : (C^\infty(I))^n \to C^\infty(I)$ dada por $\phi(f_1, \ldots, f_n) = (f_1 \cdot \ldots \cdot f_n)'$ es una aplicación multilineal.
7) Si $C[a, b]$ es el álgebra de las funciones reales continuas en el intervalo $[a, b]$, demostrar que la aplicación $\phi : (C[a, b])^n \to C[a, b]$ dada por

$$\phi(f_1, \ldots, f_n) = \int_a^b f_1 \cdot \ldots \cdot f_n$$

es multilineal.

SOLUCIÓN. 1) Es consecuencia inmediata de la definición de aplicación multilineal.
2) En efecto,

$$\phi(x + y, T) = T(x + y) = T(x) + T(y) = \phi(x, T) + \phi(y, T),$$
$$\phi(\alpha x, T) = T(\alpha x) = \alpha T(x) = \alpha\phi(x, T).$$

Por otra parte,

$$\phi(x, T + S) = (T + S)(x) = T(x) + S(x) = \phi(x, T) + \phi(x, S),$$
$$\phi(x, \alpha T) = (\alpha T)(x) = \alpha T(x) = \alpha\phi(x, T).$$

3) Usando conocidas propiedades de los determinantes,

$$\begin{aligned}\phi(v_1, \ldots, v_i + v_i', \ldots, v_n) &= \det[v_1 \ldots v_i + v_i' \ldots v_n] \\ &= \det[v_1 \ldots v_i \ldots v_n] + \det[v_1 \ldots v_i' \ldots v_n] \\ &= \phi(v_1, \ldots, v_i, \ldots, v_n) + \phi(v_1, \ldots, v_i', \ldots, v_n).\end{aligned}$$

Por otra parte,

$$\phi(v_1, \ldots, \alpha v_i, \ldots, v_n) = \det[v_1 \ldots \alpha v_i \ldots v_n]$$

$$= \alpha \det[v_1 \dots v_i \dots v_n] = \alpha\phi(v_1, \dots, v_i, \dots, v_n).$$

4) Usando las conocidas propiedades de un álgebra,

$$\begin{aligned}\phi(v_1, \dots, v_i + v_i', \dots, v_n) &= v_1 \cdots (v_i + v_i') \cdots v_n \\ &= v_1 \cdots v_i \cdots v_n + v_1 \cdots v_i' \cdots v_n \\ &= \phi(v_1, \dots, v_i, \dots, v_n) + \phi(v_1, \dots, v_i', \dots, v_n).\end{aligned}$$

$$\begin{aligned}\phi(v_1, \dots, \alpha v_i, \dots, v_n) &= v_1 \cdots (\alpha v_i) \cdots v_n \\ &= \alpha(v_1 \cdots v_i \cdots v_n) = \alpha\phi(v_1, \dots, v_i, \dots, v_n).\end{aligned}$$

5) Tenemos $T \circ \phi : V_1 \times \dots \times V_n \to W$. Entonces,

$$\begin{aligned}(T \circ \phi)(v_1, \dots, v_i + v_i', \dots, v_n) &= T\left[\phi(v_1, \dots, v_i + v_i', \dots, v_n)\right] \\ &= T\left[\phi(v_1, \dots, v_i, \dots, v_n) + \phi(v_1, \dots, v_i', \dots, v_n)\right] \\ &= T\left[\phi(v_1, \dots, v_i, \dots, v_n)\right] + T\left[\phi(v_1, \dots, v_i', \dots, v_n)\right] \\ &= (T \circ \phi)(v_1, \dots, v_i, \dots, v_n) + (T \circ \phi)(v_1, \dots, v_i', \dots, v_n).\end{aligned}$$

$$\begin{aligned}(T \circ \phi)(v_1, \dots, \alpha v_i, \dots, v_n) &= T\left[\phi(v_1, \dots, \alpha v_i, \dots, v_n)\right] \\ &= T\left[\alpha\phi(v_1, \dots, v_i, \dots, v_n)\right] = \alpha T\left[\phi(v_1, \dots, v_i, \dots, v_n)\right] \\ &= \alpha(T \circ \phi)(v_1, \dots, v_i, \dots, v_n).\end{aligned}$$

6) Claramente, el operador derivación $D : C^\infty(I) \to C^\infty(I)$ es lineal, y la aplicación $\phi_1 : (C^\infty(I))^n \to C^\infty(I)$ dada por $\phi_1(f_1, \dots, f_n) = f_1 \cdot \dots \cdot f_n$ es multilineal según el apartado 4. Pero $\phi = D \circ \phi_1$ que según el apartado 5 es multilineal.

7) Claramente, el operador integración $\mathrm{Int} : C[a,b] \to C[a,b]$ es lineal, y la aplicación $\phi_1 : (C[a,b])^n \to C[a,b]$ dada por $\phi_1(f_1, \dots, f_n) = f_1 \cdot \dots \cdot f_n$ es multilineal según el apartado 4. Pero $\phi = \mathrm{Int} \circ \phi_1$ que según el apartado 5 es multilineal. □

183. Espacio vectorial de las aplicaciones multilineales

Recordamos que si $X \neq \emptyset$ es un conjunto, V un espacio vectorial sobre el cuerpo K y V^X, el conjunto de las aplicaciones de X en V entonces, V^X es espacio vectorial sobre K con las operaciones habituales $(f+g)(x) = f(x) + g(x)$ (suma) y $(\alpha f)(x) = \alpha f(x)$ (producto por un escalar). Para $V_1, \dots, V_n, V$ espacios vectoriales sobre el cuerpo K denotamos por $\mathrm{Mul}_K(V_1 \times \dots \times V_n, V)$ al conjunto de todas las aplicaciones multilineales de $V_1 \times \dots \times V_n$ en V. Si E y F son dos espacios vectoriales sobre el cuerpo K, se designa por $\mathrm{Lin}_K(E,F)$ al espacio vectorial de las aplicaciones lineales $f : E \to F$.

1) Demostrar que $\mathrm{Mul}_K(V_1 \times \dots \times V_n, V)$ es subespacio vectorial de $V^{V_1 \times \dots \times V_n}$.

2) Demostrar que si $n \geq 2$ se verifica

$$\mathrm{Mul}_K(V_1 \times \dots \times V_n, V) \cap \mathrm{Lin}_K(V_1 \times \dots \times V_n, V) = \{0\}.$$

SOLUCIÓN. 1) La aplicación nula es claramente multilineal. Si $\lambda, \mu \in K$ y $\phi, \varphi \in \mathrm{Mul}_K(V_1 \times \ldots \times V_n, V)$, entonces,

$$(\lambda\phi + \mu\varphi)(v_1, \ldots, v_i + v_i', \ldots, v_n) = (\lambda\phi)(v_1, \ldots, v_i + v_i', \ldots, v_n)$$

$$+(\mu\varphi)(v_1, \ldots, v_i + v_i', \ldots, v_n) = \lambda\phi(v_1, \ldots, v_i + v_i', \ldots, v_n)$$

$$+\mu\varphi(v_1, \ldots, v_i + v_i', \ldots, v_n) = \lambda[\phi(v_1, \ldots, v_i, \ldots, v_n) + \phi(v_1, \ldots, v_i', \ldots, v_n)]$$

$$+\mu[\varphi(v_1, \ldots, v_i, \ldots, v_n) + \varphi(v_1, \ldots, v_i', \ldots, v_n)]$$

$$= [\lambda\phi(v_1, \ldots, v_i, \ldots, v_n) + \mu\varphi(v_1, \ldots, v_i, \ldots, v_n)]$$

$$+ \left[\lambda\phi(v_1, \ldots, v_i', \ldots, v_n) + \mu\varphi(v_1, \ldots, v_i', \ldots, v_n)\right]$$

$$(\lambda\phi)(v_1, \ldots, v_i, \ldots, v_n) + (\mu\varphi)(v_1, \ldots, v_i, \ldots, v_n)$$

$$+(\lambda\phi)(v_1, \ldots, v_i', \ldots, v_n) + (\mu\varphi)(v_1, \ldots, v_i', \ldots, v_n)$$

$$= (\lambda\phi + \mu\varphi)(v_1, \ldots, v_i, \ldots, v_n) + (\lambda\phi + \mu\varphi)(v_1, \ldots, v_i', \ldots, v_n),$$

y se satisface la primera condición de aplicación multilineal. Ahora, y para todo $\alpha \in K$,

$$(\lambda\phi + \mu\varphi)(v_1, \ldots, \alpha v_i, \ldots, v_n) = (\lambda\phi)(v_1, \ldots, \alpha v_i, \ldots, v_n)$$

$$+(\mu\varphi)(v_1, \ldots, \alpha v_i, \ldots, v_n) = \lambda\phi(v_1, \ldots, \alpha v_i, \ldots, v_n)$$

