Polinomios

Si $\mathbf{A}$ es un anillo conmutativo, como $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$ o $\mathbf{Z}_p$, los **polinomios** en $\mathbf{A}$ son expresiones de la forma

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_2 x^2 + a_1 x + a_0$$

donde los **coeficientes** $a_0, a_1, \dots, a_n$ son elementos de $\mathbf{A}$ y x es una **variable** o **indeterminada** que toma valores en $\mathbf{A}$.

Ejemplos

- $p(x) = 2x^3 + x^2 + 4x + 5$ es un polinomio en $\mathbf{Z}$ y también en $\mathbf{R}$ y en $\mathbf{C}$.
- $p(x) = x^3 + \pi x^2 + 4/3 x + 7$ es un polinomio en $\mathbf{R}$ y en $\mathbf{C}$ pero no en $\mathbf{Z}$
- $p(x) = 2x^3 + ix^2 + (4-i)x + 5 - 3i$ es un polinomio en $\mathbf{C}$.

Los polinomios en $\mathbf{Z}$, $\mathbf{R}$ o $\mathbf{C}$ son llamados respectivamente polinomios enteros, reales o complejos.

El **grado** del polinomio $p(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_2 x^2 + a_1 x + a_0$ es el exponente más grande con que aparece x , que es n si asumimos $a_n \neq 0$.

El término de grado j es el monomio $a_j x^j$, el término de grado 0 es el término independiente o constante a_0 .

Ejemplos:

- Los polinomios de grado 0 son los polinomios constantes $p(x) = a_0$,
- Los polinomios de grado 1 son los polinomios lineales $p(x) = a_1 x + a_0$,
- Los polinomios de grado 2 son los polinomios cuadráticos $p(x) = a_2 x^2 + a_1 x + a_0$,

Los polinomios en un anillo conmutativo $\mathbf{A}$ definen funciones polinomiales de $\mathbf{A}$ en $\mathbf{A}$: al asignarle a la variable x un valor a en $\mathbf{A}$, obtenemos una suma de productos de elementos de $\mathbf{A}$ (que es un elemento en $\mathbf{A}$) llamado el **valor** del polinomio en a .

Ejemplo. En $\mathbf{C}$, si $p(x) = 3x^2 + 2x - 1$ entonces $p(i) = -4 + 2i$ y $p(1/3) = 0$

Los polinomios en un anillo $\mathbf{A}$, pueden sumarse y multiplicarse:

Ejemplo. Si $p(x) = 3x + 1$ y $q(x) = 2x^2 - 4x + 5$ entonces

$$p(x) + q(x) = (3x - 2) + (x^2 - 4x + 1) = x^2 - x - 1$$

$$p(x) \cdot q(x) = (3x - 2)(x^2 - 4x + 1) = 3x^3 - 12x^2 + 3x - 2x^2 + 4x - 2 = 3x^3 - 14x^2 + 7x - 2$$

La suma y el producto de polinomios en un anillo conmutativo $\mathbf{A}$ son asociativas y conmutativas, y el producto se distribuye sobre la suma. Además cada polinomio $p(x)$ tiene un inverso aditivo $-p(x)$ y hay un neutro aditivo que es el polinomio 0 . Así que con esta suma y producto los polinomios en $\mathbf{A}$ forman un anillo conmutativo, llamado el **anillo de polinomios** en $\mathbf{A}$.

Observar que el grado de la suma $p(x)+q(x)$ es menor o igual al máximo de los grados de $p(x)$ y $q(x)$, y el grado del producto $p(x) \cdot q(x)$ es *menor o igual* que la suma de los grados de $p(x)$ y $q(x)$.

Si en el anillo A no hay divisores de 0 entonces el grado del producto es la suma de los grados, (así que en el anillo de polinomios en A tampoco hay divisores de 0).

Si $p(x)$ y $q(x)$ son polinomios sobre un anillo A , decimos que $p(x)$ **divide** a $q(x)$ si existe un polinomio $c(x)$ sobre A tal que $p(x) \cdot c(x) = q(x)$.

Ejemplos.

- $p(x) = 3x$ divide a $q(x) = x^2$ en $\mathbf{R}$, ya que $x^2 = (1/3x)(3x)$ y $c(x) = 1/3 x$ es un polinomio en $\mathbf{R}$. Pero $p(x)$ no divide a $q(x)$ en $\mathbf{Z}$ porque $c(x) = 1/3x$ no es un polinomio en $\mathbf{Z}$.
- $p(x) = x+2$ divide a $q(x) = x^2+3x+2$ en $\mathbf{R}$ ya que $(x+1)(x+2) = x^2+3x+2$, pero $p(x) = x+2$ no divide a $q(x) = x^2+2x+3$ ya que ningún polinomio en $\mathbf{R}$ multiplicado por $x+2$ da x^2+2x+3 .
- Un polinomio $q(x)$ es divisible entre x en $\mathbf{R}$ si el término constante de $q(x)$ es 0 .

Aún cuando un polinomio $p(x)$ no divide a otro polinomio $q(x)$, podemos tratar de acercarnos a *lo mas posible* a $q(x)$ con múltiplos de $p(x)$.

Ejemplos.

