Introducció als polinomis

Definicions bàsiques

Definició

Un polinomi és una expressió algebraica consistent en sumar productes de "nombres" per potències d'una "variable".

$$p(x) = \sum_{k=0}^{n} a_k x^k,$$

on a_k poden ser nombres naturals, enters, racionals, etc...
Per exemple, són polinomis

$$p(x) = x^3 - x^2 + 2x - 3 \quad \text{i} \quad p(x) = x^5 - \pi x^2 + 2x + 1$$

però

$$\sqrt{x} + \frac{1}{x} \quad \text{i} \quad \sin(x) - 2\cos(x)$$

no ho són.

Definicions bàsiques

$$p(x) = \underbrace{x^4}_{\text{terme grau 4}} \underbrace{-2x^3}_{\text{terme grau 3}} \underbrace{+2x}_{\text{terme lineal}} \underbrace{+1}_{\text{terme independent}}$$

- **Grau o ordre d'un terme**: exponent de la part literal
- **Coeficient d'ordre** n: coeficient del terme de grau n
- **Grau o ordre d'un polinomi**: grau més elevat amb coeficient no nul
- **Monomi: polinomi d'un sol terme**: $3x^2$, $15x^3$,...
- **Binomi: polinomi de dos termes**: $3x^3 - x$, $25x^{15} + 4x$,...

Conjunt de polinomis

Segons com siguin els coeficients els podem classificar en diferents conjunts:

Definició

Conjunt de polinomis de qualsevol grau amb coeficients a $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ *i* $\mathbb{R}$ *són* $\mathbb{N}[x]$, $\mathbb{Z}[x]$, $\mathbb{Q}[x]$ *o* $\mathbb{R}[x]$, *respectivament.*

Per exemple:

$$p(x) = 2x^5 + x^3 \qquad p(x) \in \mathbb{N}[x]$$

$$p(x) = 2x^5 - x^2 + 1 \qquad p(x) \in \mathbb{Z}[x],\ p(x) \notin \mathbb{N}[x]$$

$$p(x) = x^6 + \frac{3}{2}x + \frac{1}{3} \qquad p(x) \in \mathbb{Q}[x],\ p(x) \notin \mathbb{Z}[x]$$

$$p(x) = x^3 - \sqrt{2}x^2 - \pi x \qquad p(x) \in \mathbb{R}[x],\ p(x) \notin \mathbb{Q}[x]$$

Avaluació d'un polinomi a un valor

Els polinomis els poden veure com funcions (tema que vindrà després). És a dir, en donar valors a la variable x prenen diferents valors. Per exemple, si

$$p(x) = x^2 - 2x + 1,$$

$p(2) = 2^2 - 2 \cdot 2 + 1 = 1$, o $p(\sqrt{3}) = \sqrt{3}^2 - 2\sqrt{3} + 1 = 4 - 2\sqrt{3}$.

Arrels d'un polinomi

Un valor molt especial és aquell que fa que el polinomi s'anul·li:

$$p(x) = 0.$$

Tenim fórmules per 1r, 2n, 3r i 4rt grau (fórmules de Cardano, segle XVI). Però a partir de grau 5 no és possible trobar-ne cap.
Évariste Galois, matemàtic francès del segle XIX va demostrar-ho als 20 anys (edat a la que morir en un duel a mort) i ho va relacionar amb la resolució de polígons amb regla i compàs.

Arrels d'un polinomi

Grau 1:

$$x + c = 0 \rightarrow x = -c$$

Grau 2:

$$x^2 + bx + c = 0 \rightarrow x = \frac{-b \pm \sqrt{b^2 - 4c}}{2}$$

Grau 3:

$$x^3 + px + q = 0$$

$$x = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$$

Operacions amb polinomis

Els polinomis tenen la mateixa estructura que $\mathbb{Z}$ (els nombres enters) (són un anell Abelià), es poden:

- Sumar (element neutre, commutativa, associativa, oposat)
- Producte (element neutre, commutativa, associativa, distributiva respectes la seuma, no tenen invers)
- Divisibilitat (divisió Euclidiana)
- Factorització
- Màxim comú divisor
- Mínim comú múltiple
- Generen el cos de fraccions