$$+\mu\varphi(v_1, \ldots, \alpha v_i, \ldots, v_n) = \alpha\lambda\phi(v_1, \ldots, v_i, \ldots, v_n) + \alpha\mu\varphi(v_1, \ldots, v_i, \ldots, v_n)$$

$$= \alpha[\lambda\phi(v_1, \ldots, v_i, \ldots, v_n) + \mu\varphi(v_1, \ldots, v_i, \ldots, v_n)]$$

$$= \alpha[(\lambda\phi)(v_1, \ldots, v_i, \ldots, v_n) + (\mu\varphi)(v_1, \ldots, v_i, \ldots, v_n)]$$

$$= \alpha(\lambda\phi + \mu\varphi)(v_1, \ldots, v_i, \ldots, v_n).$$

La aplicación $\lambda\phi + \mu\varphi$ es por tanto multilineal. Concluimos que $\mathrm{Mul}_K(V_1 \times \ldots \times V_n, V)$ es subespacio vectorial de $V^{V_1 \times \ldots \times V_n}$. 2) Fijemos $i \in \{1, 2, \ldots, n\}$ y sea $\phi : V_1 \times \ldots \times V_n \to V$ multilineal y lineal. Por ser multilineal se verifica

$$\phi(v_1, \ldots, v_i + v_i, \ldots, v_n) = \phi(v_1, \ldots, v_i, \ldots, v_n) + \phi(v_1, \ldots, v_i, \ldots, v_n).$$

Por ser lineal. se verifica

$$\phi(v_1, \ldots, v_i + v_i, \ldots, v_n) = \phi(v_1, \ldots, v_i, \ldots, v_n) + \phi(0, \ldots, v_i, \ldots, 0).$$

De las dos relaciones anteriores, $\phi(v_1, \ldots, , v_n) = \phi(0, \ldots, v_i, \ldots, 0)$. De nuevo, por ser ϕ lineal,

$$\phi(v_1, \ldots, v_n) = \phi\left(\sum_{i=1}^{n}(0, \ldots, v_i, \ldots, 0))\right) = \sum_{i=1}^{n}\phi(0, \ldots, v_i, \ldots, 0)$$

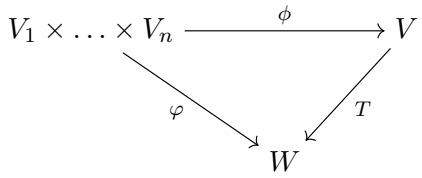
Restando a la última igualdad la $\phi(v_1, \ldots, , v_n) = \phi(0, \ldots, v_i, \ldots, 0)$, obtenemos $\phi(v_1, \ldots, v_{i-1}, 0, v_{i+1}, \ldots, v_n) = 0$. Ahora para $n \geq 2$, al ser v_i arbitrario también lo es el subindice i por tanto para todo $(v_1, \ldots, v_n) \in V_1 \times \ldots \times V_n$ tenemos $\phi(v_1, \ldots, v_n) = \phi(0, v_2, \ldots, v_n) + \phi(v_1, 0, \ldots, 0) = 0 + 0 = 0$. $\square$

184. Problema de la aplicación universal

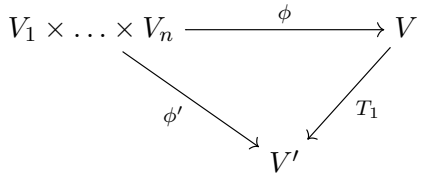
Vimos que una manera de construir aplicaciones multilineales sobre $V_1 \times \ldots \times V_n$ es elegir una aplicación multilineal fija de $V_1 \times \ldots \times V_n$ sobre V y luego componerla con varias aplicaciones lineales de V en otro espacio vectorial. Se plantea la siguiente pregunta: ¿podemos con una adecuada elección de V construir todas las aplicaciones multilineales sobre $V_1 \times \ldots \times V_n$ de esta manera?
La respuesta a esta pregunta es afirmativa, y nos llevará a construir el producto tensorial de los espacios $V_1, \ldots, V_n$. De forma más precisa, planteamos el siguiente problema, llamado *problema de la aplicación universal para aplicaciones multilineales.*

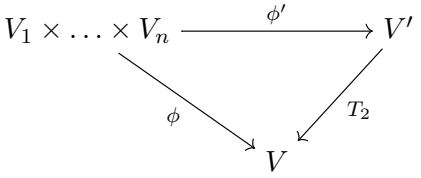
Problema. Sean $V_1, \ldots, V_n$ espacios vectoriales sobre K, ¿existe un espacio vectorial V sobre K y una aplicación multilineal $\phi : V_1 \times \ldots \times V_n \to V$ tal que para cada aplicación multilineal $\varphi : V_1 \times \ldots \times V_n \to W$ existe una única $T \in \mathrm{Lin}_K(V, W)$ tal que $\varphi = T \circ \phi$?

En términos de diagrama conmutativo: ¿podemos construir una aplicación multilineal $\phi : V_1 \times \ldots \times V_n \to V$ con la propiedad de que para toda $\varphi : V_1 \times \ldots \times V_n \to W$ multilineal existe una única $T \in \mathrm{Lin}_K(V, W)$ tal que el siguiente diagrama es conmutativo?



Nótese que cualquier solución al problema planteado consiste en un par (V, ϕ) con $\phi : V_1 \times \ldots \times V_n \to V$ multilineal. Antes de construir una solución al problema, demostremos que la solución es esencialmente única salvo isomorfismos.
Sean (V, ϕ) y (V', ϕ') dos soluciones al problema de la aplicación universal. Demostrar que existen dos isomorfismos $T_1 \in \mathrm{Lin}_K(V, V')$ y $T_2 \in \mathrm{Lin}_K(V', V)$ tales que
(*a*) $T_1 \circ T_2 = I_V,\ T_2 \circ T_1 = I_{V'}$.
(*b*) Los siguientes diagramas son conmutativos

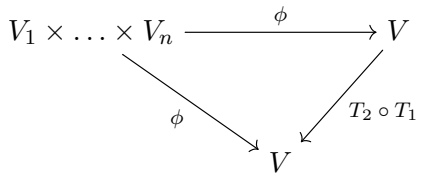




SOLUCIÓN. Como (V, ϕ) es solución al problema de la aplicación universal, existe un único $T_1 \in \mathrm{Lin}_K(V, V')$ tal que $T_1 \circ \phi = \phi'$. Como (V', ϕ') también lo es, existe un único $T_2 \in \mathrm{Lin}_K(V', V)$ tal que $T_2 \circ \phi' = \phi$. Esto demuestra que los dos diagramas dados son conmutativos. Por otra parte,

$$(T_2 \circ T_1) \circ \phi = T_2 \circ (T_1 \circ \phi) = T_2 \circ \phi' = \phi,$$

lo cual implica que el siguiente diagrama también es conmutativo



Si sustituimos $T_2 \circ T_1$ por I_V, el anterior diagrama también es conmutativo. Pero al ser (V, ϕ) es solución al problema, sólo hay una aplicación lineal tal que dicho diagrama es conmutativo lo cual implica que $T_2 \circ T_1 = I_V$. De manera análoga se demuestra que $T_1 \circ T_2 = I_{V'}$. □

185. Espacio vectorial producto

Vamos a construir el espacio vectorial producto de una colección cualquiera de espacios vectoriales. Sea Δ un conjunto no vacío de índices y $\{V_i : i \in \Delta\}$ una colección de espacios vectoriales sobre el cuerpo K. El conjunto producto cartesiano de los V_i se define según sabemos como

$$V = \prod_{i \in \Delta} V_i = \{f : \Delta \to \bigcup_{i \in \Delta} V_i : f \text{ es aplicación con } f(i) \in V_i \ \forall i \in \Delta\}.$$

Demostrar que$V$ es espacio vectorial con las operaciones:
Suma. Para todo $f, g \in V$, $(f + g)(i) = f(i) + g(i)$
Ley externa. Para todo $\alpha \in K$ y para todo $f \in V$, $(\alpha f)(i) = \alpha f(i)$.

SOLUCIÓN. 1) Veamos que $(V, +)$ es grupo abeliano.
Interna. Si $f, g \in V$, para todo $i \in \Delta$ se verifica $f(i) \in V_i$ y $g(i) \in V_i$ con lo cual $(f + g)(i) = f(i) + g(i) \in V_i$ luego $f + g \in V$.
Asociativa. Para todo $f, g, h \in V$ y para todo $i \in \Delta$,

$$((f + g) + h)(i) = (f + g)(i) + h(i) = (f(i) + g(i)) + h(i)$$
$$= f(i) + (g(i) + h(i)) = f(i) + (g + h)(i) = (f + (g + h))(i)$$
$$\Rightarrow (f + g) + h = f + (g + h).$$

Conmutativa. Para todo $f, g \in V$ y para todo $i \in \Delta$,

$$(f+g)(i) = f(i) + g(i) = g(i) + f(i) = (g+f)(i) \Rightarrow f + g = g + f.$$

Existencia de elemento neutro. Sea la aplicación $f_0(i) = 0$ para todo $i \in \Delta$. Claramente $f_0 \in V$ y para toda $f \in V$ y para todo $i \in \Delta$,

$$(f + f_0)(i) = f(i) + f_0(i) = f(i) + 0 = f(i) \Rightarrow f + f_0 = f,$$

con lo cual f_0 es elemento neutro para la suma.
Existencia de elemento simétrico. Sea la aplicación $f \in V$ y definimos la aplicación $-f$ como $(-f)(i) = -f(i)$ para todo $i \in \Delta$. Claramente $-f \in V$ y además

$$(f + (-f))(i) = f(i) + (-f)(i) = f(i) - f(i) = 0 \ \forall i \in \Delta \Rightarrow f + (-f) = f_0,$$

con lo cual $-f$ es elemento simétrico de f para la suma.