- ¿Que tanto nos podemos acercar a $q(x) = 2x^2+3x+4$ con múltiplos de $p(x) = x+2$?
 Multiplicando a $p(x)$ por $2x$ obtenemos un polinomio que empieza igual que $q(x)$:
 $2x(x+2) = 2x^2+4x$ que difiere de $q(x)$ en $-x+4$. Esta diferencia se parece a $-p(x)$ y podemos acercarnos mas a $q(x)$ añadiéndole a $2x$ el término constante -1 :
 $(2x-1)(x+2) = 2x^2+4x -x-2 = 2x^2+3x-2$ que difiere de $q(x)$ en 6 .
 La aproximación que obtenemos es $q(x) = (2x-1) p(x) + 6$
 y esta es la mejor aproximación de $q(x)$ por múltiplos de $p(x)$.
- ¿Cual es el múltiplo de $p(x) = x^2+2x+3$ mas cercano a $q(x) = x^4+5x^3-x^2+5$?
 $(x^2)(x^2+2x+3) = x^4+2x^3+3x^2$ que difiere de $q(x)$ en $3x^3-4x^2+5$. Esta diferencia se parece a $3xp(x)$ así que podemos acercarnos mas a $q(x)$ sumándole a x^2 el término $3x$:
 $(x^2+3x)(x^2+2x+3) = x^4+2x^3+3x^2+3x^3+6x^2+9x = x^4+5x^3+9x^2+9x$
 que difiere de $q(x)$ en $-10x^2-9x+5$. Esta diferencia se parece a $-10p(x)$ así que podemos acercarnos mas a $q(x)$ sumando a x^2+3x el término -10 :
 $(x^2+3x-10)(x^2+2x+3) = x^4+2x^3+3x^2+3x^3+6x^2+9x -10x^2-20x-30 = x^4+5x^3-x^2-11x-30$
 que difiere de $q(x)$ en $11x+35$.
 La aproximación que obtenemos es $q(x) = (x^2+3x-10) p(x) + 11x+35$
 y esta es la mejor aproximación de $q(x)$ por múltiplos de $p(x)$.

Algoritmo de la división para polinomios. Si $p(x)$ y $q(x)$ son dos polinomios en un campo y $p(x) \neq 0$ entonces existen dos *únicos* polinomios $c(x)$ y $r(x)$ tales que $q(x) = c(x)p(x) + r(x)$ donde $\text{grado } r(x) < \text{grado } p(x)$.

Los polinomios $c(x)$ y $r(x)$ son el **cociente** y el **residuo** de la división de $q(x)$ entre $p(x)$.

Demostración. La idea es aproximar a $q(x)$ con un múltiplo de $p(x)$ de modo que la diferencia entre el múltiplo y $q(x)$ sea un polinomio del menor grado posible. El polinomio por el que hay que multiplicar a $p(x)$ será el cociente $q(x)$ y lo que le falte al múltiplo para ser $q(x)$ será el residuo $r(x)$.

Si $\text{grado } q(x) < \text{grado } p(x)$ ya acabamos, porque $q(x) = 0 \cdot p(x) + q(x)$ cumple 1 y 2, así que podemos suponer que $\text{grado } p(x) \leq \text{grado } q(x)$.

Vamos a hallar múltiplos de $p(x)$ que se aproximen cada vez mejor a $q(x)$.

$$\begin{aligned} \text{Si } p(x) &= a_m x^m + a_{m-1} x^{m-1} + \dots + a_2 x^2 + a_1 x + a_0 \\ q(x) &= b_n x^n + b_{n-1} x^{n-1} + \dots + b_2 x^2 + b_1 x + b_0 \end{aligned}$$

Podemos acercarnos a $q(x)$ multiplicando a $p(x)$ por $m(x) = b_n/a_m x^{n-m}$.

La diferencia $d_1(x) = q(x) - m_1(x)p(x)$ tiene grado menor que n .

$$q(x) = m_1(x)p(x) + d_1(x) \text{ donde } d_1(x) \text{ es un polinomio de grado a lo mas } n-1.$$

Si $d_1(x)$ tiene grado menor que m ya acabamos.

Si $d_1(x)$ tiene grado mayor o igual a m podemos aproximarnos a $d_1(x)$ con un múltiplo $m_2(x)p(x)$

de modo que la diferencia $d_2(x) = d_1(x) - m_2(x)p(x)$ tenga grado menor o igual a $n-2$.

$$q(x) = m(x)p(x) + d_1(x) = m(x)p(x) + m_1(x)p(x) + d_2(x)$$

donde $d_2(x)$ es un polinomio de grado menor o igual a $n-2$.

Si $d_2(x)$ tiene grado menor que m ya acabamos.

Si $d_2(x)$ tiene grado mayor o igual a m podemos aproximarnos a $d_2(x)$ con un múltiplo $m_3(x)p(x)$

de modo que la diferencia $d_2(x) = d_1(x) - m_2(x)p(x)$ tenga grado menor o igual a $n-2$.

$$q(x) = m(x)p(x) + m_1(x)p(x) + d_2(x) = m(x)p(x) + m_1(x)p(x) + m_2(x)p(x) + d_3(x)$$

donde $d_3(x)$ es un polinomio de grado menor o igual a $n-3$.

Si $d_3(x)$ tiene grado menor que m ya acabamos.

Repetimos esto hasta que la diferencia $q_k(x)$ tenga grado menor que m (esto ocurre en a lo mas $n-m$ pasos)

$$\text{y entonces ya acabamos, porque } q(x) = m_1(x)p(x) + m_2(x)p(x) + \dots + m_k(x)p(x) + q_k(x)$$

Así que $q(x)$ es la suma de un múltiplo de $p(x)$ y el polinomio $q_k(x)$ de grado menor que m .

Falta ver que solo hay una forma de escribir $q(x) = c(x)p(x) + r(x)$ con grado de $r(x) < \text{grado de } p(x)$.

