Polinomios

Primeras definiciones. En este tema $\mathbb{K}$ denota al cuerpo de los números reales $\mathbb{R}$ o al cuerpo de los números complejos $\mathbb{C}$. Un *polinomio de una variable* x *con coeficientes en* $\mathbb{K}$ es una expresión del tipo

$$P(x) = p_0 + p_1 x + \cdots + p_n x^n = \sum_{j=0}^{n} p_j x^j \qquad p_n \neq 0$$

donde $p_0, p_1, \ldots, p_n \in \mathbb{K}$. Usaremos las siguientes notaciones:

- El *término independiente* es $p_0 = P(0)$.
- El *coeficiente principal* es p_n.
- El polinomio es *mónico* cuando $p_n = 1$.
- Si no es mónico, podemos *normalizarlo*, es decir, convertirlo en mónico dividiéndolo por p_n.
- El *grado* del polinomio es n y escribiremos $\operatorname{gr}[P(x)] = n$. (El polinomio nulo no tiene grado.)
- $\mathbb{K}[x]$ denota al conjunto de polinomios con coeficientes en $\mathbb{K}$.
- $\mathbb{K}_n[x]$ denota al conjunto de polinomios con coeficientes en $\mathbb{K}$ de grado menor o igual que n.

Las operaciones básicas para trabajar con polinomios son la *suma de polinomios*, el *producto por escalar* y el *producto de polinomios*. Una manera compacta de listar las propiedades de las primeras operaciones consiste en decir que $(\mathbb{K}[x], +, \cdot)$ es un $\mathbb{K}$-ev y $\mathbb{K}_n[x]$ es un sev de dimensión $n+1$ de $\mathbb{K}[x]$. El producto de polinomios es una operación asociativa, conmutativa y posee elemento neutro (¿cuál?).

La relación de estas operaciones con el grado es la siguiente:

- $\operatorname{gr}[P(x) + Q(x)] \leq \text{máx}\big\{ \operatorname{gr}[P(x)], \operatorname{gr}[Q(x)]\big\}$.
- $\operatorname{gr}[P(x) \cdot Q(x)] = \operatorname{gr}[P(x)] + \operatorname{gr}[Q(x)]$.
- $\operatorname{gr}[\lambda \cdot P(x)] = \operatorname{gr}[P(x)]$, para todo $0 \neq \lambda \in \mathbb{K}$.

División entera de polinomios. Ya sabemos que es la división de números enteros, en la cual se obtiene un cociente y un resto. Por ejemplo, al dividir $p = 37$ entre $q = 5$ se obtiene un cociente $c = 7$ y un resto $r = 2$. Cuando el resto da cero, decimos que la división es exacta y entonces p es un múltiplo de q. Por ejemplo, $p = 35$ es un múltiplo de $q = 5$. Se puede hacer lo mismo con polinomios.

En el *Teorema de la División Entera de Polinomios* se afirma que dados dos polinomios $P(x)$ y $Q(x)$ (llamados *dividendo* y *divisor*), siendo $Q(x)$ no nulo, existen dos únicos polinomios $C(x)$ y $R(x)$ (llamados *cociente* y *resto*) tales que:

- $P(x) = Q(x) \cdot C(x) + R(x)$ y
- O bién $R(x) = \mathbf{0}$, o bién $\operatorname{gr}[R(x)] < \operatorname{gr}[Q(x)]$.

Cuando el resto de la división sea nulo (es decir, si la división es *exacta*), diremos que $Q(x)$ es un *divisor* de $P(x)$, $P(x)$ es un *múltiplo* de $Q(x)$ y escribiremos el símbolo $Q(x) \,\big|\, P(x)$.

Ejercicio. Probar que las siguientes divisiones enteras son correctas.

a) $P(x) = x^{99} + 1, Q(x) = x^{45} + 1 \Rightarrow C(x) = x^{54} - x^9, R(x) = x^9 + 1 \Rightarrow x^{45} + 1 \nmid x^{99} + 1$.
b) $P(x) = x^{45} + 1, Q(x) = x^9 + 1 \Rightarrow C(x) = x^{36} - x^{27} + x^{18} - x^9 + 1, R(x) = \mathbf{0} \Rightarrow x^9 + 1 \,\big|\, x^{45} + 1$.