2) Veamos que se cumplen los cuatro axiomas de ley externa.
(a) Para todo $f, g \in V$ para todo $\alpha \in K$ y para todo $i \in \Delta$,

$$[\alpha(f+g)](i) = \alpha(f+g)(i) = \alpha(f(i) + g(i)) = \alpha f(i) + \alpha g(i)$$

$$= (\alpha f)(i) + (\alpha g)(i) = (\alpha f + \alpha g)(i) \Rightarrow \alpha(f+g) = \alpha f + \alpha g.$$

(b) Para todo $f \in V$ para todo $\alpha, \beta \in K$ y para todo $i \in \Delta$,

$$[(\alpha+\beta)f](i) = (\alpha+\beta)f(i) = \alpha f(i) + \beta f(i) = (\alpha f)(i) + (\beta f)(i)$$

$$= (\alpha f + \beta f)(i) \Rightarrow (\alpha+\beta)f = \alpha f + \beta f.$$

(c) Para todo $f \in V$ para todo $\alpha, \beta \in K$ y para todo $i \in \Delta$,

$$[(\alpha\beta)f](i) = (\alpha\beta)f(i) = \alpha[\beta f(i)] = \alpha[(\beta f)(i)]$$

$$= [\alpha(\beta f)](i) \Rightarrow (\alpha\beta)f = \alpha(\beta f).$$

(d) Para todo $f \in V$ y para todo $i \in \Delta$,

$$(1f)(i) = 1f(i) = f(i) \Rightarrow 1f = f.$$

□

186. Espacio suma directa externa

Sea Δ un conjunto no vacío de índices, $\{V_i : i \in \Delta\}$ una colección de espacios vectoriales sobre el cuerpo K y $V = \prod_{i\in\Delta} V_i$ el correspondiente espacio vectorial producto. Se define la *suma directa externa* de los espacios V_i como

$$\bigoplus_{i\in\Delta} V_i = \{f \in V : f(i) = 0 \text{ salvo un número finito de índices } i \in \Delta\}.$$

Demostrar que la suma directa externa de los espacios V_i es subespacio de V.

SOLUCIÓN. El vector nulo de f_0 de V cumple $f_0(i) = 0$ para todo $i \in \Delta$ luego lo cumple salvo el número finito nulo de subindides de Δ, es decir $f_0 \in \bigoplus_{i\in\Delta} V_i$. Si $f, g \in \bigoplus_{i\in\Delta} V_i$, entonces existen subconjuntos finitos Δ_1 y Δ_2 de Δ tales que

$$f(i) = 0 \text{ si } i \in \Delta - \Delta_1, \quad f(i) \neq 0 \text{ si } i \in \Delta_1,$$
$$g(i) = 0 \text{ si } i \in \Delta - \Delta_2, \quad g(i) \neq 0 \text{ si } i \in \Delta_2.$$

Entonces, si $\alpha, \beta \in K$ se verifica

$$i \in (\Delta - \Delta_1) \cap (\Delta - \Delta_2) \Rightarrow (\alpha f + \beta g)(i) = \alpha f(i) + \beta g(i) = 0$$

Ahora bien,

$$(\Delta - \Delta_1) \cap (\Delta - \Delta_2) = (\Delta \cap \Delta_1^c) \cap (\Delta \cap \Delta_2^c)$$
$$= \Delta \cap \Delta_1^c \cap \Delta_2^c = \Delta_1^c \cap \Delta_2^c = (\Delta_1 \cup \Delta_2)^c.$$

Entonces, $(\alpha f + \beta g)(i) \neq 0$ a lo sumo en $\Delta_1 \cup \Delta_2$ que es un conjunto finito. Es decir, $\alpha f + \beta g \in \bigoplus_{i\in\Delta} V_i$. □

Sea ahora $V_i = K$ para todo $i \in K$ y llamemos $U = \bigoplus_{i\in\Delta} K$, es decir la suma directa externa consta ahora de $|\Delta|$ copias de K. Para todo $i \in \Delta$ definimos el vector $\delta_i \in U$ de la forma $\delta_i(j) = 1$ si $j = i$ y $\delta_i(j) = 0$ si $j \neq i$. Es decir, $\delta_i(j) = \delta_{ij}$ (deltas de Kronecker).

187. Base del espacio suma directa externa

Demostrar que $B = \{\delta_i : i \in \Delta\}$ es base de $U = \bigoplus_{i\in\Delta} K$.

SOLUCIÓN. Veamos que B es sistema libre. Elijamos $S = \{\delta_{i_1}, \ldots, \delta_{i_m}\} \subset B$ y sea

$$\alpha_1\delta_{i_1} + \cdots + \alpha_m\delta_{i_m} = 0 \quad \text{con} \quad \alpha_1, \ldots, \alpha_m \in K.$$

Para todo $i = i_k$ con $k = 1, \ldots, m$ tenemos

$$(\alpha_1\delta_{i_1} + \cdots + \alpha_m\delta_{i_m})(i_k) = 0(i_k) \Rightarrow \alpha_k \cdot 1 = 0 \Rightarrow \alpha_k = 0.$$

Veamos que B es sistema generador. Si $f \in U$, existe un subconjunto finito $\Delta' = \{i_1, \ldots, i_n\}$ de Δ tal que $f(i) = 0$ si $i \in \Delta - \Delta'$ y $f(i) = 1$ si $i \in \Delta_1$. Veamos que se verifica

$$f = f(i_1)\delta_{i_1} + \cdots + f(i_n)\delta_{i_n}. \qquad (*)$$

En efecto,

$$i \in \Delta - \Delta' \Rightarrow (f(i_1)\delta_{i_1} + \cdots + f(i_n)\delta_{i_n})(i) = f(i_1)\delta_{i_1}(i) + \cdots + f(i_n)\delta_{i_n}(i)$$
$$= f(i_1) \cdot 0 + \cdots + f(i_n) \cdot 0 = 0 = f(i).$$

$$i \in \Delta' \Rightarrow (f(i_1)\delta_{i_1} + \cdots + f(i_n)\delta_{i_n})(i) = f(i)\delta_i(i) = f(i) \cdot 1 = f(i).$$

en consecuencia, se verifica la igualdad $(*)$. □

188. Solución al problema de la aplicación universal

Supongamos que el conjunto de índices Δ es un espacio vectorial. Entonces, tiene sentido en el espacio suma directa externa $U = \bigoplus_{i\in\Delta} K$ considerar vectores de la forma

$$\delta_{(i_1+\ldots+i_n)} - \delta_{i_1} - \ldots - \delta_{(i_1+\ldots+i_n)}, \quad \delta_{\alpha i} - \alpha\delta_i.$$

Sean ahora $V_1, \ldots, V_n$ espacios vectoriales sobre el cuerpo K y por simplicidad de notación, llamemos $Z = V_1 \times \ldots \times V_n$. Consideremos

$$U = \bigoplus_{(v_1,\ldots,v_n)\in Z} K$$

es decir, U es la suma directa externa de $|Z|$ copias de K. Consideremos el subespacio U_0 de U generado por vectores de la forma

$$\begin{aligned} &\delta_{(v_1,\ldots,v_i+v_i',\ldots,v_n)} - \delta_{(v_1,\ldots,v_i,\ldots,v_n)} - \delta_{(v_1,\ldots,v_i',\ldots,v_n)}, \\ &\delta_{(v_1,\ldots,\alpha v_i,\ldots,v_n)} - \alpha\delta_{(v_1,\ldots,v_i,\ldots,v_n)}. \end{aligned} \tag{188.1}$$

en donde i varía de 1 a n, y α recorre K. Por último, Consideremos el espacio vectorial cociente $V = U/U_0$ y la aplicación

$$\phi : V_1 \times \ldots \times V_n \to V, \quad \phi(v_1, \ldots, v_n) = \delta_{(v_1,\ldots,v_n)} + U_0.$$

Demostrar que el par (V, ϕ) es solución al problema de la aplicación universal.