Operacions amb polinomis: suma

Els polinomis es poden sumar, grau a grau:

$$p(x) = x^3 - 2x + 1 \qquad q(x) = 2x^5 - x^3 + x$$

$$p(x) + q(x) = 2x^5 - x + 1$$

- Neutre: és el polinomi nul: $p(x) + 0 = p(x)$
- Propietats commutativa i associativa
- Polinomi invers respecte de la suma (polinomi oposat):

$$\underbrace{2x^2 - 3x + 1}_{p(x)} + \Big(\underbrace{-2x^2 + 3x - 1}_{-p(x)}\Big) = 0$$

  Oju! Necessitem almenys estar a $\mathbb{Z}[x]$!!! Els polinomis a $\mathbb{N}[x]$ no tenen polinomi oposat!
- grau $\Big(p(x) + q(x)\Big) \leq \max\Big(\text{grau } p(x), \text{grau } q(x)\Big)$: en sumar dos polinomis el grau no augmenta.
- $\mathbb{Z}[x]$ és un grup amb la suma

Operacions amb polinomis: producte

Els polinomis es poden multiplicar, fent servir la propietat distributiva del producte respecte la suma

$$p(x) = x^3 - 2x + 1 \qquad q(x) = 2x^5 - x^3 + x$$

$$p(x) \cdot q(x) = 2x^8 - 5x^6 + 2x^5 + 3x^4 - x^3 - 2x^2 + x$$

Observeu:

- Neutre: és el polinomi 1
- Propietats commutativa, associativa i distributiva respecte la suma
- grau $(p(x) \cdot q(x)) =$ grau $(p(x)) +$ grau $(q(x))$: en multiplicar polinomis el grau augmenta
- Polinomi invers respecte el producte: no existeix a $\mathbb{R}[x]$: es necessiten cossos finits (àlgebra abstraca, aplicacions a criptografia: algorisme RSA).
- $\mathbb{Z}[x]$ és un anell amb la suma i el producte (com els nombres enters)

Divisió Euclidiana de nombres enters

A partir d'ara només considerarem polinomis a $\mathbb{Z}[x]$, és a dir, polinomis amb coeficients enters.
Divisió Euclidiana (amb quocient i residu): respon a la pregunta quantes vegades cap un nombres dins d'un altre? Dit d'una altra manera, tenim p i som q, quant toca a cadascú?
Per exemple, si tenim 16 i som 3 obtenim

$$\underbrace{16}_{\text{Dividend}} = \underbrace{3}_{\text{Divisor}} \cdot \underbrace{5}_{\text{Quocient}} + \underbrace{1}_{\text{Residu}}$$

És a dir, 3 hi cap 5 vegades dins de 16 i en sobre 1, ja que $1 < 3$ i 3 "no hi cap dins de 1". Dit d'una altra manera, ens toca 5 a cadascú i en sobre 1.

Divisió Euclidiana

Si $p(x)$ i $d(x)$ són dos polinomis, ens podem preguntar quantes vegades hi cap d dins de p. Necessitem que grau $(p) >$ grau (d).

$$\underbrace{p(x)}_{\text{Dividend}} = \underbrace{d(x)}_{\text{Divisor}} \cdot \underbrace{q(x)}_{\text{Quocient}} + \underbrace{r(x)}_{\text{Residu}}$$

$$x^3 - 2x^2 + 3x + 1 = (x^2 - 1) \cdot (x - 2) + 4x - 3$$

Observeu:

- grau $r <$ grau d
- grau $p =$ grau $d +$ grau q
- Si grau $(p) <$ grau (d) aleshores $q(x) = 0$ (el polinomi d no hi cap dins de p perquè té grau més alt) i $r(x) = p(x)$

Exemple

Volem dividir $x^4 + 10x^3 - 10x^2 + 3x - 10$ entre $x^2 + 2x - 1$

$$
\begin{array}{r|rrrrr}
 & & & x^2 & +8x & -25 \\ \hline
x^2+2x-1 & x^4 & +10x^3 & -10x^2 & +3x & -10 \\
 & -x^4 & -2x^3 & +x^2 & & \\ \hline
 & & 8x^3 & -9x^2 & +3x & \\
 & & -8x^3 & -16x^2 & +8x & \\ \hline
 & & & -25x^2 & +11x & -10 \\
 & & & 25x^2 & +50x & -25 \\ \hline
 & & & & 61x & -35
\end{array}
$$

Obtenim

$$\underbrace{x^4 + 10x^3 - 10x^2 + 3x - 10}_{\text{Dividend}} = \underbrace{\left(x^2 + 2x - 1\right)}_{\text{Divisor}} \cdot \underbrace{\left(x^2 + 8x - 25\right)}_{\text{Quocient}} + \underbrace{61x - 35}_{\text{Residu}}$$

Múltiples i divisors

Què passa si el residu és 0?