Supongamos que hubiera otra forma, $q(x) = c'(x)p(x) + r'(x)$.

$$\text{Entonces } c(x)p(x) + r(x) = c'(x)p(x) + r'(x) \text{ y por lo tanto } r(x) - r'(x) = c'(x)p(x) - c(x)p(x)$$

y esto muestra que $r(x) - r'(x)$ es un múltiplo de $p(x)$.

Pero $\text{grado } r(x) - r'(x) < \text{grado } p(x)$, y el único múltiplo de $p(x)$ de grado menor que $p(x)$ es el polinomio 0.

Por lo tanto $r(x) - r'(x) = 0$ así que $r(x) = r'(x)$. Pero $c'(x)p(x) - c(x)p(x) = r(x) - r'(x) = 0$, por lo tanto

$$[c'(x) - c(x)] p(x) = 0 \text{ y como } p(x) \neq 0 \text{ entonces } c'(x) - c(x) = 0, \text{ así que } c'(x) = c(x). \quad \bullet$$

El algoritmo de la división dice que podemos dividir a los polinomios sobre un campo igual que dividimos enteros:

Ejemplo. Dividir $q(x) = 2x^2 - 3x + 1$ entre $p(x) = x - 2$

$$\begin{array}{r} 2x+1 \\ x-2 \overline{) 2x^2-3x+1} \\ \underline{2x^2-4x} \\ x+1 \\ \underline{x-2} \\ 3 \end{array}$$

$$\text{así que } 2x^2 - 3x + 1 = \underbrace{(2x+1)}_{\text{cociente}} \underbrace{(x-2)}_{\text{residuo}} + 3$$

Ejemplo. ¿Cual es el múltiplo de $p(x) = x^2 - 2x + 3$ mas cercano a $q(x) = x^5 + 3x^4 - 5x^3 - 6x + 7$?

$$\begin{array}{r} x^3+5x^2+12x+9 \\ x^2-2x+3 \overline{) x^5+3x^4-5x^3+0x^2-6x+7} \\ \underline{x^5-2x^4+3x^3} \\ 5x^4+2x^3+0x^2 \\ \underline{5x^4-10x^3+15x^2} \\ 12x^3-15x^2-6x \\ \underline{12x^3-24x^2+36x} \\ 9x^2-42x+7 \\ \underline{9x^2-18x+27} \\ -24x-20 \end{array}$$

$$\text{Así que } x^5 + 3x^4 - 5x^3 + 0x^2 - 6x + 7 = \underbrace{(x^3 + 5x^2 + 12x + 9)}_{\text{cociente}} \underbrace{(x^2 - 2x + 3)}_{\text{residuo}} - 24x - 20$$

Ejemplo. Dividir a $q(x) = x^4 + 5x^3 + 3x + 2$ entre $p(x) = 2x^2 + 3$

$$\begin{array}{r} \frac{1}{2}x^2 + \frac{5}{2}x - \frac{3}{4} \\ 2x^2+3 \overline{) x^4 + 5x^3 + 0x^2 + 3x + 2} \\ \underline{x^4 + 0x^3 + \frac{3}{2}x^2} \\ 5x^3 - \frac{3}{2}x^2 + 3x \\ \underline{5x^3 + 0x^2 + \frac{15}{2}x} \\ -\frac{3}{2}x^2 - \frac{9}{2}x + 2 \\ \underline{\frac{3}{2}x^2 + 0x - \frac{9}{4}} \\ -\frac{9}{2}x + \frac{13}{4} \end{array}$$

$$\text{Así que } x^4 + 5x^3 + 3x + 2 = \left(\frac{1}{2}x^2 + \frac{5}{2}x - \frac{3}{4}\right) (2x^2 + 3) - \frac{9}{2}x + \frac{13}{4}$$

El algoritmo de la división solo vale para polinomios sobre un campo, no sobre cualquier anillo.

Ejemplo. En el anillo $\mathbf{Z}$, si $p(x) = 2x$ y $q(x) = x^2$ entonces no hay múltiplos de $p(x)$ que se acerquen a $q(x)$ de modo que la diferencia entre el múltiplo de $p(x)$ y $q(x)$ tenga grado menor que 2.

Problemas.

1. Calcula explícitamente

a. $(x+1)(x+2)(x+3)$

b. $(x^2+2x+4)(5x^2-3x+1)$

c. $(x+i)^3$ ojo: dice i

2. a. Muestra que $x^4+x^3+x^2+x+1$ divide a x^5-1 .

b. Muestra que x^2+x+1 divide a x^4+x^2+1 .

3. Calcula el cociente y el residuo de dividir $q(x)$ entre $p(x)$

a. $p(x) = 2x+1$

$q(x) = x^2+x+1$

b. $p(x) = x+2$

$q(x) = x^3+2x^2-3x+4$

c. $p(x) = x^3+1$

$q(x) = x^2+3$

d. $p(x) = ix^2-x+3$

$q(x) = x^4+x^2+i$

e. $p(x) = x^2-x+1$

$q(x) = x^5$

El máximo común divisor.

Observar que si un polinomio $m(x)$ en un anillo A divide a dos polinomios $p(x)$ y $q(x)$, entonces divide a todas las combinaciones $a(x)p(x)+b(x)q(x)$ donde $a(x)$ y $b(x)$ son polinomios en A .

Lema. Si $p(x)$ y $q(x)$ son dos polinomios en un campo, entonces existe una combinación $a(x)p(x)+b(x)q(x)$ que divide a $p(x)$ y $q(x)$.

