Polinomios y Raíces

Teresa Krick*

Departamento de Matemática. Facultad de Ciencias Exactas y Naturales.

Universidad de Buenos Aires. -1428- Buenos Aires. ARGENTINA.

Contents

*Estas notas amplían un curso dado en la REM, Río Cuarto, del 16 al 18 de Octubre del 95, y fueron realizadas en el marco del subsidio UBACyT-EX001 (1995-1997)

1 Introducción y Notaciones

1.1 Introducción

Constantemente, al plantear en términos matemáticos problemas de distintas áreas (economía, física, ingeniería, biología, etc.), aparece la siguiente cuestión : tratar de determinar los ceros de ciertas funciones, es decir valores para los cuales la función se anula.

Después de las funciones lineales, las funciones polinomiales (en 1 variable) son las más simples. Estudiar los ceros (raíces) de funciones polinomiales tiene un gran interés por lo menos por las dos razones siguientes :
– No se puede pretender poder resolver el problema para funciones más generales si no se logra resolverlo en este caso más sencillo.
– Muchas veces es posible traducir de alguna manera el problema original de hallar ceros de una función cualquiera al de calcular las raíces de ciertos polinomios (que "aproximan" a la función original).

Generalmente, para las aplicaciones, uno trabaja con funciones reales, y se trata de encontrar ceros reales. Más aún, debido a la estructura de los números con los cuales trabajan las computadoras, las funciones suelen tener coeficientes racionales y los ceros que seremos capaces de calcular serán números racionales que aproximan suficientemente una verdadera solución al problema.

En este texto, se trata de profundizar sobre raíces de polinomios con coeficientes en $\mathbb{Q}$ (el cuerpo de los números racionales), $\mathbb{R}$ (el cuerpo de los números reales) y $\mathbb{C}$ (el cuerpo de los números complejos). Se verá en qué medida la teoría sobre $\mathbb{Q}$ está más resuelta, y la de $\mathbb{C}$, más teórica, permite aclarar la estructura de los polinomios en $\mathbb{R}[X]$.

Este texto presupone cierta familiaridad con la teoría general básica de polinomios en 1 variable, aunque todos los resultados que se usan están resumidos (en general sin ejemplificación) en la Sección 2. También se requieren ciertas nociones de Análisis elemental, para el caso de funciones reales continuas y derivables (como por ejemplo los Teoremas de Bolzano y de Rolle).

Quisiera agradecer aquí a Alicia Dickenstein por su minuciosa lectura y comentarios.

1.2 Notaciones

- En la sección siguiente, $\mathbf{K}$ denotará un cuerpo cualquiera, por ejemplo $\mathbf{K} = \mathbb{Q}, \mathbb{R}$ ó $\mathbb{C}$, y $\mathbf{K}[X]$ el anillo de los polinomios con coeficientes en $\mathbf{K}$, cuyos elementos son de la forma $f = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_0$, con $a_i \in \mathbf{K}$ $(1 \leq i \leq n)$ y $a_n \neq 0$ si $f \neq 0$.

- Si $f \neq 0$, se notará con $\mathrm{gr}(f)$ el *grado* del polinomio f, es decir el máximo exponente n de los monomios no nulos de f.

- Se notará con $\mathrm{cp}(f)$ el *coeficiente principal* de f, es decir el coeficiente que acompaña a $X^{\mathrm{gr}(f)}$. Si $\mathrm{cp}(f) = 1$ se dice que f es *mónico*.

- La relación de divisibilidad se nota con $|$: Sean $f, g \in \mathbf{K}[X]$, $g \,|\, f$ (g *divide a* f) $\iff$ existe $q \in \mathbf{K}[X]$ tal que $f = q\, g$. En caso contrario, g no divide a f y se nota $g \not| f$.

- Se recuerda que se dice que $\alpha \in \mathbf{K}$ es *raíz* de f si $f(\alpha) = 0$.