- Amb els nombres enters: $15 = 3 \cdot 5 + 0 \longrightarrow 15$ és múltiple de 3, o bé 3 és divisor de 15.
- Amb els polinomis $p(x) = d(x) \cdot q(x) + 0 \longrightarrow p$ és múltiple de d o bé d divideix p: $x^3 - 13x - 12 = \left(x^2 + 4x + 3\right)(x - 4)$

Conseqüències: arrels d'un polinomi

Ens preguntem ara per les arrels de $p(x)$: solucions de l'equació

$$p(x) = 0$$

Imaginem que $p(x)$ és múltiple de $d(x)$. Aleshores si dividim $p(x)$ entre $d(x)$ obtenim

$$p(x) = d(x) \cdot q(x)$$

Aleshores, si $x = a$ és una arrel de $p(x)$ aleshores

$$p(a) = d(a) \cdot q(a) = 0$$

- Les arrels de $p(x)$ són arrels de $d(x)$ i/o de $q(x)$
- Les arrels de $d(x)$ i de $q(x)$ també són arrels de $p(x)$

Divisió per $x - a$

Imaginem que $x = a \in \mathbb{Z}$ és una arrel de $p(x)$, $p(a) = 0$.
Dividim $p(x)$ entre $x - a$

$$p(x) = (x - a) \cdot q(x) + r, \quad r \in \mathbb{Z}$$

Avaluem en $x = a$

$$p(a) = \underbrace{(a - a)}_{=0} \cdot q(a) + r = 0 \Longrightarrow r = 0$$

Per tant,

$$p(x) = (x - a) \cdot q(x)$$

Observem:

- trobem $q(x)$ dividint $p(x)$ entre $x - a$
- grau $(p) =$ grau $(q) + 1$.

Ruffini

Quan dividim entre polinomis de la forma $x - a$ podem fer la divisió més ràpidament.

Per exemple, dividim $p(x) = x^3 - 6x^2 + 11x - 6$ entre $x - 2$. Si fem la divisió pel mètode tradicional obtenim

$$
\begin{array}{r|l}
 & x^2 - 4x + 3 \\ \hline
x - 2 & x^3 - 6x^2 + 11x - 6 \\
 & -x^3 + 2x^2 \\ \hline
 & -4x^2 + 11x \\
 & 4x^2 - 8x \\ \hline
 & 3x - 6 \\
 & -3x + 6 \\ \hline
 & 0
\end{array}
$$

$$
\begin{array}{c|cccc}
 & 1 & -6 & 11 & -6 \\
2 & & 2 & -8 & 6 \\ \hline
 & 1 & -4 & 3 & 0
\end{array}
$$

$$x^3 - 6x^2 + 11x - 6 = (x-2)\left(x^2 - 4x + 3\right) = (x-2)(x-3)(x-1)$$

Candidats a arrel

Volem veure si $x - a$ divideix el nostre polinomi. D'on traiem el valor d'a? Recordem, si $x - a$ ha dividir $p(x)$ aleshores

$$p(x) = (x - a) \cdot q(x)$$

Si avaluem aquestes dues expressions $x = 0$ obtenim

$$p(0) = -a \cdot q(0)$$

Observem que $p(0)$ i $q(0)$ són els termes independents, que són enters. Per tant, a **ha de ser un divisor del terme independent**.

Exemple

Volem resoldre l'equació

$$x^3 - 13x - 12 = 0,$$

que són les arrels del polinomi $p(x) = x^3 - 13x - 12$.
Provem si hi ha alguna arrel entera: divisors del terme independent: $1, -1, 2, -2, 3, 3, 4, -4, 12$ i -12.

$$p(1) = -24$$
$$p(-1) = 0$$

Com -1 és una arrel, dividim el polinomi entre $x + 1$ (alerta el canvi de signe). Ho fem per Ruffini:

$$\begin{array}{r|rrrr}
 & 1 & 0 & -13 & -12 \\
-1 & & -1 & 1 & 12 \\
\hline
 & 1 & -1 & -12 & \multicolumn{1}{|r}{0}
\end{array}$$

Exemple

Per tant tenim

$$x^3 - 13x - 12 = (x+1)\left(x^2 - x - 12\right).$$

Si hi ha més arrels aquestes són les del quocient:

$$x = \frac{1 \pm \sqrt{1 + 4 \cdot 12}}{2} \Longrightarrow x = 4 \text{ i } x = -3.$$

Per tant les solucions són -1, -3 i -4.