Demostración. De entre todas las combinaciones $a(x)p(x)+b(x)q(x)$ distintas de 0, tomemos una combinación $m(x)$ de grado mínimo. Entonces $m(x)$ debe dividir a $p(x)$, porque si no el algoritmo de la división daría polinomios $c(x)$ y $r(x)$ tales que $p(x)=c(x)m(x)+r(x)$ con $\text{grado } r(x) < \text{grado } m(x)$ y $r(x) \neq 0$. Pero $r(x)=p(x)-c(x)m(x)$ es una combinación de $p(x)$ y $q(x)$ (porque $m(x)$ y $p(x)$ lo son), lo que contradice que $m(x)$ es un polinomio de grado mínimo que es combinación de $p(x)$ y $q(x)$. •

Corolario. Si $p(x)$ y $q(x)$ son dos polinomios en un campo, entonces existe un polinomio $m(x)$ que divide a ambos y que es divisible entre todos los polinomios que dividen a $p(x)$ y $q(x)$.

Demostración. Si $s(x)$ es un polinomio que divide a $p(x)$ y $q(x)$ entonces $s(x)$ divide a todas las combinaciones $a(x)p(x)+b(x)q(x)$, en particular a la combinación distinta de 0 de grado mínimo, que por el lema anterior divide a $p(x)$ y también a $q(x)$. •

El polinomio $m(x)$ del corolario anterior es un *máximo común divisor (mcd)* de $p(x)$ y $q(x)$. El mcd de dos polinomios está bien definido salvo multiplicación por constantes. Podemos obtener el mcd de dos polinomios $p(x)$ y $q(x)$ usando repetidamente el algoritmo de la división, igual que lo hicimos para enteros.

Ejemplo. Si $p(x)=x^3+5x^2-12x+9$ y $q(x)=x^2-2x+3$

$$\begin{aligned} \text{entonces } x^3+5x^2-12x+9 &= (x+7)(x^2-2x+3) - x-12 \\ x^2-2x+3 &= (-x+10)(-x-12) + 123 \end{aligned}$$

así que el mcd es un polinomio constante.

$$\begin{aligned} 123 &= x^2-2x+3 - (-x+10)(-x-12) = x^2-2x+3 - (-x+10)[(x^3+5x^2-12x+9)-(x+7)(x^2-2x+3)] = \\ &= [1+(-x+10)(x+7)](x^2-2x+3) - (-x+10)(x^3+5x^2-12x+9) \\ &= (-x^2+3x+71)(x^2-2x+3) + (x-10)(x^3+5x^2-12x+9) \end{aligned}$$

Problemas.

4. Muestra que todos los polinomios de grado máximo que dividen a $p(x)$ y $q(x)$ difieren por un factor constante.

5. Encuentra un polinomio no constante que divida a $p(x)$ y $q(x)$

a. $p(x) = 6x^2-x-2$

b. $p(x) = x^3+6x^2+11x+12$

$q(x) = 3x^2-11x+6$

$q(x) = x^4+3x^3+4x^2+x-3$

6. Para los polinomios dados, encuentra polinomios $a(x)$ y $b(x)$ tales que $a(x)p(x)+b(x)q(x)=1$.

a. $p(x) = x^2-2x+3$

b. $p(x) = x^3+2x^2+3x+4$

$q(x) = x^2+3x+1$

$q(x) = 3x^4+2x^2+1$

Polinomios irreducibles.

Decimos que un polinomio no constante $p(x)$ en un campo K es **reducible** si es el producto de dos polinomios de grado menor en K . Decimos que $p(x)$ es **irreducible** si no es reducible, es decir, si no es el producto de dos polinomios de grado menor en K .

Ejemplos

- El polinomio x^2-2 es reducible sobre $\mathbf{R}$, ya que $x^2-2 = (x+\sqrt{2})(x-\sqrt{2})$. Pero x^2-2 es irreducible sobre $\mathbf{Q}$ porque si fuera reducible sería el producto de dos polinomios de grado 1: $x^2-2=(x+a)(x-b)=x^2+(a+b)x+ab$ de modo que $a+b=0$ y $ab=2$ de donde $b=-a$ y $a^2=2$ así que $a=\pm\sqrt{2}$, pero $\sqrt{2}$ no está en $\mathbf{Q}$ así que los factores no son polinomios en $\mathbf{Q}$.
- El polinomio x^2+1 es irreducible sobre $\mathbf{R}$ (no es el producto de dos polinomios reales de grado 1) pero es reducible sobre $\mathbf{C}$, ya que $x^2+1 = (x+i)(x-i)$.
- El polinomio x^4+1 es reducible sobre $\mathbf{R}$ ya que puede descomponerse como producto de 2 polinomios reales de grado 2 (tarea).

Lema. Si un polinomio irreducible en un campo K divide al producto de dos polinomios, entonces divide a uno de ellos.

Demostración. Supongamos que el polinomio $s(x)$ es irreducible en K y que $s(x)$ divide a $p(x)q(x)$ pero $s(x)$ no divide a $p(x)$. Entonces el máximo común divisor de $s(x)$ y $p(x)$ debe ser una constante, ya que como $s(x)$ es irreducible, la otra posibilidad es que el mcd fuera un múltiplo de $s(x)$, pero entonces $s(x)$ dividiría a $p(x)$. Así podemos suponer que el mcm de $s(x)$ y $p(x)$ es 1. Por un lema anterior existen polinomios $a(x)$ y $b(x)$ tales que $a(x)s(x)+b(x)p(x)=1$ y multiplicando por $q(x)$ obtenemos $a(x)s(x)q(x)+b(x)p(x)q(x)=q(x)$. Como $q(x)$ es una combinación de $s(x)$ y $p(x)q(x)$ y estos dos polinomios son divisibles entre $s(x)$ entonces $q(x)$ es divisible entre $s(x)$. •

Teorema. Cada polinomio sobre un campo K es producto de polinomios irreducibles sobre K y la factorización es única salvo productos por constantes.