2 Hechos generales

En esta sección, se recuerdan (mayormente sin demostración) los resultados básicos de la teoría de polinomios, que serán usados luego para exponer las teorías más específicas de los polinomios con coeficientes en $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$. Como es bien sabido, la aritmética de los polinomios con coeficientes en un cuerpo es similar a la de los enteros, en cuanto a divisibilidad, algoritmo de división, factorización, etc. Las diferencias empiezan a aparecer en cuanto se trata más particularmente de estudiar raíces de polinomios y su comportamiento. Todas las demostraciones pueden ser consultadas en [3] y [2]. Otro libro más antiguo pero muy interesante y completo es [7].

2.1 Algoritmo de División

Teorema 1 (Algoritmo de División) *Dados polinomios* $f,\ g \in \mathbf{K}[X],\ g \neq 0$, *existen únicos polinomios* q *(cociente) y* r *(resto) en* $\mathbf{K}[X]$ *tales que*

$$f = q\,g + r \quad \text{con} \quad r = 0 \quad \acute{o} \quad \mathrm{gr}(r) < \mathrm{gr}(g)$$

Proposición 2 (Teorema del Resto) *Dados* $f \in \mathbf{K}[X]$ *y* $\alpha \in \mathbf{K}$, *se tiene*

$$f(X) = q(X)(X - \alpha) + f(\alpha)$$

Consecuencia 3
$\alpha \in \mathbf{K}$ *es raíz de* $f \iff f(\alpha) = 0 \iff X - \alpha \,|\, f \iff f = (X - \alpha)q$ *para algún* $q \in \mathbf{K}[X]$.

Ejemplos

- f constante : $f = c$ con $c \in \mathbf{K}$.
  Entonces, ó bien $c = 0$ y todo $\alpha \in \mathbf{K}$ es raíz de f, ó bien $c \neq 0$ y f no tiene ninguna raíz en $\mathbf{K}$.
- f de grado 1 : $f = aX + b$ con $a, b \in \mathbf{K},\ a \neq 0$.
  Entonces $-\frac{b}{a}$ es raíz de f y $f = a(X - (-\frac{b}{a}))$.
- f de grado 2 : $f = aX^2 + bX + c$ con $a, b, c \in \mathbf{K},\ a \neq 0$
  Supondremos aquí que $2 \neq 0$ en $\mathbf{K}$ (o sea la característica de $\mathbf{K}$ es distinta de 2).
  Luego

$$f = a\left(X^2 + \frac{b}{a}X + \frac{c}{a}\right) = a\left(\left(X + \frac{b}{2a}\right)^2 - \frac{b^2}{4a^2} + \frac{c}{a}\right) = a\left(\left(X + \frac{b}{2a}\right)^2 - \frac{b^2 - 4ac}{4a^2}\right)$$

  Se define el *discriminante* de f como $\Delta = \Delta(f) := b^2 - 4ac$. Entonces, si existe $\beta \in \mathbf{K}$ tal que $\beta^2 = \Delta$, se tiene que :

$$f = a\left(\left(X + \frac{b}{2a}\right)^2 - \left(\frac{\beta}{2a}\right)^2\right) = a\left(X - \frac{-b + \beta}{2a}\right)\left(X - \frac{-b - \beta}{2a}\right)$$

  y se obtienen las raíces (a lo mejor la misma repetida) :

$$\alpha_1 = \frac{-b + \beta}{2a} \quad , \quad \alpha_2 = \frac{-b - \beta}{2a}$$

– Cuando $\mathbf{K} = \mathbb{C}$, siempre existe $\beta \in \mathbb{C}$ tal que $\beta^2 = \Delta (= b^2 - 4ac)$ (pues todo número complejo tiene raíz cuadrada), luego todo polinomio de grado 2 tiene dos raíces en $\mathbb{C}$ (que pueden ser distintas o la misma repetida dos veces cuando $\beta = 0$).

– Cuando $\mathbf{K} = \mathbb{R}$, existe $\beta = \sqrt{\Delta}$ si y sólo si $\Delta \geq 0$. Por lo tanto, probamos que si $\Delta \geq 0$ entonces el polinomio tiene dos raíces reales (o la misma repetida dos veces). Por otro lado, existen polinomios de grado 2 que no tienen raíces reales como por ejemplo $X^2 + 1$ ó $X^2 + c$ con $c > 0$.