Factorització de polinomis

Recordem, amb els nombres enters podem factoritzar, és a dir, escriure com a producte de nombres més petits.

$$420 = 7 \cdot 4 \cdot 15$$

ja que 7, ,4 i 15 són divisors de 420. Doncs podem fer el mateix amb polinomis: escriure'ls com a producte de polinomis de grau més petit. Per exemple,

$$x^8 + 4x^7 + 2x^6 + 2x^5 + 17x^4 + 2x^3 - 8x^2 + 4x - 24 =$$
$$(x^2 + 5x + 6) \cdot (x^3 + 4) \cdot (x - 1) \cdot (x^2 + 1)$$

Polinomis primers o irreductibles

Com amb els nombres enters, amb els polinomis podem parlar de polinomis irreductibles, que fan el paper de nombres primers. És a dir

Divisió Euclidiana

Direm que

- Direm que $d(x)$ divideix $p(x)$ quan $r(x) = 0$, i escriurem $d(x)|p(x)$.
- Si a és una arrel de $p(x)$, aleshores $x - a|p(x)$. Per tant, podrem escriure

$$p(x) = (x - a) \cdot q(x)$$

- Conseqüències:
  - El nombre màxim d'arrels d'un polinomi és el seu grau.
  - Si $p(x) \in \mathbb{Z}[x]$ i $a \in \mathbb{Z}$ és una arrel, aleshores a divideix el terme independent de $p(x)$.

Nombre màxim d'arrels

El nombre màxim d'arrels d'un polinomi de grau n és n. Suposem que no fos així i que un polinomi $p(x)$ de grau n tingués $n+1$ arrels. Aleshores el polinomi es podria escriure de la forma $(x-r_1)(x-r_2)\cdots(x-r_n)(x-r_{n+1})$. Però aquest polinomi té grau $n+1$, i per tant no pot ser.

Polinomis primers (o irreductibles)

Direm que un polinomi és irreductible (o primer) si només és divisible entre ell mateix (o entre un nombre). Observem que tot polinomi és divisible entre un nombre, per exemple

$$x^2 - 2x + 3 = 2 \cdot \left(\frac{x^2}{2} - x + \frac{3}{2} \right)$$

Els polinomis

$$p(x) = x^2 + x + 2 \quad q(x) = x - 1$$

són irreductibles a $\mathbb{R}[x]$: $p(x)$ no té arrels reals, i $q(x)$ és de grau 1.

Polinomis primers (o irreductibles)

A $\mathbb{R}[x]$ els únics polinomis irreductibles són de la forma $x - a$ o bé polinomis de 2n grau sense arrels reals. A $\mathbb{C}[x]$, els polinomis factoritzen *completament* en factors de grau 1 (Teorem fonamental de l'àlgebra: $\mathbb{C}$ és algebraicament tancat).

Factorització de polinomis

A $\mathbb{R}[x]$ qualsevol polinomi es pot escriure com a producte de factors irreductibles de primer i segon grau:

$$p(x) = \Pi(x - r_i) \cdot \Pi(x^2 + b_i x + c_i),$$

on r_i són les arrels (reals) de $p(x)$ i $x^2 + b_i x + c_i$ són polinomis de 2n sense arrels reals.

Mínim comú múltiple

El mínim comú múltiple de dos polinomis és el polinomis de grau més baix que és múltiple de tots dos. Com amb els nombres enters, el més senzill per trobar-lo és factoritzar i completar amb el factors que faltin. Per exemple els polinomis,

$$p(x) = x^2 + x - 6 = (x-2)(x+3)$$
$$q(x) = x^2 + 2x - 3 = (x-1)(x+3)$$

tenen un factor comú, $x+3$. Per tant el mínim comú múltiple serà

$$mcm(p(x), q(x)) = (x-2)(x+3)(x-1) = x^3 - 7x + 6$$

S'obté escollint els factor comuns i els no comus de grau més alt.