SOLUCIÓN. Veamos que la aplicación ϕ es multilineal. Dado que

$$\begin{aligned} &\delta_{(v_1,\ldots,v_i+v_i',\ldots,v_n)} - \delta_{(v_1,\ldots,v_i,\ldots,v_n)} - \delta_{(v_1,\ldots,v_i',\ldots,v_n)} \in U_0, \\ &\delta_{(v_1,\ldots,\alpha v_i,\ldots,v_n)} - \alpha\delta_{(v_1,\ldots,v_i,\ldots,v_n)} \in U_0, \end{aligned}$$

y por definición de espacio cociente, podemos escribir

$$\begin{aligned} \phi(v_1, \ldots, v_i + v_i', \ldots, v_n) &= \delta_{(v_1,\ldots,v_i+v_i',\ldots,v_n)} + U_0 \\ &= \left(\delta_{(v_1,\ldots,v_i,\ldots,v_n)} + \delta_{(v_1,\ldots,v_i',\ldots,v_n)}\right) + U_0 \\ &= \left(\delta_{(v_1,\ldots,v_i,\ldots,v_n)} + U_0\right) + \left(\delta_{(v_1,\ldots,v_i',\ldots,v_n)} + U_0\right) \\ &= \phi(v_1, \ldots, v_i, \ldots, v_n) + \phi(v_1, \ldots, v_i', \ldots, v_n). \end{aligned}$$

De manera análoga,

$$\begin{aligned} \phi(v_1, \ldots, \alpha v_i, \ldots, v_n) &= \delta_{(v_1,\ldots,\alpha v_i,\ldots,v_n)} + U_0 \\ &= \alpha\delta_{(v_1,\ldots,v_i,\ldots,v_n)} + U_0 \\ &= \alpha\left(\delta_{(v_1,\ldots,v_i,\ldots,v_n)} + U_0\right) \\ &= \alpha\phi(v_1, \ldots, v_i, \ldots, v_n), \end{aligned}$$

y por tanto ϕ es multilineal.
Sea $\varphi : V_1 \times \ldots \times V_n \to W$ una aplicación multilineal. Tenemos que demostrar que existe una única aplicación lineal $T : V \to W$ tal que $T \circ \phi = \varphi$. Sabemos que $B = \{\delta_{(v_1,\ldots,v_n)} : (v_1, \ldots, v_n) \in Z\}$ es base de U y por tanto, existe una

única aplicación lineal $T_0 : U \to W$ tal que $T_0\left(\delta_{(v_1,\dots,v_n)}\right) = \varphi(v_1,\dots,v_n)$ para todo $(v_1,\dots,v_n) \in Z$. Como φ es multilineal, anula a los generadores 188.1 de U_0 y por tanto $U_0 \subset \ker T_0$. Por un conocido teorema de isomorfía, T_0 induce una aplicación lineal $T : U/U_0 \to W$ tal que

$$T\left(\delta_{(v_1,\dots,v_n)} + U_0\right) = T_0\left(\delta_{(v_1,\dots,v_n)}\right) = \varphi(v_1,\dots,v_n),$$

para todo $(v_1,\dots,v_n) \in Z$. Dado que $\phi(v_1,\dots,v_n) = \delta_{(v_1,\dots,v_n)} + U_0$, se verifica $T \circ \phi = \varphi$.
Por último, supongamos que $T' : V \to W$ es una aplicación lineal que verifica $T' \circ \phi = \varphi$. Tenemos que demostrar que $T' = T$. Dado que $T' \circ \phi = \phi$, se verifica $T' = T$ sobre Im ϕ. Pero de la construcción de V y ϕ es Im $\phi = V$ y por tanto $T' = T$. □

189. Concepto de espacio topológico (I)

1) *Definición.* Si X es un conjunto no vacío, se llama *topología* en X a cualquier colección T de subconjuntos de X que satisface los axiomas:

(1) $\emptyset, X \in T$.
(2) Si A y B son elementos de T, entonces $A \cap B \in T$.
(3) Si $\{A_i : i \in I\}$ es una familia de elementos de T, entonces $\bigcup_{i\in I} A_i \in T$.

A los elementos de T se les llama *conjuntos abiertos* y al par (X,T), e*spacio topológico.* Si no ha lugar a confusiones, al espacio topológico (X,T) se le designará simplemente por X.
Se considera el conjunto $X = \{1,2,3,4,5\}$. Demostrar que T es topología en X, siendo $T = \{\emptyset, X, \{1\}, \{3,4\}, \{1,3,4\}, \{2,3,4,5\}\}$.
2) Se considera el conjunto $X = \{1,2,3,4,5\}$. Demostrar que T no es topología en X, siendo $T = \{\emptyset, X, \{1\}, \{3,4\}, \{1,3,4\}, \{2,3,4\}\}$.
3) Se considera el conjunto $X = \{1,2,3,4,5\}$. Demostrar que T no es topología en X, siendo $T = \{\emptyset, X, \{1\}, \{3,4\}, \{1,3,4\}, \{1,2,4,5\}\}$.
4) Sea $X \neq \emptyset$ y $T = P(X)$ (conjunto de las partes de X). Demostrar que T es topología en X. Se la llama *topología discreta.*
5) Sea $X \neq \emptyset$ y $T = \{\emptyset, X\}$ Demostrar que T es topología en X. Se la llama *topología indiscreta.*
6) Sea $X \neq \emptyset$ y $T = \{\emptyset\} \cup \{A \subset X : A^c$ es finito$\}$. Demostrar que T es topología en X. Se la llama *topología de los complementos finitos.*

solución. 1) Los conjuntos $\emptyset$ y X pertenecen a T y es fácil comprobar que se verifican los otras dos condiciones de topología.

2) $\{1,3,4\}$ y $\{2,3,4\}$ pertenecen a T, sin embargo $\{1,3,4\} \cup \{2,3,4\} = \{1,2,3,4\} \notin T$.

3) $\{1,3,4\}$ y $\{1,2,4,5\}$ pertenecen a T, sin embargo $\{1,3,4\} \cap \{1,2,4,5\} = \{1,4\} \notin T$.

4) $\emptyset$ y X pertenecen a $P(X)$. Por otra parte sabemos $P(X)$ es cerrado con respecto a uniones e intersecciones arbitrarias, en consecuencia $T = P(X)$ es topología en X.

5) $\emptyset$ y X pertenecen a T. Por otra parte es inmediato verificar las otras dos condiciones de topología.

6) $\emptyset \in T$ por definición de T y $X^c = \emptyset$ que es finito, luego $X \in T$. Si $A, B \in T$ entonces, si uno de ellos es vacío, $A \cap B = \emptyset \in T$. Si ninguno de ellos es vacío, $(A \cap B)^c = A^c \cup B^c$ y al ser A^c y B^c finitos $A^c \cup B^c$ también lo es, luego $A \cap B \in T$. Sea ahora una familia $\{A_i : i \in I\}$ de elementos de T. Podemos suponer sin pérdida de generalidad que todos son no vacíos pues si algunos lo fueran, se pueden suprimir y la unión $\bigcup_{i\in I} A_i$ no varía. Tenemos $\left(\bigcup_{i\in I} A_i\right)^c = \bigcap_{i\in I} A_i^c$ y este conjunto es finito al estar contenido en cada A_i^c que es finito. Por tanto, $\bigcup_{i\in I} A_i \in T$.¡/li¿ □

190. Concepto de espacio topológico (II)

1) Sea X un conjunto y $p \in X$ fijo. Demostrar que $T = \{\emptyset\} \cup \{A \subset X : p \in X\}$ es un topología en X. Se la llama *topología del punto particular.*
2) Para todo $n \in \mathbb{N}$ se define $S_n = \{n.n + 1, n + 2, \ldots\}$. Demostrar que $T = \{\emptyset\} \cup \{S_n : n \in \mathbb{N}\}$ es una topología en $\mathbb{N}$. Determinar todos los abiertos que contienen al número natural n_0.
3) Demostrar que $T = \{\emptyset, \mathbb{R}\} \cup \{I_q : q \in \mathbb{Q}\}$ con $I_q = (0, +\infty)$ no es una topología en $\mathbb{R}$.
4) Sea $X \neq \emptyset$ un conjunto e (Y, T') un espacio topológico. Sea $f : X \to Y$ una aplicación. Demostrar que $T = \{f^{-1}(G) : G \in T'\}$ es topología en X.
5) Sea (X, T) un espacio topológico tal que para todo $x \in X$ el conjunto unitario $\{x\}$ es abierto. Demostrar que T es la topología discreta.
6) Sea X un conjunto infinito y T una topología sobre X en la cual todos los subconjuntos infinitos de X son abiertos. Demostrar que T es la topología discreta.

solución. 1) $\emptyset \in T$ por definición de T y $p \in X$ por tanto, $X \in T$. Si A y B son abiertos y alguno de ellos es vacío, $A \cap B = \emptyset$, que es abierto. Si ambos son no vacíos, ambos contienen a p y por tanto, $A \cap B$ también lo contiene, es decir $A \cap B$ es abierto. De la misma forma si $\{A_i\}$ es familia de abiertos, podemos suponer sin pérdida de generalidad que todos son no vacíos pues si algunos lo fueran, se pueden suprimir y la unión $\bigcup_i A_i$ no varía. Entonces $p \in A_i$ para todo i con lo cual $p \in \bigcup_i A_i$ y por tanto $\bigcup_i A_i$ es abierto.