– Cuando $\mathbf{K} = \mathbb{Q}$, si Δ tiene una raíz cuadrada en $\mathbb{Q}$, entonces el polinomio tiene dos raíces racionales. Pero en este caso también existen polinomios de grado 2 con raíces reales pero sin raíces racionales, por ejemplo $X^2 - 2$.

■

Lo que se probó en el ejemplo de los polinomios de grado 2 en un cuerpo $\mathbf{K}$ de característica distinta de 2 es una condición suficiente : si existe $\beta \in \mathbf{K}$ tal que $\beta^2 = b^2 - 4ac$, entonces el polinomio $aX^2 + bX + c$ tiene dos raíces en $\mathbf{K}$ (a lo mejor la misma repetida dos veces). Pero todavía no hemos investigado la recíproca. Un poco más adelante podremos mostrar que en realidad esta condición es necesaria y suficiente, es decir :"existe $\beta \in \mathbf{K}$ tal que $\beta^2 = b^2 - 4ac$ si y sólo si el polinomio $aX^2 + bX + c$ tiene dos raíces en $\mathbf{K}$". Para ello necesitamos conocer algo de factorización de polinomios, que se resume en el párrafo 2.3.

2.2 Máximo común divisor

Definición 4 *Sean $f, g \in \mathbf{K}[X]$ no ambos nulos. El <u>máximo común divisor</u> entre f y g (que se nota $\mathrm{mcd}(f; g)$) es el (único) polinomio mónico $h \in \mathbf{K}[X]$ que verifica simultáneamente las dos condiciones siguientes :*

- $h \,|\, f$ *y* $h \,|\, g$,
- *Si* $\tilde{h} \in K[X]$ *verifica que* $\tilde{h} \,|\, f$ *y* $\tilde{h} \,|\, g$, *entonces* $\tilde{h} \,|\, h$.

Ejemplos Sean $f, g \in \mathbf{K}[X]$, $g \neq 0$. Entonces :

- Sea $c \in \mathbf{K} \setminus \{0\}$, $\mathrm{mcd}(c; g) = 1$
- Si $g \,|\, f$, $\mathrm{mcd}(f; g) = \frac{g}{\mathrm{cp}(g)}$.

■

El Lema siguiente nos permitirá deducir un algoritmo para calcular el máximo común divisor :

Lema 5 *Sean $f, g \in \mathbf{K}[X]$, $g \neq 0$, y sean $q, r \in \mathbf{K}[X]$ con $f = qg + r$, entonces* $\mathrm{mcd}(f; g) = \mathrm{mcd}(g; r)$.

Como consecuencia, se obtiene el siguiente algoritmo, debido a Euclides (Siglo III AC), que permite calcular siempre el máximo común divisor entre dos polinomios $f, g \in \mathbf{K}[X]$ y además expresarlo como como combinación polinomial de f y g, es decir hallar polinomios $s, t \in \mathbf{K}[X]$ tales que $\mathrm{mcd}(f; g) = sf + tg$:

Observación 6 (Algoritmo de Euclides)
Sean $f, g \in \mathbf{K}[X]$, *no nulos y con* $\mathrm{gr}(f) \geq \mathrm{gr}(g)$. *Entonces* $\mathrm{mcd}(f;g)$ *es el último resto* r_k *no nulo (dividido por su coeficiente principal para volverlo mónico) que aparece en la sucesión de divisiones siguiente :*

$$\begin{array}{lcll} f & = & q_1 g + r_1 & con \quad \mathrm{gr}(r_1) < \mathrm{gr}(g) \\ g & = & q_2 r_1 + r_2 & con \quad \mathrm{gr}(r_2) < \mathrm{gr}(r_1) \\ r_1 & = & q_3 r_2 + r_3 & con \quad \mathrm{gr}(r_1) < \mathrm{gr}(g) \\ & \vdots & & \\ r_{k-2} & = & q_k r_{k-1} + r_k & con \quad \mathrm{gr}(r_k) < \mathrm{gr}(r_{k-1}) \\ r_{k-1} & = & q_{k+1} r_k & \end{array}$$