Demostración. Veamos primero que la factorización siempre existe. Si $p(x)$ es un polinomio irreducible ya acabamos. Si no, es el producto de dos polinomios de grado menor. Nos fijamos en cada uno de ellos, si son irreducibles ya acabamos, si no alguno (o ambos) son producto de polinomios de grado aun menor, y nos fijamos en cada uno de ellos. Si el grado de $p(x)$ es n , este proceso de descomposición en productos debe acabar en a lo mas n pasos, ya que la suma de los grados de todos los factores es n y los polinomios de grado 1 son irreducibles.

Para ver que la factorización es única, supongamos que tenemos dos factorizaciones de $p(x)$ como producto de polinomios irreducibles:

$$p(x) = p_1(x)p_2(x)\dots p_m(x) = q_1(x)q_2(x) \dots q_n(x) \quad \text{donde } p_i(x) \text{ y } q_j(x) \text{ son irreducibles}$$

Como $p_1(x)$ es irreducible y divide al producto $q_1(x)q_2(x)\dots q_n(x)$, entonces por el lema anterior $p_1(x)$ debe dividir a alguno de los $q_i(x)$, que podemos suponer (reordenando los factores) que es $q_1(x)$. Como $q_1(x)$ es irreducible, sus únicos divisores son los polinomios constantes y los productos de $q_1(x)$ por constantes. Así que $q_1(x)=c_1p_1(x)$, y podemos dividir $p(x)$ entre $p_1(x)$ y obtener

$$p(x)/p_1(x) = p_2(x)\dots p_m(x) = c_1q_2(x) \dots q_n(x)$$

Ahora podemos repetir el argumento con $p_2(x)$ para ver que $p_2(x)=c_2q_2(x)$, dividir entre $p_2(x)$, y luego repetir el argumento con $p_3(x)$ y seguir dividiendo hasta que no quede ningún $p_j(x)$ (o no quede ningún $q_j(x)$, y en ese momento solo pueden quedar constantes, lo que dice que cada $p_i(x)$ es igual a un $q_j(x)$, multiplicado por una constante. •

Problemas.

7. Demuestra que x^2+x-1 es irreducible sobre $\mathbf{Q}$ y que x^2+x+1 es irreducible sobre $\mathbf{R}$.

8. Factoriza a los siguientes polinomios como producto de polinomios irreducibles sobre $\mathbf{R}$

a. x^2-1 b. x^3-1 c. x^3+1 d. x^4-1 e. x^2+3x-2 f. x^2+3x+4

9. Factoriza los polinomios anteriores como producto de polinomios irreducibles sobre $\mathbf{C}$.

10. Muestra directamente que x^4+1 es reducible sobre $\mathbf{R}$. Hint: ve que puede factorizarse como $(x^2+ax+1)(x^2-ax+1)$ para algún real a .

Raíces

Una **raíz** del polinomio $p(x)$ sobre un campo K es un elemento a de K tal que $p(a)=0$.

Ejemplos.

- Si $p(x)=x^3-3x^2+2$ 1 es una raíz de $p(x)$ ya que $p(1)=(1)^3-3(1)^2+2=0$
2 no es raíz de $p(x)$ ya que $p(2)=(2)^3-3(2)^2+2=-2$
- $p(x)=x^2-2$ no tiene raíces en $\mathbf{Q}$, pero tiene 2 raíces en $\mathbf{R}$, que son $\sqrt{2}$ y $-\sqrt{2}$.
- $p(x)=x^2+1$ no tiene raíces en $\mathbf{R}$, pero tiene 2 raíces en $\mathbf{C}$, que son i y $-i$.

Lema. Si $p(x)$ es un polinomio sobre un campo, el residuo al dividir $p(x)$ entre $x-a$ es $p(a)$.

Demostración. Por el algoritmo de la división, $p(x)=q(x)(x-a)+r(x)$ donde $\text{grado } r(x) < \text{grado } (x-a)=1$ así que $r(x)$ es una constante. Evaluando en a obtenemos $p(a)=q(a)(a-a)+r(a)=0+r(a)$. •

Corolario. Si $p(x)$ es un polinomio sobre un campo entonces a es raíz de $p(x)$ si y solo si $x-a$ divide a $p(x)$.

Demostración. El residuo al dividir $p(x)$ entre $x-a$ es $p(a)$, así que a es una raíz de $p(x)$ si y solo si el residuo es 0. •

Ejemplo. Si $p(x)=x^4-3x^3+5x^2-7x+2$ entonces $p(2)=0$ por lo tanto $x-2$ divide a $p(x)$, lo que podemos comprobar directamente

$$\begin{array}{r} x^3-x^2+3x-1 \\ x-2 \overline{) x^4-3x^3+5x^2-7x+2} \\ \underline{x^4-2x^3} \\ -x^3+5x^2 \\ \underline{-x^3+2x^2} \\ 3x^2-7x \\ \underline{3x^2-6x} \\ -x+2 \\ \underline{-x+2} \\ 0 \end{array} \qquad x^4-3x^3+5x^2-7x+2 = (x-2)(x^3-x^2+3x-1)$$

Teorema. Cada polinomio de grado n en un campo K tiene a lo mas n raíces en K .