2) $\emptyset \in T$ por definición de T y $\mathbb{N} = S_0 \in T$. Si $A, B \in T$ entonces, si uno de ellos es vacío, $A \cap B = \emptyset \in T$. Si ninguno de ellos es vacío, entonces $A = S_m$ y $B = S_k$ para ciertos m, k números naturales y $S_m \cap S_k = S_{\text{máx}\{m,k\}} \in T$. Sea una familia $\{A_i : i \in I\}$ de elementos de T. Podemos suponer sin pérdida de generalidad que todos son no vacíos pues si algunos lo fueran, se pueden

suprimir y la unión de los A_i no varía. Entonces, la unión de los A_i es de la forma $\bigcup_{i\in I\subset\mathbb{N}} S_i = S_{\text{mín}\{i:i\in I\}} \in T$. Es claro que los abiertos que contienen a n_0 son $S_0, S_1 S_2, \ldots, S_{n_0}$.

3) Consideremos la familia de elementos de T dada por $\{I_q : q > \sqrt{2}\}$. Es claro que su unión es $\bigcup_{q>\sqrt{2}} I_q = (\sqrt{2}, +\infty)$ y por tanto no pertenece a T pues $\sqrt{2}$ es irracional.

4) $\emptyset = f^{-1}(\emptyset)$ y $X = f^{-1}(Y)$ con lo cual $\emptyset, X \in T$. Si $A, B \in T$ existen $G_1, G_2 \in T'$ tales que $A = f^{-1}(G_1)$ y $B = f^{-1}(G_2)$. Entonces, $A \cap B = f^{-1}(G_1) \cap f^{-1}(G_2) = f^{-1}(G_1 \cap G_2)$. Pero $G_1 \cap G_2 \in T'$ por ser T' topología, luego $A \cap B \in T$. Si $\{A_i : i \in I\}$ es una familia de elementos de T, existen $G_i \in T'$ tales que $A_i = f^{-1}(G_i)$. Entonces, $\bigcup_{i\in I} A_i = \bigcup_{i\in I} f^{-1}(G_i) = f^{-1}\left(\bigcup_{i\in I} G_i\right)$. Pero $\bigcup_{i\in I} G_i \in T'$ por ser T' toplogía, luego $\bigcup_{i\in I} A_i \in T$.

5) Si $A \subset X$ entonces, $A = \bigcup_{x\in A}\{x\}$ que es unión de abiertos y por tanto abierto. Nótese que también es váldo para $A = \emptyset$ pues sabemos que la unión de una familia vacía de conjuntos es el conjunto vacío.

6) Al ser X infinito, contiene a un subconjunto numerable, conjunto que será de la forma $\{x_1, x_2, x_3, \ldots\}$. Llamemos $A = \{x_1, x_3, x_5, \ldots\}$. Entonces, A y A^c son infinitos y para todo $x \in X$ se verifica $\{x\} = (A \cup \{x\}) \cap (A^c \cup \{x\})$. Pero $A \cup \{x\}$ y $A^c \cup \{x\}$ son infinitos y por tanto abiertos, con lo cual todo subconjunto unitario $\{x\}$ de X es abierto. Por el problema anterior concluimos que T es la topología discreta. □

191. Concepto de espacio topológico (III)

1) Demostrar el siguiente teorema:
Teorema. Sea $\{T_i : i \in I\}$ una familia de topologías en un conjunto X. Entonces, la intersección $T = \bigcap_i T_i$ es también una topología en X.
2) Demostrar la unión de dos topologías en X no tiene por qué ser topología en X.
3) *Definición.* Sean T y T' dos topologías en X. Se dice que T es *menos fina* que T' o bien que T' es *más fina* que T, si $T \subset T'$. Dado un conjunto X no vacío, determinar la topología más fina y la menos fina que se pueden definir en X.
4) Demostrar el siguiente teorema:
Teorema. Sea X un conjunto no vacío y sea

$$\mathscr{T}(X) = \{T : T \text{ es topología en } X\} \subset P\left(P(X)\right).$$

Entonces, $(\mathscr{T}(X), \subset)$ es un conjunto ordenado con primer y último elemento. Si X es un conjunto con más de un elemento, $(\mathscr{T}(X), \subset)$ no está totalmente ordenado.
5) Sea X un conjunto no vacío y T una colección de subconjuntos de X. Demostrar que T es una topología en X si y sólo si se verifican los axiomas:

[1) $\emptyset, X \in T$.
(2) Si A y B son elementos de T, entonces $A \cap B \in T$.
(3′) Si $\{A_i : i \in I\}$ es una familia de elementos de $T - \{\emptyset, X\}$, entonces $\bigcup_{i\in I} A_i \in T$.
6) Para cada entero positivo n se considera el intervalo abierto de la recta real $I_n = (-n, n)$. Demostrar que $(\mathbb{R}, T)$ es espacio topológico, en donde $T = \{\emptyset, \mathbb{R}\} \cup \{I_n : n = 1, 2, \ldots\}$.

SOLUCIÓN. 1) (1) Al ser T_i topología para todo i, $\emptyset$ y $X \in T_i$ para todo i, por tanto $\emptyset, X \in \bigcap_i T_i$.
(2) Si $A, B \in \bigcap_i T_i$, entonces, $A, B \in T_i$ para todo i y al ser T_i topología, $A \cap B \in T_i$ para todo i luego $A \cap B \in \bigcap_i T_i$.
(3) Si $\{A_j : j \in J\}$ es familia de elementos de $\bigcap_i T_i$, entonces para todo j, $A_j \in T_i$ para todo i. Al ser T_i topología, $\bigcup_j A_j \in T_i$ para todo i, luego $\bigcup_j A_j \in \bigcap_i T_i$.

2) Sea $X = \{a, b, c\}$. Es inmediato comprobar que $T_1 = \{\emptyset, X, \{a\}\}$ y $T_2 = \{\emptyset, X, \{b\}\}$ son topologías en X. Sin embargo $T_1 \cup T_2 = \{\emptyset, X, \{a\}, \{b\}\}$ no es topología pues $\{a\}$ y $\{b\}$ pertenecen a $T_1 \cup T_2$ sin embargo, $\{a\} \cup \{b\} = \{a, b\} \notin T_1 \cup T_2$.

3) Claramente la menos fina es la indiscreta y la más fina, la discreta.

4) $\mathscr{T}(X)$ es un conjunto ordenado por la inclusión $\subset$ por ser subconjunto de $P(P(X))$ que está ordenado por $\subset$. Claramente la topología indiscreta T_I es el primer elemento de $\mathscr{T}(X)$ y la discreta T_D es el último elemento. Si X contiene a los elementos distintos x_1 y x_2, entonces $T_1 = \{\emptyset, X, \{x_1\}\}$ y $T_2 = \{\emptyset, X, \{x_2\}\}$ son topologías en X no comparables.

5) Si T es topología se verifican trivialmente los axiomas (1), (2) y (3′). Si se verifican los axiomas (1), (2) y (3′), trivialmente se verifican los axiomas (1) y (2) de topología. Falta pues demostrar que se verifica el (3). En efecto, sea $\{A : A \in \mathscr{A}\}$ una familia de elementos de T. Si $X \in \mathscr{A}$ entonces, $\bigcup_{A\in\mathscr{A}} A = X$ que pertenece a T por (1). Si $X \notin \mathscr{A}$, entonces $\bigcup_{A\in\mathscr{A}} A = \bigcup_{A\in\mathscr{A}-\{X\}} A$. Dado que el conjunto vacío no añade ningún elemento a la unión, podemos expresar

$$\bigcup_{A\in\mathscr{A}} A = \bigcup_{A\in\mathscr{A}-\{X\}} A = \bigcup_{A\in\mathscr{A}-\{X,\emptyset\}} A,$$

y por (3′), $\bigcup_{A\in\mathscr{A}} A \in T$.

6) Por hipótesis. $\emptyset$ y $\mathbb{R}$ pertenecen a T. Sean $A, B \in T$. Los elementos de T están totalmente ordenados por inclusión: $\emptyset \subset I_1 \subset I_2 \subset \ldots \subset \mathbb{R}$ y por tanto, la intersección de dos elementos de T pertenece a T. Usamos el apartado anterior. Sea $\{A_i : i \in I\}$ una familia de elementos de $T - \{\emptyset, \mathbb{R}\}$. Cada i es de la forma $A_i = I_{n_i}$ con n_i entero positivo. Pero en este caso, si el conjunto

$\{n_i : i \in I\}$ está acotado superiormente, $\bigcup_{n_i \in I} I_{n_i} = I_{\text{máx}\{n_i : i \in I\}} \in T$ y si no está acotado, $\bigcup_{n_i \in I} I_{n_i} = \mathbb{R} \in T$. □

192. Punto de acumulación (I)

Sea X un espacio topológico. Un punto $x \in X$ se dice que es *punto de acumulación* o *punto límite* de un subconjunto A de X si para todo abierto G que contiene a x se verifica $(G - \{x\}) \cap A \neq \emptyset$. Al conjunto de los puntos de acumulación de A se le denota por A' y se le llama *conjunto derivado* de A.