(pues resulta $\mathrm{mcd}(f;g) = \mathrm{mcd}(g;r_1) = \mathrm{mcd}(r_1;r_2) = \cdots = \mathrm{mcd}(r_{k-2};r_{k-1}) = \mathrm{mcd}(r_{k-1};r_k) = \frac{r_k}{\mathrm{cp}(r_k)}$, *ya que* $r_k | r_{k-1}$ *).*
Luego, despejando r_k *de la anteúltima igualdad, y volviendo hacia arriba despejando paso a paso* r_{k-1}, $r_{k-2}, \ldots,$ r_2, r_1 *en las igualdades anteriores, se logra escribir* r_k *en la forma* $r_k = s'f + t'g$. *Finalmente, dividiendo toda la expresión por la constante* $\mathrm{cp}(r_k)$, *se obtienen* $s, t \in \mathbf{K}[X]$ *tales que* $\mathrm{mcd}(f;g) = sf + tg$.

Ejemplo Sean $f = X^5 + X^4 - 3X^3 + 4X^2 + 2X$ y $g = X^4 + 3X^3 - X^2 - 6X - 2$. Se tiene :

$$\begin{array}{lcll} f & = & (X-2)g + r_1 & \text{con} \quad r_1 = 4X^3 + 8X^2 - 8X - 4 \\ g & = & (\frac{1}{4}X + \frac{1}{4})r_1 + r_2 & \text{con} \quad r_2 = -X^2 - 3X - 1 \\ r_1 & = & (-4X + 4)r_2 & \end{array}$$

Luego $\mathrm{mcd}(f;g) = \frac{r_2}{\mathrm{cp}(r_2)} = X^2 + 3X + 1$ y

$$\begin{array}{rcl} r_2 & = & g - (\frac{1}{4}X + \frac{1}{4})r_1 \\ & = & g - (\frac{1}{4}X + \frac{1}{4})(f - (X-2)g) \\ & = & -(\frac{1}{4}X + \frac{1}{4})f + [1 + (\frac{1}{4}X + \frac{1}{4})(X-2)]g \\ & = & -(\frac{1}{4}X + \frac{1}{4})f + (\frac{1}{4}X^2 - \frac{1}{4}X + \frac{1}{2})g \end{array}$$

Así : $\mathrm{mcd}(f;g) = -r_2 = (\frac{1}{4}X + \frac{1}{4})f - (\frac{1}{4}X^2 - \frac{1}{4}X + \frac{1}{2})g$.

■

Corolario 7 *El máximo común divisor entre* f *y* g *es el (único) polinomio mónico* $h \in \mathbf{K}[X]$ *que verifica simultáneamente las dos condiciones siguientes :*

- $h \mid f$ *y* $h \mid g$,
- *Existen* $s, t \in \mathbf{K}[X]$ *tales que* $h = sf + tg$.

Prueba.– Que la definición del mcd implica la segunda condición del Corolario resulta del Algoritmo de Euclides. La recíproca es inmediata usando propiedades elementales de la divisibilidad.

■

Definición 8 (Polinomios coprimos) *Se dice que* $f, g \in \mathbf{K}[X]$ *son* <u>coprimos</u> *si verifican* $\mathrm{mcd}(f;g) = 1$, *es decir si ningún polinomio de grado* ≥ 1 *divide simultáneamente a* f *y a* g, *o equivalentemente si existen polinomios* $s, t \in \mathbf{K}[X]$ *tales que* $1 = sf + tg$.

Proposición 9 *Sean* $f, g, h \in \mathbf{K}[X]$ *, entonces :*

1. $f \mid h$, $g \mid h$ *y* f, g *coprimos* $\implies fg \mid h$
2. $f \mid gh$ *y* f, g *coprimos* $\implies f \mid h$.

Prueba.– $\mathrm{mcd}(f;g) = 1 \implies \exists\, s,t \in \mathbf{K}[X]$ tales que $1 = sf + tg$. Luego $h = sfh + tgh$.