Demostración. Por inducción sobre el grado de $p(x)$.

Si $p(x)$ tiene grado 1 entonces $p(x)=x-a_1$ y la única raíz es a_1 .

Supongamos ahora que la afirmación es cierta para todos los polinomios de grado menor que n y tomemos un polinomio $p(x)$ de grado n .

Si a_1 es raíz de $p(x)$ entonces $p(x)=(x-a_1)p_1(x)$ donde $p_1(x)$ es un polinomio de grado $n-1$.

Como $p(x)=(x-a_1)p_1(x)$ las raíces de $p(x)$ son a_1 y las raíces de $p_1(x)$

Pero por hipótesis de inducción $p_1(x)$ tiene a lo mas $n-1$ raíces, así que $p(x)$ tiene a lo mas n raíces. •

El teorema anterior dice que cada polinomio $p(x)$ sobre un campo K se puede factorizar como

$$p(x) = (x-a_1)(x-a_2) \dots (x-a_k) p'(x)$$

donde las a_i 's son raíces del polinomio en K y $p'(x)$ es un polinomio que no tiene raíces en K .

Los factores $x-a_i$ pueden estar repetidos, el número de veces que se repite un $x-a_i$ es la **multiplicidad** de la raíz a_i .

Ejemplos.

- $x^2+x-6 = (x-2)(x+3)$ en $\mathbf{Q}$. Las raíces en $\mathbf{Q}$ (y en $\mathbf{R}$ y en $\mathbf{C}$) son 2 y -3, cada una con multiplicidad 1.
- $x^4-2x^2 = x^2(x^2-2)$ en $\mathbf{Q}$. La única raíz en $\mathbf{Q}$ es 0, con multiplicidad 2.
 $x^4-2x^2 = x^2(x-\sqrt{2})(x+\sqrt{2})$ en $\mathbf{R}$. Las raíces en $\mathbf{R}$ son 0 (multiplicidad 2), $\sqrt{2}$ y $-\sqrt{2}$ (multiplicidad 1).
- $x^3+x = x(x^2+1)$ en $\mathbf{R}$. La única raíz del polinomio en $\mathbf{R}$ es 0, con multiplicidad 1.
 $x^3+x = x(x+i)(x-i)$ en $\mathbf{C}$. Las raíces del polinomio en $\mathbf{C}$ son 0, i y $-i$ todas con multiplicidad 1.

Encontrar las raíces de un polinomio en un campo puede ser muy difícil, aun saber si las raíces existen puede ser complicado.

Ejemplo. ¿Cuales serán las raíces de x^3+2x^2+3x+4 en $\mathbf{Q}$? ¿en $\mathbf{R}$? ¿en $\mathbf{C}$?

¿Pueden decir al menos si hay raíces o no?

Lema. Si un polinomio en $\mathbf{R}$ toma valores positivos y negativos entonces tiene una raíz real.

Idea de la demostración. Cada polinomio real $p(x)$ define una función continua de $\mathbf{R}$ en $\mathbf{R}$ que a cada real x le asigna el valor $p(x)$. Si existen dos números reales a y b tales que $p(a) < 0$ y $p(b) > 0$, entonces como el valor de $p(x)$ varía continuamente al variar x , debe haber un número real c entre a y b tal que $p(c) = 0$, esto dice que c es una raíz de $p(x)$. •

Corolario. Todo polinomio real de grado impar tiene al menos una raíz real.

Demostación. Si $p(x)$ tiene grado impar, entonces $p(x)$ toma valores positivos y negativos, así que por el lema anterior $p(x)$ tiene una raíz. •

Ejemplos.

- $p(x) = x^5+2x^4+3x^3+4x^2+5x+6$ debe tener raíces reales, como $p(-1)=3$ y $p(-2)=-12$ entonces $p(x)$ debe tener una raíz entre -2 y -1.
- $p(x) = x^4+2x^3+3x^2+4x+5$ no tiene raíces reales pero $q(x) = x^4+2x^3+3x^2+4x+1$ si las tiene, porque $q(0)=1$ y $q(-1)=-1$.

Algunos polinomios reales tienen raíces reales y otros no, pero algunos de los que no tienen raíces reales si tienen raíces complejas. ¿Será que todos los polinomios reales tienen raíces complejas?

Esta es una pregunta que los matemáticos se hicieron durante dos siglos, hasta que pudieron probar el siguiente teorema:

El Teorema Fundamental del Algebra. Cada polinomio no constante en $\mathbf{C}$ tiene al menos una raíz en $\mathbf{C}$.

Un caso particular es:

Corolario. Cada polinomio no constante en $\mathbf{R}$ tiene al menos una raíz en $\mathbf{C}$.

De hecho, el resultado para polinomios en $\mathbf{C}$ es equivalente al resultado para polinomios en $\mathbf{R}$:

Al multiplicar un polinomio complejo $p(z)$ por su polinomio conjugado $\overline{p}(z)$ queda un polinomio real. Las raíces del producto $p(z)\overline{p}(z)$ son las raíces de $p(z)$ y las de $\overline{p}(z)$, pero las raíces de $\overline{p}(z)$ son las conjugadas de las raíces de $p(z)$, así que si $p(z)\overline{p}(z)$ tiene raíces en $\mathbf{C}$ entonces $p(z)$ también tiene raíces en $\mathbf{C}$.

La demostración del teorema fundamental es muy avanzada para el curso. No hay pruebas puramente algebraicas porque hace falta usar propiedades de los números reales que no son algebraicas, y las pruebas simples requieren análisis complejo o topología.