Ejercicio. Sea $\lambda \in \mathbb{K}$ tal que $\lambda \neq 0$. Probar que:

- Si $Q(x)$ es un divisor de $P(x)$, el polinomio $\lambda \cdot Q(x)$ también es un divisor de $P(x)$.
- Si $P(x)$ es un múltiplo de $Q(x)$, el polinomio $\lambda \cdot P(x)$ también es un múltiplo de $Q(x)$.

Problema relacionado. 10.

MCD y MCM. Al igual que en el párrafo anterior, pensar primero en números enteros ayuda a entender las definiciones y resultados que se dan a continuación.

Dados dos polinomios $P(x)$ y $Q(x)$, su *máximo común divisor* $D(x) = \text{m.c.d.}[P(x), Q(x)]$ es el polinomio mónico del mayor grado posible que es un divisor de $P(x)$ y $Q(x)$, mientras que su *mínimo común múltiplo* $M(x) = \text{m.c.m.}[P(x), Q(x)]$ es el polinomio mónico del menor grado posible que es un múltiplo de $P(x)$ y $Q(x)$. Diremos que los polinomios $P(x)$ y $Q(x)$ son *primos entre sí* cuando $D(x)=1$. Si p_n es el coeficiente principal de $P(x)$ y q_m es el coeficiente principal de $Q(x)$, entonces

$$P(x)\cdot Q(x)=p_n\cdot q_m\cdot D(x)\cdot M(x).$$

Además, se cumple la *identidad de Bèzout*:

$$\forall P(x),Q(x)\in\mathbb{K}[x]\quad \exists P_1(x),Q_1(x)\in\mathbb{K}[x] \text{ t.q. } D(x)=P_1(x)\cdot P(x)+Q_1(x)\cdot Q(x).$$

Estos polinomios $P_1(x)$ y $Q_1(x)$ no son únicos. No vamos a probar ni la existencia y unicidad de los polinomios $D(x)$ y $M(x)$, ni la existencia de los polinomios $P_1(x)$ y $Q_1(x)$. Sin embargo, describiremos el *algoritmo de Euclides* que sirve para calcularlos. La idea fundamental del algoritmo consiste en aplicar repetidamente el resultado contenido en el siguiente ejercicio.

Ejercicio. Si $R(x)$ es el resto de $P(x)/Q(x)$, entonces m.c.d.$[P(x),Q(x)]$ = m.c.d.$[Q(x),R(x)]$.

El algoritmo de Euclides para calcular $D(x)$, $M(x)$, $P_1(x)$ y $Q_1(x)$ consta de los siguientes pasos.

1. *Cálculo del MCD.* Suponiendo que $\mathrm{gr}[P(x)]\geq \mathrm{gr}[Q(x)]$, efectuamos una cadena de divisiones que empieza por $P(x)/Q(x)$ y acaba en una división exacta. Tras realizar cualquier división no exacta de esa cadena, en la siguiente división hay que dividir el divisor anterior entre el resto anterior. El resto normalizado de la última división no exacta es $D(x)$.
2. *Cálculo del MCM.* $M(x)=\frac{P(x)\cdot Q(x)}{p_n\cdot q_m\cdot D(x)}$.
3. *Cálculo de la identidad de Bèzout.* Seguimos la cadena en orden inverso. Ver ejemplo.

Ejemplo. Dados $P(x)=x^5-32$ y $Q(x)=x^3-8$, calcular $D(x)$, $M(x)$, $P_1(x)$ y $Q_1(x)$.

1. *Cálculo del MCD.* Obtenemos la siguiente cadena de divisiones.
   - Primera: En $P(x)/Q(x)$, el cociente es $C_1(x)=x^2$ y el resto es $R_1(x)=8x^2-32$.
   - Segunda: En $Q(x)/R_1(x)$, el cociente es $C_2(x)=x/8$ y el resto es $R_2(x)=4x-8$.
   - Tercera: En $R_1(x)/R_2(x)$, el cociente es $C_3(x)=2x+4$ y el resto es $R_3(x)=\mathbf{0}$.