1. h es divisible por fg pues cada sumando lo es ($g \mid h$ en el primer sumando y $f \mid h$ en el segundo).
2. f divide a cada sumando, por lo tanto f divide a h .

■

Observación 10 *Sean* $f, g \in \mathbf{K}[X]$ *, entonces* $\frac{f}{\mathrm{mcd}(f;g)}$ *y* $\frac{g}{\mathrm{mcd}(f;g)}$ *son coprimos.*

2.3 Factorización de polinomios

Definición 11 (Polinomios irreducibles) *Sea* $f \in \mathbf{K}[X]$ *, no constante (o sea* $\mathrm{gr}(f) \geq 1$ *). Se dice que* f *es* <u>*irreducible*</u> *si y sólo si no existe ningún* $g \in \mathbf{K}[X]$ *con* $1 \leq \mathrm{gr}(g) < \mathrm{gr}(f)$ *tal que* $g \mid f$ *, o equivalentemente, no existen polinomios* $g, h \in \mathbf{K}[X]$ *, ambos de grado estrictamente menor que el de* f *, de manera que* $f = g\,h$.
En caso contrario, se dice que f *es* <u>*reducible*</u>*, eso es cuando existe* $g \in \mathbf{K}[X]$ *no constante y de grado estrictamente menor que el de* f *tal que* $g \mid f$.

Ejemplos

- X^2-1 es reducible en $\mathbb{Q}[X]$, $\mathbb{R}[X]$ y $\mathbb{C}[X]$ pues $X+1 \mid X^2-1$ y $1 \leq \mathrm{gr}(X+1) < \mathrm{gr}(X^2-1)$.
- Todo polinomio f de grado 1 en $\mathbf{K}[X]$ es irreducible en $\mathbf{K}[X]$, para $\mathbf{K}$ cuerpo cualquiera, pues no puede existir ningún polinomio g tal que $1 \leq \mathrm{gr}(g) < \mathrm{gr}(f) = 1$.
- X^2+1 es irreducible en $\mathbb{Q}[X]$ y $\mathbb{R}[X]$ pues si no lo fuera, sería producto de dos polinomios de grado 1, y por lo tanto, tendría raíces en $\mathbb{Q}$ ó $\mathbb{R}$ (como vimos antes, todo polinomio de grado 1 tiene raíz).
- El polinomio $(X^2+1)(X^2+2)$ es reducible, si bien no tiene raíces ni en $\mathbb{Q}$ ni en $\mathbb{R}$.
- Todo polinomio $f \in \mathbf{K}[X]$ de grado mayor o igual que 2 que tiene una raíz $\alpha \in \mathbf{K}$ es reducible, pues $X - \alpha \mid f$ con $1 = \mathrm{gr}(X-\alpha) < \mathrm{gr}(f)$. Pero la recíproca es falsa en general : f puede ser reducible sin tener ninguna raíz en $\mathbf{K}$ (por lo menos para $\mathbf{K} = \mathbb{Q}$ ó $\mathbb{R}$). Acabamos de ver un ejemplo más arriba.

■

La propiedad siguiente de los polinomios irreducibles es una consecuencia de la definición de polinomio irreducible y de la Proposición 9.

Observación 12 (Primalidad de los polinomios irreducibles) *Sean* $f, g, h \in \mathbf{K}[X]$ *, con* f <u>*irreducible*</u>*, entonces :*

- $\mathrm{mcd}(f;g) = \frac{f}{\mathrm{cp}(f)}$ *si* $f \mid g$ *y* $\mathrm{mcd}(f;g) = 1$ *si* $f \not\mid g$.
- $f \mid gh \implies f \mid g$ *ó* $f \mid h$.