1) Se considera el conjunto $X = \{1, 2, 3, 4, 5\}$ con la topología

$$T = \{\emptyset, X, \{1\}, \{3, 4\}, \{1, 3, 4\}, \{2, 3, 4, 5\}\}.$$

Determinar el conjunto derivado de $A = \{1, 2, 3\}$.

2) Sea X el espacio topológico indiscreto, es decir con la topología indiscreta T_I. Determinar el conjunto derivado de cualquier subconjunto A de X.

3) Sea X el espacio topológico discreto, es decir con la topología discreta T_D. Determinar el conjunto derivado de cualquier subconjunto A de X.

4) Sean A y B dos subconjuntos de un espacio topológico X. Demostrar que $A \subset B \Rightarrow A' \subset B'$.

solución. 1) Analicemos cada elemento de X :

(a) Punto $x = 1$. $G = \{1\}$ es abierto que contiene a 1, pero $(G - \{1\}) \cap A = \emptyset$, luego 1 no es punto de acumulación de A.

(b) Punto $x = 2$. Los abiertos G que contienen a 2 son X y $\{2, 3, 4, 5\}$ y en ambos casos $(G - \{2\}) \cap A \neq \emptyset$, luego 2 es punto de acumulación de A.

(c) Punto $x = 3$. $G = \{3, 4\}$ es abierto que contiene a 3 pero $(G - \{3\}) \cap A = \emptyset$, luego 3 no es punto de acumulación de A.

(d) Punto $x = 4$. Los abiertos G que contienen a 4 son X, $\{3, 4\}$, $\{1, 3, 4\}$, y $\{2, 3, 4, 5\}$ y en todos lo casos $(G - \{4\}) \cap A \neq \emptyset$, luego 4 es punto de acumulación de A.

(e) Punto $x = 5$. Los abiertos G que contienen a 5 son X y $\{2, 3, 4, 5\}$ y en ambos casos $(G - \{5\}) \cap A \neq \emptyset$, luego 5 es punto de acumulación de A.

Concluimos que el conjunto derivado de A es $A' = \{2, 4, 5\}$.

2) El único abierto que contiene a algún punto es $G = X$. Si $A = \emptyset$, entonces para todo $x \in X$ se verifica $(G - \{x\}) \cap A = \emptyset$, luego $A = \emptyset$ no tiene puntos de acumulación. Si $A = \{a\}$ consta de un único elemento se verifica $(G - \{a\}) \cap A = \emptyset$ y $(G - \{x\}) \cap A \neq \emptyset$ si $x \neq a$, luego los puntos de acumulación son todos los $x \in X$ distintos de a. Si $A = \{a, b, \ldots\}$ consta de más de un punto, entonces $(G - \{x\}) \cap A \neq \emptyset$ para todo $x \in X$ y los puntos de A son todos los de X. En consecuencia,

$$A' = \begin{cases} \emptyset & \text{si} \quad A = \emptyset \\ X - \{a\} & \text{si} \quad A = \{a\} \\ X & \text{si} \quad A \text{ contiene más de un punto.} \end{cases}$$

3) Sea $A \subset X$. Para todo $x \in X$ el conjunto $G = \{x\}$ es abierto que contiene a x y se verifica $(G - \{x\}) \cap A = \emptyset \cap A = \emptyset$ luego A no tiene puntos de acumulación. Concluimos que $A' = \emptyset$ para todo $A \subset X$.

4) Si $x \in A'$, para todo abierto G que contiene a x se verifica $(G - \{x\}) \cap A \neq \emptyset$. Pero al cumplirse $A \subset B$, también $(G - \{x\}) \cap B \neq \emptyset$ lo cual implica que $x \in B'$. Es decir, $A' \subset B'$. □

193. Punto de acumulación (II)

1) Sea A un subconjunto de un espacio topológico X. Demostrar que $x \in X$ no es punto de acumulación de A si y sólo si existe un abierto G tal que $x \in G$ y $G \cap A \subset \{x\}$.
2) Sean A y B dos subconjuntos de un espacio topológico X. Demostrar que $(A \cup B)' = A' \cup B'$.
3) Sean A y B dos subconjuntos de un espacio topológico X. Demostrar que $(A \cap B)' \subset A' \cap B'$.
4) Encontrar un caso en el que no se verifique la igualdad $(A \cap B)' = A' \cap B'$.
5) Sean T y T' dos topologías en X con T' más fina que T y sea $A \subset X$. Demostrar que si x es punto de acumulación de A con respecto a T', también lo es con respecto a T. Construir un contraejemplo que demuestre que el recíproco es falso.

solución. 1) Tenemos las siguientes equivalencias:
x no es punto de acumulación de A
$\Leftrightarrow \exists G$ abierto con $x \in G$ y $(G - \{x\}) \cap A = \emptyset$
$\Leftrightarrow \exists G$ abierto con $x \in G$ y o bien $G \cap A = \emptyset$ o bien $G \cap A = \{x\}$
$\Leftrightarrow \exists G$ abierto con $x \in G$ y $G \cap A \subset \{x\}$.

2) Veamos que $A' \cup B' \subset (A \cup B)'$. Se verifica $A \subset A \cup B$ y $B \subset A \cup B$ y por apartado 4) del problema anterior, $A' \subset (A \cup B)'$ y $B' \subset (A \cup B)'$ por tanto, $A' \cup B' \subset (A \cup B)'$. Veamos ahora que $(A \cup B)' \subset A' \cup B'$. Si $x \not\subset A' \cup B'$, entonces $x \notin A'$ y $x \notin B'$. Por el apartado anterior, existen abiertos G, H tales que $x \in G$, $G \cap A \subset \{x\}$, $x \in H$, $H \cap B \subset \{x\}$. El conjunto $G \cap H$ es abierto y $x \in G \cap H$. Además,

$$(G \cap H) \cap (A \cup B) = (G \cap H \cap A) \cup (G \cap H \cap B) \subset \{x\} \cup \{x\} = \{x\},$$

lo cual implica que $x \notin (A \cup B)'$. Es decir, $(A \cup B)' \subset A' \cup B'$.

3) Si $x \in (A \cap B)'$ entonces, para todo abierto G que contiene a x se verifica $(G - \{x\}) \cap (A \cap B) \neq \emptyset$. Ahora bien, tanto $(G - \{x\}) \cap A$ como $(G - \{x\}) \cap B$ contienen a $(G - \{x\}) \cap (A \cap B)$ y por tanto, son no vacíos con lo cual $x \in A'$ y $x \in B'$, esto es, $x \in A' \cap B'$.

4) Consideremos en el conjunto con tres elementos $X = \{a, b, c\}$ la topología indiscreta. Elijamos $A = \{a\}$ y $B = \{b\}$. Según el apartado 2) del

problema anterior, $A' = \{b, c\}$ y $B' = \{a, c\}$. Entonces, $(A \cap B)' = \emptyset' = \emptyset$ y $A' \cap B' = \{c\}$. Es decir, no se verifica la igualdad.