   Por tanto, $D(x)=R_2(x)/4=x-2$.
2. *Cálculo del MCM.* $M(x)=\frac{P(x)\cdot Q(x)}{D(x)}=(x^5-32)\cdot(x^2+2x+4)=x^7+2x^6+4x^5-32x^2-64x-128$.
3. *Cálculo de la identidad de Bèzout.* Usando las divisiones anteriores en orden inverso, queda

$$\begin{aligned} R_2(x) &= Q(x)-R_1(x)\cdot C_2(x)\\ &= Q(x)-\big(P(x)-Q(x)\cdot C_1(x)\big)\cdot C_2(x)\\ &= -C_2(x)\cdot P(x)+\big(1+C_1(x)\cdot C_2(x)\big)\cdot Q(x). \end{aligned}$$

   Si dividimos esta igualdad entre cuatro, obtenemos

$$D(x)=R_2(x)/4=P_1(x)\cdot P(x)+Q_1(x)\cdot Q(x)$$

   donde $P_1(x)=-C_2(x)/4=-x/32$ y $Q_1(x)=\big(1+C_1(x)\cdot C_2(x)\big)/4=1/4+x^3/32$.

Problemas relacionados. 5 y 7.

Raíces de un polinomio. Dado un polinomio no nulo $P(x)\in\mathbb{K}[x]$, decimos que el número $\alpha\in\mathbb{K}$ es una *raíz* de $P(x)$ cuando $P(\alpha)=0$. La raíz α tiene (o es de) *multiplicidad* k cuando

$$P(\alpha)=P'(\alpha)=\cdots=P^{(k-1)}(\alpha)=0\qquad P^{(k)}(\alpha)\neq 0.$$

Las raíces de multiplicidad uno, se denominan *simples*, las de multiplicidad dos, *dobles*, etc.

Sean $\alpha\in\mathbb{K}$ y $P(x)\in\mathbb{K}[x]$. Los siguientes resultados son básicos.

- *Teorema de Ruffini:* α es una raíz de $P(x)\iff x-\alpha\,\big|\,P(x)$.
- *Fórmula de Taylor:* Si $n=\mathrm{gr}[P(x)]$, entonces

$$P(x)=P(\alpha)+P'(\alpha)(x-\alpha)+\frac{P''(\alpha)}{2}(x-\alpha)^2+\cdots+\frac{P^{(n)}(\alpha)}{n!}(x-\alpha)^n=\sum_{j=0}^{n}\frac{P^{(j)}(\alpha)}{j!}(x-\alpha)^j.$$

  (Más aún, los polinomios $1,x-\alpha,\ldots,(x-\alpha)^n$ forman una base de $\mathbb{K}_n[x]$.)
- α es una raíz de $P(x)$ de multiplicidad $k\iff (x-\alpha)^k\,\big|\,P(x)$ & $(x-\alpha)^{k+1}\nmid P(x)$.

A partir de estos resultados, se puede deducir la siguiente propiedad. Dado un polinomio $P(x) \in \mathbb{K}[x]$, $\alpha_1, \dots, \alpha_l \in \mathbb{K}$ son raíces de multiplidades $k_1, \dots, k_l \in \mathbb{N}$ de $P(x)$ si y sólo si $\exists\, Q(x) \in \mathbb{K}[x]$ tal que

- $P(x) = (x - \alpha_1)^{k_1} \cdots (x - \alpha_l)^{k_l} \cdot Q(x)$
- $Q(\alpha_1), \dots, Q(\alpha_l) \neq 0$.

Conviene recordar dos consecuencias importantes de la última propiedad:

- Un polinomio de grado n no puede tener más de n raíces contadas con multiplicidad.
- Si dos polinomios de $\mathbb{K}_n[x]$ tienen el mismo valor en $n+1$ puntos, entonces son iguales.

La expresión *contadas con multiplicidad* significa que una raíz de multiplicidad k se cuenta k veces.

Un truco para encontrar raíces de polinomios con coeficientes enteros es que si $\alpha = \frac{n}{d} \in \mathbb{Q}$ es una raíz racional (no simplificable) de un polinomio $Q(x) = q_0 + \cdots + q_m x^m \in \mathbb{Z}[x]$, entonces $n \,\big|\, q_0$ y $d \,\big|\, q_m$.

Ejercicio. Probar la afirmación anterior.