Màxim comú divisor

El màxim comú divisor de dos polinomis és el polinomi de grau més alt possible que els divideix a tots dos. Per exemple, a l'exemple anterior obtenim $Mcd(p(x), q(x)) = x + 3$ (comuns de grau més baix). Un altre exemple, si

$$
\begin{aligned}
p(x) &= x^4 + 5x^3 + x^2 - 21x - 18 = (x-2)(x+3)^2(x+1) \\
q(x) &= x^5 + 4x^4 - 7x^3 - 34x^2 + 12x + 72 = (x-2)^2(x+3)^2(x+2),
\end{aligned}
$$

aleshores $Mcd(p(x), q(x)) = (x-2)(x+3)^2 = x^3 + 4x^2 - 3x - 18$.

Fraccions de polinomis

Com amb els enters, es pot considerar el "quocient" de polinomis:

$$\frac{p(x)}{q(x)}$$

això s'anomena una fracció de polinomis.
Com amb els enters, es fraccions de polinomis es poden simplificar, sumar i mulitplicar:

Simplificació de fraccions de polinomis

Com amb els nombres enters, els factors que comuns entre numerador i denominador es cancel·len (simplifiquen). Factoritzant els polinomis podem veure si hi ha factors en comú i els podem simplificar:

$$\frac{x^3 - 2x^2 - 15x}{x^2 + 7x + 10} = \frac{x(x-3)\cancel{(x+5)}}{\cancel{(x+5)}(x+2)} = \frac{x(x-3)}{x+2}$$

- Una fracció és *irreductible* si no es pot simplificar
- Dues fraccions de polinomis són equivalents si, en simplificar-les, s'obté la mateixa fracció irreductible

Suma de fraccions de polinomis

Com amb les fraccions de nombres enters, les fraccions de polinomis es poden sumar:

$$\frac{p(x)}{q(x)} + \frac{r(x)}{s(x)} = \frac{p(x)s(x) + r(x)q(x)}{q(x)s(x)}$$

La suma té les següent propietats:

- Té neutre, i és la fracció $\frac{0}{p(x)} = 0$. Fixeu-vos que no és únic, ja que només cal que el numerador sigui 0 (i el denominador no ho sigui). No obstant, totes les fraccions amb un 0 al numerador són equivalents.
- Les fraccions tenen invers respecte la suma (fracció poposada): $\frac{p(x)}{q(x)} + \frac{-p(x)}{q(x)} = \frac{p(x)q(x) - q(x)p(x)}{q(x)} = \frac{0}{q(x)} = 0$
- Compleix les propietats commutativa i associativa.
- Si $q(x)s(x)$ no és el mínim comú mútliple de $q(x)$ i $s(x)$ aleshores la fracció resultant es podrà simplificar.

Suma amb mínim comú múltiple

Per tal de tenir el denominador resultant el més petit possible i estalviar-nos (amb sort) simplificar, és recomanble utilitzar el mínim comú múltiple dels denominadors a l'hora de sumar fraccions:

$$\frac{x^2}{x^4+5x^3+x^2-21x-18} - \frac{x^3-1}{x^5+4x^4-7x^3-34x^2+12x+72}$$

$$= \frac{x^2}{(x-2)(x+3)^2(x+1)} + \frac{x^3-1}{(x-2)^2(x+3)^2(x+2)} =$$

$$\frac{x^2(x-2)(x+2)+(x^3-1)(x-2)(x+1)}{(x-2)^2(x+3)^2(x+1)(x+2)}$$

$$= \frac{x^5-2x^3-5x^2+x+2}{(x-2)^2(x+3)^2(x+1)(x+2)}$$

Producte de fraccions

Les fraccions de polinomis es poden multiplicar:

$$\frac{p(x)}{q(x)} \cdot \frac{r(x)}{s(x)} = \frac{p(x) \cdot r(x)}{q(x) \cdot s(x)}$$

i tenen les següents propietats

- Hi ha neutre, i és la fracció $\frac{p(x)}{q(x)}$, que és equivalent a la fracció $\frac{1}{1}$.
- Tota fracció (menys la 0) té invers respecte el producte:

$$\frac{p(x)}{q(x)} \cdot \frac{q(x)}{p(x)} = \frac{\cancel{p(x)} \cdot \cancel{q(x)}}{\cancel{q(x)} \cdot \cancel{p(x)}} = \frac{1}{1}$$

- Compleix les propietats communitativa i associativa

Cos de fraccions de polinomis

Les fraccions de polinomis amb les propietats anteriors són un cos: dues operacions, les dues tenen neutre i totes dues tenen invers (excepte el neutre de la suma). Per tant, les fraccions de polinomis són "exactament iguals" que les fraccions d'enters, és a dir, que els racionals $\mathbb{Q}$.