5) Si x es punto de acumulación de A con respecto a T' entonces, para todo $G \in T'$ tal que $x \in G$ se verifica $(G - \{x\}) \cap A \neq \emptyset$. Por hipótesis $T \subset T'$, luego la relación $(G - \{x\}) \cap A \neq \emptyset$ también se verifica para todo $G \in T$ con $x \in G$ y por tanto, x es punto de acumulación de A con respecto a T. Para demostrar que el recíproco no es en general cierto, elijamos $X = \{a, b\}$, la topología indiscreta T y la discreta T', con lo cual T' es más fina que T. Si $A = \{a\}$, es inmediato verificar que b es punto de acumulación de A con respecto a T pero no con respecto a T'. □

194. Los grupos $\mathbb{R}^\times$ y $\mathbb{C}^\times$ no son isomorfos

Demostrar que los grupos multiplicativos $\mathbb{R}^\times$ y $\mathbb{C}^\times$ no son isomorfos.

solución. Supongamos que existe un isomorfismo $f : \mathbb{C}^\times \to \mathbb{R}^\times$. Tenemos $f(i^2) = f(-1)$. Ahora bien,

$$1 = f(1) = f[(-1)(-1)] = f(-1)f(-1) = f(-1)^2 \Rightarrow f(-1) = \pm 1.$$

Al ser f inyectiva y $f(1) = 1$, ha de ser necesariamente $f(-1) = -1$. Es decir, $f(i^2) = -1$. Pero al ser f homomorfismo, $f(i^2) = f(i)^2$, con lo cual queda $f(i)^2 = -1$. Esto es absurdo al ser $f(i)$ real. Concluimos que $\mathbb{R}^\times$ y $\mathbb{C}^\times$ no son isomorfos. □

195. Extensión finita y algebraica

Sea K/k una extensión de cuerpos. Se dice que K es *extensión finita* de k si $[K : k]$ es finito. Se dice que K es *extensión infinita* de k si $[K : k] = \infty$. Se dice que K es *extensión algebraica* de k si todo $\alpha \in K$ es algebraico sobre k.
1) Demostrar que toda extensión finita K de k es algebraica.
2) Sea K/k una extension de cuerpos. Demostrar que el conjunto A de los elementos $a \in K$ que son algebraicos sobre k es un cuerpo tal que $k \subset A \subset K$. Al cuerpo A se le llama *clausura algebraica* de k en K.
3) Sea la extensión $\mathbb{R}/\mathbb{Q}$ y sea A la clausura algebraica de $\mathbb{Q}$ en $\mathbb{R}$. Demostrar que $[A : \mathbb{Q}] = \infty$ (esto prueba que no toda extensión algebraica es finita).

solución. 1) Si $[K : k] = \nu$ y $\alpha \in K$. Los $\nu + 1$ elementos $e = \alpha^0, \alpha, \ldots, \alpha^\nu$ de K son linealmente dependientes sobre k y por tanto existen elementos $a_0, a_1, \ldots, a_n$ de k no todos nulos tales que $a_0 + a_1\alpha + \ldots + a_n\alpha^n = 0$ es decir, α es algebraico sobre k.

2) Sean $a, b \in A$. Por ser a algebraico sobre k la dimensión $[k(a) : k]$ es finita. Por ser b algebraico sobre k lo es sobre $k(a)$ y por tanto, la dimensión $[k(a)(b) : k(a)]$ es finita. En consecuencia $k(a, b) = k(a)(b)$ tiene dimensión finita sobre k, luego $k(a, b)$ es extensión algebraica de k. Al ser $a, b \in k(a, b)$ y $k(a, b)$ cuerpo, se verifica que $a + b$, ab y a^{-1} (si $a \neq 0$) son elementos de

$k(a,b)$ y por tanto algebraicos sobre k. En consecuencia, $a, b \in A$ implica que $a+b$, ab y a^{-1} (si $a \neq 0$) son elementos de A, luego A es cuerpo y trivialmente se verifica $k \subset A \subset K$.

3) En efecto, los números $\sqrt[n]{2}$ son algebraicos para todo entero $n \geq 1$. El polinomio $f_n(x) = x^n - 2$ es mónico y anula a $\sqrt[n]{2}$. También es irreducible en $\mathbb{Q}[x]$ como inmediatamente se comprueba aplicando el criterio de Eisenstein con $p = 2$. Es decir, f_n es polinomio mínimo de $\sqrt[n]{2}$ sobre $\mathbb{Q}$ con lo cual $[\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}] = n$. Al ser n arbitrario, la extensión $A/\mathbb{Q}$ no puede ser finita. □

196. Unicidad del cuerpo de ruptura

Sean $k(\alpha)$ y $k(\beta)$ cuerpos de ruptura de $f(x) \in k[x]$. Demostrar que $k(\alpha)$ y $k(\beta)$ son isomorfos.

solución. Si $f(x) = a_m x^m + \ldots + a_1 x + a_0$, el polinomio $p(x) = (1/a_m) f(x)$ es irreducible en $k(x)$, mónico y $p(\alpha) = 0$ por tanto $p(x)$ es polinomio mínimo de α en la extensión $k(\alpha)/k$. Esto implica que $[k(\alpha) : k] = m$ y los elementos de $k(\alpha)$ son de la forma $c_0 + c_1\alpha + \ldots + c_{m-1}\alpha^{m-1}$ con los c_i en k determinados de manera única. De manera análoga, los elementos de $k(\beta)$ son de la forma $c_0 + c_1\beta + \ldots + c_{m-1}\beta^{m-1}$ con los c_i en k determinados de manera única. Entonces, es inmediato comprobar que la aplicación $\Phi : k(\alpha) \to k(\beta)$ dada por $\Phi(c_0 + c_1\alpha + \ldots + c_{m-1}\alpha^{m-1}) = c_0 + c_1\beta + \ldots + c_{m-1}\beta^{m-1}$ es un isomorfismo de cuerpos. □

197. Un cuerpo de matrices isomorfo al de los complejos

1) Demostrar que el conjunto $\mathcal{A} = \{A_{(x,y)} = \begin{bmatrix} x & y \\ -y & x \end{bmatrix} : x, y \in \mathbb{R}\}$ es un cuerpo con las operaciones suma y producto habituales de matrices.
2) Demostrar que la aplicación $f : \mathbb{C} \to \mathcal{A}$ dada por $f(x+iy) = A_{(x,y)}$ es un isomorfismo de cuerpos.

solución. 1) Veamos que $\mathcal{A}$ es subanillo de $\mathbb{R}^{2\times 2}$. En efecto, claramente $0 = A_{(0,0)} \in \mathcal{A}$. Para todo par de matrices $A_{(x,y)}$ y $A_{(x',y')}$ se verifica

$$A_{(x,y)} - A_{(x',y')} = \begin{bmatrix} x & y \\ -y & x \end{bmatrix} - \begin{bmatrix} x' & y' \\ -y' & x' \end{bmatrix} = \begin{bmatrix} x-x' & y-y' \\ -(y-y') & x-x' \end{bmatrix}$$

y por tanto, $A_{(x,y)} - A_{(x',y')} = A_{(x-x',y-y')} \in \mathcal{A}$. Por otra parte,

$$A_{(x,y)}A_{(x',y')} = \begin{bmatrix} x & y \\ -y & x \end{bmatrix} \begin{bmatrix} x' & y' \\ -y' & x' \end{bmatrix} = \begin{bmatrix} xx'-yy' & xy'+yx' \\ -(yx'+xy') & xx'-yy' \end{bmatrix}$$

y por tanto, $A_{(x,y)}A_{(x',y')} = A_{(xx'-yy',xy'+yx')} \in \mathcal{A}$. Hemos demostrado que $\mathcal{A}$ es anillo. Es unitario pues $I = A_{(1,0)} \in \mathcal{A}$ y también conmutativo pues

$$A_{(x',y')}A_{(x,y)} = \begin{bmatrix} x' & y' \\ -y' & x' \end{bmatrix} \begin{bmatrix} x & y \\ -y & x \end{bmatrix} = \begin{bmatrix} x'x-y'y & x'y+y'x \\ -(x'y+y'x) & x'x-y'y \end{bmatrix},$$

es decir $A_{(x',y')}A_{(x,y)} = A_{(x,y)}A_{(x',y')}$. Falta demostrar que todo $A_{(x,y)} \in \mathcal{A}$ con $(x,y) \neq (0,0)$ tiene inverso en $\mathcal{A}$. En efecto, $\det A_{(x,y)} = x^2 + y^2 \neq 0$ y por tanto $A_{(x,y)}$ es invertible siendo su inversa

$$(A_{(x,y)})^{-1} = \frac{1}{x^2+y^2}\begin{bmatrix} x & -y \\ y & x \end{bmatrix} = A_{\left(\frac{x}{x^2+y^2}, \frac{-y}{x^2+y^2}\right)} \in \mathcal{A}.$$

2) Para cualquier par de números complejos $x+iy,\ x'+iy'$:

$$f[(x+iy)+(x'+iy')] = f[(x+x')+(y+y')i] = \begin{bmatrix} x+x' & y+y' \\ -(y+y') & x+x' \end{bmatrix}$$

$$= \begin{bmatrix} x & y \\ -y & x \end{bmatrix} + \begin{bmatrix} x' & y' \\ -y' & x' \end{bmatrix} = f(x+iy) + f(x'+iy').$$

Por otra parte,

$$f[(x+iy)(x'+iy')] = f[(xx'-yy')+(xy'+yx')i] =$$

$$\begin{bmatrix} xx'-yy' & xy'+yx' \\ -(xy'+yx') & xx'-yy' \end{bmatrix} = \begin{bmatrix} x & y \\ -y & x \end{bmatrix}\begin{bmatrix} x' & y' \\ -y' & x' \end{bmatrix} = f(x+iy)f(x'+iy').$$