Ejemplo. Queremos encontrar todas las raíces del polinomio $P(x) = 3x^3 - 19x^2 + 36x - 10$. Sus posibles raíces racionales son ± 1, ± 2, ± 5, ± 10, $\pm 1/3$, $\pm 2/3$, $\pm 5/3$ y $\pm 10/3$. Tras comprobarlo, tan sólo $\alpha = 1/3$ es raíz. Las otras raíces forman un pareja compleja conjugada: $z = 3 + \mathrm{i}$ y $\bar{z} = 3 - \mathrm{i}$.

Problemas relacionados. 2, 3, 4, 8, 9, 11, 12 y 14.

Polinomios irreducibles. El concepto de polinomios irreducibles es similar al concepto de números enteros primos. Un entero $p \neq 0$ es *primo* cuando los únicos enteros que lo dividen son $\pm p$ y ± 1. La definición con polinomios no puede ser tan simple, pues los polinomios de grado cero dividen a cualquier polinomio, es decir, si $\lambda \in \mathbb{K}$ es no nulo y $P(x) \in \mathbb{K}[x]$, la división $P(x)/\lambda$ siempre es exacta.

Un polinomio $P(x) \in \mathbb{K}[x]$ es *irreducible (o primo) en* $\mathbb{K}[x]$ cuando no se puede factorizar como producto de dos polinomios de $\mathbb{K}[x]$ de grado no nulo. Es decir, cuando

$$\nexists\, P_1(x), P_2(x) \in \mathbb{K}[x] \text{ t.q. } P(x) = P_1(x) \cdot P_2(x) \;\&\; \mathrm{gr}[P_1(x)], \mathrm{gr}[P_2(x)] \geq 1.$$

Las propiedades más importantes de estos polinomios son:

- Todos los polinomios de grado uno son irreducibles.
- La irreducibilidad depende del cuerpo $\mathbb{K}$. Por ejemplo, el polinomio $P(x) = x^2 + 1$ es irreducible en $\mathbb{R}[x]$, pero en $\mathbb{C}[x]$ es reducible, ya que $x^2 + 1 = (x + \mathrm{i}) \cdot (x - \mathrm{i})$.
- Cualquier polinomio se puede factorizar de forma única, salvo permutaciones de los factores, como producto de polinomios irreducibles. Es decir, $\forall\, P(x) \in \mathbb{K}[x]$:
$$\exists! P_1(x), \dots, P_l(x) \in \mathbb{K}[x] \text{ irred. en } \mathbb{K}[x] \text{ y } \exists! k_1, \dots, k_l \in \mathbb{N} \text{ t.q. } P(x) = P_1(x)^{k_1} \cdots P_l(x)^{k_l}.$$
- La factorización como producto de polinomios irreducibles se usa para calcular MCDs y MCMs:
$$\left.\begin{array}{l} P(x) = a_n \cdot R_1(x)^{k_1} \cdots R_l(x)^{k_l} \in \mathbb{K}[x] \\ Q(x) = b_m \cdot R_1(x)^{m_1} \cdots R_l(x)^{m_l} \in \mathbb{K}[x] \\ R_1(x), \dots, R_l(x) \text{ mónicos irred. en } \mathbb{K}[x] \end{array}\right\} \Rightarrow \left\{\begin{array}{l} \text{m.c.d.}[P(x), Q(x)] = R_1(x)^{i_1} \cdots R_l(x)^{i_l} \\ \text{m.c.m.}[P(x), Q(x)] = R_1(x)^{j_1} \cdots R_l(x)^{j_l} \\ i_s = \text{mín}(k_s, m_s) \text{ y } j_s = \text{máx}(k_s, m_s) \end{array}\right.$$

Ejemplo. Si $P(x) = x^3 - 3x^2 + 3x - 2 = (x^2 - x + 1)(x - 2)$ y $Q(x) = x^2 - 4x + 4 = (x - 2)^2$, entonces

$$\text{m.c.d.}[P(x), Q(x)] = x - 2 \qquad \text{m.c.m.}[P(x), Q(x)] = (x^2 - x + 1)(x - 2)^2 = x^4 - 5x^3 + 9x^2 - 8x + 4.$$