Vamos a dar el teorema fundamental por cierto y veremos que se obtiene a partir de ahí.

Corolario. Cada polinomio no constante sobre $\mathbf{C}$ es un producto de polinomios de grado 1.

Demostración. Si $p(x)$ es un polinomio no constante sobre $\mathbf{C}$, entonces por el teorema fundamental $p(x)$ tiene una raíz compleja c_1 , así que puede factorizarse como $p(x)=(x-c_1)p_1(x)$ donde $p_1(x)$ es un polinomio de grado menor sobre $\mathbf{C}$.

Si $p_1(x)$ no es constante entonces tiene una raíz c_2 y podemos factorizar $p_1(x)=(x-c_2)p_2(x)$ donde $p_2(x)$ es un polinomio de grado aún menor sobre $\mathbf{C}$. Podemos repetir esto hasta llegar a un polinomio $p_n(x)$ de grado 0, es decir una constante k . Entonces $p(x) = (x-c_1)(x-c_2)\dots(x-c_n)k$. •

El corolario anterior dice que todos los polinomios irreducibles sobre $\mathbf{C}$ tienen grado 1.

Corolario. Cada polinomio de grado n sobre $\mathbf{C}$ tiene exactamente n raíces en $\mathbf{C}$, contando sus multiplicidades.

Demostración. La prueba del corolario anterior muestra que $p(x)=(x-c_1)(x-c_2)\dots(x-c_n)k$ donde los c_{i_i} 's son raíces de $p(x)$ posiblemente repetidas. El número de factores es el grado del polinomio. •

Como los polinomios reales son también polinomios complejos, el teorema fundamental implica que cada polinomio no constante en $\mathbf{R}$ tiene al menos una raíz en $\mathbf{C}$.

Las raíces complejas (y que no son reales) de polinomios en $\mathbf{R}$ vienen en pares:

Lema. Si $p(z)$ es un polinomio con coeficientes reales y c es una raíz compleja de $p(z)$, entonces $\overline{c}$ también es una raíz de $p(z)$.

Demostración. Supongamos que $p(z) = a_n z^n + a_{n-1} z^{n-1} + \dots + a_2 z^2 + a_1 z + a_0$ donde los a_i 's son reales.

Si c es una raíz $p(c) = a_n c^n + a_{n-1} c^{n-1} + \dots + a_2 c^2 + a_1 c + a_0 = 0$ entonces

$p(\overline{c}) = a_n \overline{c}^n + \dots + a_2 \overline{c}^2 + a_1 \overline{c} + a_0 = \overline{a_n c^n + \dots + a_2 c^2 + a_1 c + a_0} = \overline{0} = 0$ así que $\overline{c}$ también es una raíz de $p(z)$. •

Algunos polinomios de grado 2 son irreducibles en $\mathbf{R}$ (por ejemplo x^2-x+1) y podemos preguntarnos si existirán polinomios de grado mayor a 2 que sean irreducibles en $\mathbf{R}$.

Corolario. Los polinomios irreducibles en $\mathbf{R}$ tienen grado 1 o 2.

Demostración. Sea $p(x)$ un polinomio real de grado mayor que 2.

Si $p(x)$ tiene alguna raíz real a entonces $x-a$ divide a $p(x)$ por lo tanto $p(x)$ es reducible.

Si $p(x)$ no tiene raíces reales entonces debe tener alguna raíz compleja c y por el lema anterior $\bar{c}$ también es raíz de $p(x)$. Así que $x-c$ y $x-\bar{c}$ dividen a $p(x)$ y por lo tanto $(x-c)(x-\bar{c})$ divide a $p(x)$.

Como $(x-\bar{c})(x-\bar{c}) = x^2+(z+\bar{c})x+z\bar{c}$ y los números $c+\bar{c}$ y $c\bar{c}$ son reales, este es un polinomio real de grado 2 que divide a $p(x)$, que tiene grado al menos 3, así que $p(x)$ es reducible. •

Ejemplo. Escribir a x^4+4 como producto de polinomios irreducibles en $\mathbf{R}$, y como producto de polinomios irreducibles en $\mathbf{C}$.

Las raíces complejas de x^4+4 son las raíces cuartas de -4 , que son $1+i$, $1-i$, $-1+i$ y $-1-i$ así que el polinomio se factoriza sobre $\mathbf{C}$ como $x^4+4 = (x-1-i)(x-1+i)(x+1-i)(x+1+i)$.

Para factorizar a x^4+4 sobre $\mathbf{R}$ apareamos las raíces conjugadas

$$(x-1-i)(x-1+i) = (x^2-2x+2) \text{ y } (x+1-i)(x+1+i) = (x^2+2x+2)$$

así que $x^4+4 = (x^2-2x+2)(x^2+2x+2)$ sobre $\mathbf{R}$.

Todos los polinomios en $\mathbf{C}$ tienen raíces complejas y que al menos los polinomios de grado impar en $\mathbf{R}$ tienen raíces reales. Veremos que la mayoría de los polinomios en $\mathbf{Q}$ no tienen raíces racionales.

Aunque puede ser muy difícil hallar las raíces reales o complejas de los polinomios en $\mathbf{R}$ o $\mathbf{C}$, hallar las raíces racionales de un polinomio sobre $\mathbf{Q}$ es fácil, en caso que las haya.

Observar que dado un polinomio con coeficientes racionales, existe otro polinomio con coeficientes enteros que tiene las mismas raíces, ya que podemos multiplicar al polinomio por el mínimo común múltiplo de los denominadores de sus coeficientes y las raíces no cambian.