Al ser la imagen de f no trivial, f es homomorfismo entre los cuerpos $\mathbb{C}$ y $\mathcal{A}$. Su núcleo es:

$$\ker f = \{x+iy \in \mathbb{C} : f(x+iy) = \begin{bmatrix} x & y \\ -y & x \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}\} = \{0+0i\} = \{0\},$$

por tanto f es inyectiva. Por último, cualquier elemento de $\mathcal{A}$ se puede expresar en la forma:

$$\begin{bmatrix} x & y \\ -y & x \end{bmatrix} = f(x+iy),$$

es decir f es sobreyectiva. Hemos demostrado pues que f es un isomorfismo entre los cuerpos $\mathbb{C}$ y $\mathcal{A}$. □

198. Inverso en un cuerpo de ruptura

1) Sea $k(\xi)$ cuerpo de ruptura de un polinomio $f(x) \in k[x]$. Si $0 \neq \beta \in k(\xi)$, dar una fórmula para calcular β^{-1} en términos de una igualdad de Bezout. 2) *Aplicación.* Sea $f(x) = x^3 - 3x - 1 \in \mathbb{Q}[x]$ y $\mathbb{Q}(\xi)$ cuerpo de ruptura de $f(x)$. Determinar el inverso en $\mathbb{Q}(\xi)$ de $\beta = \xi^4 + 2\xi^3 + 3$.

solución. 1) Podemos expresar β en la forma $\beta = g(\xi)$ con $g(x) \in k[x]$ y grad $g(x) <$ grad $f(x)$. Por la igualdad de Bezout, existen $A(x), B(x) \in k[x]$ tales que

$$A(x)f(x) + B(x)g(x) = D(x), \quad D(x) = \text{mcd } \{f(x), g(x)\}.$$

Pero $f(x)$ es irreducible y grad $g(x) <$ grad $f(x)$, por tanto $D(x) = 1$. Sustituyendo x por ξ y teniendo en cuenta que $f(\xi) = 0$ queda $B(\xi)g(\xi) = 1$. Es decir, $\beta^{-1} = B(\xi)$.

2) Las únicas posibles raíces racionales de $f(x)$ son ± 1 pero $f(1) \neq 0$ y $f(-1) \neq 0$ y al ser de tercer grado, es irreducible en $\mathbb{Q}$. Dividiendo x^4+2x^3+3

entre $f(x)$ obtenemos como resto $g(x) = 3x^2 + 7x + 5$ con lo cual $\beta = 3\xi^2 + 7\xi + 5$. Tenemos mcd $\{f(x), g(x)\} = 1$ y aplicando el algoritmo de Euclides, obtenemos la igualdad de Bezout

$$\left(-\frac{7}{37}x + \frac{29}{111}\right) f(x) + \left(\frac{7}{111}x^2 - \frac{26}{111}x + \frac{28}{111}\right) g(x) = 1,$$

por tanto $\beta^{-1} = (7/111)\xi^2 - (26/111)\xi + 28/111$. □

199. El conjunto de los números algebraicos es contable

Trabajamos en la extensión de cuerpos $\mathbb{R}/\mathbb{Q}$.
1) Demostrar que el conjunto de los números algebraicos es contable.
2) Demostrar que el conjunto de los números trasdecendentes no es contable.

solución. 1) El conjunto A de los números algebraicos se puede expresar en la forma: $A = \bigcup_{p\in P} R(p)$ en donde P representa el conjunto de los polinomios mónicos de $\mathbb{Q}[x]$ y $R(p)$ el conjunto de las raíces de p. Dado que para cada p el conjunto $R(p)$ es finito, bastará demostrar que P es contable. Pero $P = \bigcup_{n=1}^{\infty} P_n$ en donde P_n es el conjunto de los polinomios mónicos de grado n con coeficientes racionales. La aplicación

$$\mathbb{Q}^n \to P_n, \quad (a_0, a_1, \ldots, a_{n-1}) \mapsto x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$$

es claramente biyectiva y al ser $\mathbb{Q}^n$ contable, lo es P_n. Entonces P es unión contable de conjuntos contables y por tanto es contable.

2) Si T es el conjunto de los números trascendentes, tenemos $\mathbb{R} = A \cup T$. Si T fuera contable, al ser A contable también lo sería $\mathbb{R}$ lo cual es una contradicción. □

200. Anillos $\mathbb{Z}[\sqrt{d}]$

Sea $d \in \mathbb{Z} - \{0, 1\}$ y libre de cuadrados, es decir no es divisible por el cuadrado de ningún entero salvo el 1. Se define

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

1) Demostrar que $\mathbb{Z}[\sqrt{d}]$ es subanillo de $\mathbb{C}$.
2) Demostrar que $\mathbb{Z}[\sqrt{d}]$ es dominio de integridad.
3) Para todo $\alpha = a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ se define el *conjugado* de α como $\overline{\alpha} = a - b\sqrt{d}$. Demostrar que para todo $\alpha, \beta \in \mathbb{Z}[\sqrt{d}]$ se verifica $\overline{\alpha\beta} = \overline{\alpha}\overline{\beta}$.
4) Para todo $\alpha \in \mathbb{Z}[\sqrt{d}]$ se define la *norma* de α como $N(\alpha) = \alpha\overline{\alpha}$. Demostrar que N es función con valores enteros y multiplicativa.
5) Sea $\alpha \in \mathbb{Z}[\sqrt{d}]$. Demostrar que: $N(\alpha) = \pm 1 \Leftrightarrow \alpha$ es unidad en $\mathbb{Z}[\sqrt{d}]$.

solución. 1) Claramente $\emptyset \neq \mathbb{Z}[\sqrt{d}] \subset \mathbb{C}$. Si $a + b\sqrt{d}, a' + b'\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$, se verifica

$$(a + b\sqrt{d}) - (a' + b'\sqrt{d}) = (a - a') + (b - b')\sqrt{d}$$

y al ser $a-a'$ y $b-b'$ enteros, $(a+b\sqrt{d})-(a'+b'\sqrt{d})\in\mathbb{Z}[\sqrt{d}]$. Por otra parte

$$(a+b\sqrt{d})(a'+b'\sqrt{d})=aa'+dbb'+(ab'+ba')\sqrt{d}$$

y al ser $aa'+dbb'$ y $ab'+ba'$ enteros, $(a+b\sqrt{d})(a'+b'\sqrt{d})\in\mathbb{Z}[\sqrt{d}]$. Concluimos pues que $\mathbb{Z}[\sqrt{d}]$ es subanillo de $\mathbb{C}$.

2) $\mathbb{Z}[\sqrt{d}]$ es conmutativo por serlo $\mathbb{C}$, es unitario pues $1=1+0\sqrt{d}\in\mathbb{Z}[\sqrt{d}]$ y es anillo de integridad por serlo $\mathbb{C}$, en consecuencia $\mathbb{Z}[\sqrt{d}]$ es dominio de integridad.

3) En efecto, si $\alpha=a+b\sqrt{d}$ y $\beta=a'+b'\sqrt{d}$,

$$\overline{\alpha}\,\overline{\beta}=(a-b\sqrt{d})(a'-b'\sqrt{d})=aa'+dbb'-(ab'+ba')\sqrt{d},$$

$$\overline{\alpha\beta}=\overline{aa'+dbb'+(ab'+ba')\sqrt{d}}=aa'+dbb'+(ab'-ba')\sqrt{d}.$$

4) Para todo $\alpha=a+b\sqrt{d}$, su norma es $N(\alpha)=\alpha\overline{\alpha}=(a+b\sqrt{d})(a-b\sqrt{d})=a^2-db^2\in\mathbb{Z}$. Por otra parte, para todo $\alpha,\beta\in\mathbb{Z}[\sqrt{d}]$ tenemos

$$N(\alpha\beta)=(\alpha\beta)(\overline{\alpha\beta})=\alpha\beta\,\overline{\alpha}\,\overline{\beta}=\alpha\overline{\alpha}\,\beta\overline{\beta}=N(\alpha)N(\beta).$$

5) $\Rightarrow$) Si $N(\alpha)=1$, entonces $\alpha\overline{\alpha}=1$ y por tanto α es unidad en $\mathbb{Z}[\sqrt{d}]$. Si $N(\alpha)=-1$, entonces $\alpha(-\overline{\alpha})=1$ y por tanto α es unidad en $\mathbb{Z}[\sqrt{d}]$.
$\Leftarrow$) Si $\alpha\in\mathbb{Z}[\sqrt{d}]$ es unidad, existe $\alpha^{-1}\in\mathbb{Z}[\sqrt{d}]$ tal que $\alpha\alpha^{-1}=1$. Tomando normas, y usando que la norma es multiplicativa, $1=N(1)=N(\alpha\alpha^{-1})=N(\alpha)N(\alpha^{-1})$. Ahora bien, la norma es un número entero y por tanto $N(\alpha)$ ha de ser 1 o -1.

□

Fernando Revilla. Jefe del Departamento de Matemáticas del IES Santa Teresa de Jesús de la Comunidad de Madrid y Profesor de Métodos Matemáticos de la Universidad Alfonso X El Sabio de Villanueva de la Cañada, Madrid (Hasta el curso académico 2008-2009).
E-mail address: frej0002@ficus.pntic.mec.es