Ejercicio. Probar que dados cuatro polinomios $P(x)$, $Q_1(x)$, $Q_2(x)$ y $Q(x) = Q_1(x) \cdot Q_2(x)$, entonces:

- $\text{m.c.d.}[P(x), Q_1(x)] = 1$ y $\text{m.c.d.}[P(x), Q_2(x)] = 1 \Longrightarrow \text{m.c.d.}[P(x), Q(x)] = 1$.
- $P(x) \,\big|\, Q(x)$ y $\text{m.c.d.}[P(x), Q_1(x)] = 1 \Longrightarrow P(x) \,\big|\, Q_2(x)$.
- $\text{m.c.d.}[Q_1(x), Q_2(x)] = 1$, $Q_1(x) \,\big|\, P(x)$ y $Q_2(x) \,\big|\, P(x) \Longrightarrow Q(x) \,\big|\, P(x)$.

A continuación, listamos los polinomios irreducibles en $\mathbb{C}[x]$. En el *Teorema Fundamental del Álgebra* se establece que cualquier polinomio $P(x) \in \mathbb{C}[x]$ tiene $n = \mathrm{gr}[P(x)]$ raíces contadas con multiplicidad. Es decir, si $z_1, \dots, z_l \in \mathbb{C}$ son todas las raíces de un polinomio $P(x) \in \mathbb{C}[x]$ y sus multiplicidades son $k_1, \dots, k_l \in \mathbb{N}$, entonces $k_1 + \cdots + k_l = n = \mathrm{gr}[P(x)]$ y, por tanto,

$$P(x) = p_0 + p_1 x + \cdots + p_{n-1} x^{n-1} + p_n x^n = p_n \cdot (x - z_1)^{k_1} \cdots (x - z_l)^{k_l} = p_n \cdot \prod_{s=1}^{l} (x - z_s)^{k_s}.$$

Ejercicio. Usando esa expresión, probar que $p_{n-1} = -(k_1 z_1 + \cdots + k_l z_l) p_n$ y $p_0 = (-1)^n z_1^{k_1} \cdots z_l^{k_l} p_n$.

Todo lo anterior implica que: *"Los únicos polinomios irreducibles en* $\mathbb{C}[x]$ *son los polinomios de grado uno"*. En cambio, los polinomios irreducibles en $\mathbb{R}[x]$ son:

- Los polinomios de grado uno ($a_1 x + a_0$ con $a_1, a_0 \in \mathbb{R}$).
- Los polinomios de grado dos y *discriminante* negativo ($\alpha x^2 + \beta x + \gamma$ con $\Delta := \beta^2 - 4\alpha\gamma < 0$).

Este resultado es una consecuencia del siguiente hecho: *"Las raíces complejas de un polinomio real van siempre agrupadas en pares conjugados"*. Además, dada una raíz $z = a + b\mathrm{i} \in \mathbb{C}$ vemos que

$$(x - z)(x - \bar{z}) = x^2 - (z + \bar{z})x + z\bar{z} = x^2 - 2\operatorname{Re} z \cdot x + |z|^2 = x^2 - 2ax + a^2 + b^2 \in \mathbb{R}[x]$$

luego los factores complejos de la factorización en $\mathbb{C}[x]$ de un polinomio real se pueden agrupar en parejas que se convierten en polinomios reales de grado dos y discriminante negativo.

Ejemplo. Queremos factorizar el polinomio $P(x) = x^4 + 1$ en $\mathbb{R}[x]$. Primero lo factorizamos en $\mathbb{C}[x]$. Las raíces de $P(x)$ son las raíces cuartas de $z = -1 = \mathrm{e}^{\pi \mathrm{i}}$, a saber,

$$\begin{aligned}
z_0 &= \mathrm{e}^{\pi \mathrm{i}/4} = \cos(\pi/4) + \mathrm{i}\sin(\pi/4) = \sqrt{2}/2 + \mathrm{i}\sqrt{2}/2 \\
z_1 &= \mathrm{e}^{3\pi \mathrm{i}/4} = \cos(3\pi/4) + \mathrm{i}\sin(3\pi/4) = -\sqrt{2}/2 + \mathrm{i}\sqrt{2}/2 \\
z_2 &= \mathrm{e}^{5\pi \mathrm{i}/4} = \cos(5\pi/4) + \mathrm{i}\sin(5\pi/4) = -\sqrt{2}/2 - \mathrm{i}\sqrt{2}/2 \\
z_3 &= \mathrm{e}^{7\pi \mathrm{i}/4} = \cos(7\pi/4) + \mathrm{i}\sin(7\pi/4) = \sqrt{2}/2 - \mathrm{i}\sqrt{2}/2.
\end{aligned}$$