Ejemplo. El polinomio racional $p(x) = \frac{1}{2}x^3 + \frac{4}{3}x^2 + \frac{5}{6}x - \frac{1}{4}$.

tiene las mismas raíces que el polinomio entero $p'(x) = 6x^3 + 16x^2 + 10x - 3$.

Lema. Si $p(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_2 x^2 + a_1 x + a_0$ es un polinomio con coeficientes enteros, y r/s es una raíz racional de $p(x)$ escrita en forma reducida, entonces $r|a_0$ y $s|a_n$.

Demostración. Si r/s es raíz de $p(x)$ entonces $a_n (r/s)^n + a_{n-1} (r/s)^{n-1} + \dots + a_2 (r/s)^2 + a_1 (r/s) + a_0 = 0$

Multiplicando por s^n obtenemos $a_n r^n + a_{n-1} r^{n-1} s + \dots + a_2 r^2 s^{n-2} + a_1 r s^{n-1} + a_0 s^n = 0$.

Como esta combinación vale 0 y todos sus términos salvo quizás el último son múltiplos de r , el último también debe ser múltiplo de r . Así que $r|a_0 s^n$ y como r y s son primos relativos entonces $r|a_0$.

Como la combinación vale 0 y todos sus términos salvo quizás el primero son múltiplos de s , el primero también debe ser múltiplo de s . Así que $s|a_n r^n$ y como r y s son primos relativos entonces $s|a_n$. •

Ejemplos.

- ¿Cuales son las raíces racionales de $p(x) = 3x^3 + 2x^2 + 5x - 2$?

Como $a_3=3$ y $a_0=-2$, las raíces racionales deben ser de la forma m/n donde $m|-2$ y $n|3$. Las posibilidades son $\pm 2/1, \pm 2/3, \pm 1/3$ y podemos probarlas todas

$$p(2)=40 \quad p(-2)=-28 \quad p(1/3)=0 \quad p(-1/3)=-34/9 \quad p(2/3)=28/9 \quad p(-2/3)=-16/3$$

y la única raíz racional es $1/3$.

- ¿Cuales son las raíces racionales de $p(x) = x^4 + 3x^3 - 15x^2 - 15x + 50$?

Son de la forma m/n donde $n|50$ y $n|1$. Así que solo pueden ser $\pm 1, \pm 2, \pm 5, \pm 10, \pm 25, \pm 50$. Como son muchas podemos empezar por probar las mas fáciles: $p(1)=24, p(-1)=22, p(2)=0$ así que 2 es raíz, y podemos dividir a $p(x)$ entre $x-2$ y obtener $q(x)=x^3+5x^2-5x-25$.

Las raíces racionales de $q(x)$ solo pueden ser $\pm 1, \pm 5, \pm 25$, pero ya sabemos que 1 y -1 no lo son. $q(5)=150, q(-5)=0$ así que -5 es raíz y podemos dividir $q(x)$ entre $x+5$ y obtener $r(x)=x^2-5$, cuyas raíces son $\sqrt{5}$ y $-\sqrt{5}$ que no son racionales.

Concluimos que las raíces racionales de $p(x)=x^4+3x^3-15x^2-15x+50$ son 2 y -5 .

Problemas.

11. Demuestra que si $p(x)$ es un polinomio sobre un campo y a es cualquier elemento del campo, entonces $x-a$ divide a $p(x)-p(a)$.

12. Muestra que si $p(x) = x^n + a_{n-1}x^{n-1} + \dots + a_2x^2 + a_1x^1 + a_0$ es un polinomio real o complejo, entonces el producto de todas sus raíces complejas (contando multiplicidades) es $\pm a_0$ y la suma de todas sus raíces (con multiplicidades) es $-a_{n-1}$.

13. Muestra que si $p(x) = x^n + a_{n-1}x^{n-1} + \dots + a_2x^2 + a_1x^1 + a_0$ tiene coeficientes enteros, entonces las raíces *racionales* de $p(x)$ son enteras.

14. Da un polinomio *real* que tenga entre sus raíces a i y $1+i$.

15. ¿Existen polinomios de grado 5 sobre $\mathbf{R}$ que tengan (contando multiplicidades) una raíz real? ¿Dos raíces reales? ¿Tres raíces reales? ¿Cuatro raíces reales? ¿Cinco raíces reales?

16. Encuentra todas las raíces *racionales* de los siguientes polinomios:

a. $3x^2 + 11x - 4$

b. $4x^3 + x^2 + 5x - 6$

c. $7x^3 + 3x^2 - 14x - 6$

d. $5x^3 - 4x^2 + 3x - 2$

e. $4x^4 - 5x^2 + 1$

f. $x^5 + x^4 + x^3 + x^2 + x + 1$

17. ¿Existe un polinomio de grado 3 en $\mathbf{Q}$ que tenga 3 raíces reales y ninguna sea racional?

18. Muestra que el polinomio $x^4 + 1$ es irreducible en $\mathbf{Q}$ (ojo: que no tenga raíces racionales no implica que sea irreducible en $\mathbf{Q}$)

19. Si $p(x)$ y $q(x)$ son dos polinomio reales, encuentra polinomios reales $u(x)$ y $i(x)$ tales que

a. Las raíces de $u(x)$ sean las raíces de $p(x)$ y las raíces de $q(x)$.

b. Las raíces de $i(x)$ sean las raíces *comunes* de $p(x)$ y $q(x)$.

Hint $u(x)$ y $i(x)$ pueden obtenerse combinado de una manera apropiada a $p(x)$ y $q(x)$.