Por tanto, $P(x) = (x - z_0)(x - z_1)(x - z_2)(x - z_3)$. Para factorizar en $\mathbb{R}[x]$, agrupamos estas raíces en pares complejos conjugados: z_0 con $z_3 = \bar{z}_0$ y z_1 con $z_2 = \bar{z}_1$. Entonces

$$P(x) = (x - z_0)(x - \bar{z}_0)(x - z_1)(x - \bar{z}_1) = \big(x^2 - \sqrt{2}x + 1\big)\big(x^2 + \sqrt{2}x + 1\big).$$

Problemas relacionados. 1, 6 y 13.

Fracciones racionales. Una *fracción racional de una variable* x *sobre* $\mathbb{K}$ es una expresión del tipo $P(x)/Q(x)$, donde $P(x), Q(x) \in \mathbb{K}[x]$ y $Q(x) \neq 0$. Debido a que

$$P(x)/Q(x) = \tilde{P}(x)/\tilde{Q}(x) \Leftrightarrow P(x)\tilde{Q}(x) = \tilde{P}(x)Q(x)$$

cualquier fracción racional se puede escribir, simplificándola si es necesario, de forma que su numerador y su denominador sean primos entre sí.

Notamos por $\mathbb{K}(x)$ al cuerpo de las fracciones racionales sobre $\mathbb{K}$. Las *fracciones simples* de $\mathbb{K}(x)$ son aquellas fracciones de la forma $P(x)/Q(x)^k$ tales que $Q(x)$ es irreducible en $\mathbb{K}[x]$ y $\operatorname{gr}[P(x)] < \operatorname{gr}[Q(x)]$.

La *descomposición de fracciones racionales como suma de fracciones simples* consiste en lo siguiente. Si $P(x)/Q(x)$ es una fracción racional no simplificable y $Q(x) = Q_1(x)^{k_1} \cdots Q_l(x)^{k_l}$ es la factorización en polinomios irreducibles de $Q(x)$ en $\mathbb{K}[x]$, entonces existe una única descomposición del tipo

$$\frac{P(x)}{Q(x)} = C(x) + \frac{R(x)}{Q(x)} = C(x) + \sum \left(\begin{array}{c} \text{fracciones simples con denominadores} \\ \text{de la forma } Q_j(x)^m \text{ con } 1 \leq m \leq k_j \end{array} \right)$$

donde $C(x), R(x) \in \mathbb{K}[x]$ son el cociente y el resto de la división entera $P(x)/Q(x)$.

Esta descomposición se utiliza, entre otras cosas, para integrar fracciones racionales. La idea es que la integral de un fracción racional es igual a la suma de las integrales de sus fracciones simples y se sabe como calcular estas últimas integrales.

La descomposición de fracciones racionales como suma de fracciones simples depende del cuerpo $\mathbb{K}$, al igual que la factorización de polinomios como producto de polinomios irreducibles.

Ejemplo. Si $P(x) = -50x - 10$ y $Q(x) = (x-1)^2(x+2)(x^2+1)$, entonces

$$\begin{aligned}
\frac{P(x)}{Q(x)} &= \frac{-10}{(x-1)^2} + \frac{5}{x-1} + \frac{2}{x+2} + \frac{9 - 7x}{x^2+1} \ (\text{si } \mathbb{K} = \mathbb{R}) \\
&= \frac{-10}{(x-1)^2} + \frac{5}{x-1} + \frac{2}{x+2} - \frac{\frac{7}{2} - \frac{9}{2}\mathrm{i}}{x+\mathrm{i}} - \frac{\frac{7}{2} + \frac{9}{2}\mathrm{i}}{x-\mathrm{i}} \ (\text{si } \mathbb{K} = \mathbb{C}).
\end{aligned}$$

Problemas relacionados. 15 y 16.