Teorema 13 (Teorema Fundamental de la Aritmética) *Sea* $\mathbf{K}$ *un cuerpo, y sea* $f \in \mathbf{K}[X]$ *un polinomio no constante. Entonces existen únicos polinomios irreducibles mónicos distintos* $g_1, \ldots, g_m$ *en* $\mathbf{K}[X]$ *de manera que :*

$$f = c\, {g_1}^{k_1} {g_2}^{k_2} \ldots {g_m}^{k_m} \quad \text{donde} \quad c \in \mathbf{K} \setminus \{0\} \text{ y } k_1, \ldots, k_m \in \mathbb{N}$$

(Claramente la unicidad de los factores irreducibles g_i *es salvo el orden de los factores.)*
La constante c *resulta ser el coeficiente principal de* f *.*

Ejemplo El polinomio $(X^2+1)(X^2-2)$ está factorizado en factores irreducibles en $\mathbb{Q}[X]$ (pues ambos factores son irreducibles) pero su factorización en $\mathbb{R}[X]$ es $(X^2+1)(X-\sqrt{2})(X+\sqrt{2})$ y su factorización en $\mathbb{C}[X]$ es $(X+i)(X-i)(X+\sqrt{2}i)(X-\sqrt{2}i)$.

■

Observación 14 *Si* $f \in \mathbf{K}[X]$ *tiene una raíz* $\alpha \in \mathbf{K}$*, entonces el polinomio* $X-\alpha$ *es uno de los factores de la factorización en irreducibles de* f *(pues* $f = (X-\alpha)q$ *y por la unicidad de la factorización, para factorizar* f *alcanza con factorizar* q*).*

Estamos ahora en condiciones de retomar el ejemplo de los polinomios de grado 2 : podemos mostrar ahora que si aX^2+bX+c tiene una raíz en $\mathbf{K}$ (con $\text{car}(\mathbf{K}) \neq 2$) entonces b^2-4ac es un cuadrado en $\mathbf{K}$. Con ésto, concluiremos la demostración de la afirmación : "existe $\beta \in \mathbf{K}$ tal que $\beta^2 = b^2-4ac$ si y sólo si el polinomio aX^2+bX+c tiene dos raíces en $\mathbf{K}$".
En efecto, si $f = aX^2+bX+c$ tiene una raíz $\alpha_1 \in \mathbf{K}$, entonces, por la observación anterior, $X-\alpha_1$ aparece en la factorización de f, y por razones de grado, el otro factor irreducible mónico tiene grado uno, y se puede escribir $X-\alpha_2$. Por consiguiente, f tiene sus dos raíces α_1 y α_2 en $\mathbf{K}$ y se escribe en la forma :

$$f = a(X-\alpha_1)(X-\alpha_2) = aX^2 - a(\alpha_1+\alpha_2)X + a\alpha_1\alpha_2$$

Igualando coeficiente a coeficiente, resulta que $b = -a(\alpha_1+\alpha_2)$ y $c = a\alpha_1\alpha_2$.
Por lo tanto, $b^2-4ac = a^2(\alpha_1+\alpha_2)^2 - 4a^2\alpha_1\alpha_2 = a^2(\alpha_1^2+\alpha_2^2-2\alpha_1\alpha_2) = [a(\alpha_1-\alpha_2)]^2$ y resulta ser un cuadrado en $\mathbf{K}$!

■

Finalmente, se puede describir el máximo común divisor entre dos polinomios f y g en términos de los factores irreducibles mónicos de sus factorizaciones :

Observación 15 *Sean* $f, g \in \mathbf{K}[X]$*, entonces* $\text{mcd}(f;g)$ *es el producto de los factores irreducibles mónicos que aparecen en común en las factorizaciones de* f *y* g*, a la mínima potencia con la que aparecen. Por ejemplo* $\text{mcd}(3X^3(X-1)^2; 2X^2(X-1)^3) = X^2(X-1)^2$.

La Observación precedente puede parecer a primer vista un algoritmo para calcular el máximo común divisor entre dos polinomios, incluso más simple que el de Euclides, pero en realidad no es así ya que no se conocen algoritmos para factorizar polinomios, por lo menos en los casos $\mathbf{K} = \mathbb{R}$ ó $\mathbf{K} = \mathbb{C}$. Esto se discutirá más adelante.

2.4 Raíces múltiples

Una raíz de un polinomio f puede estar repetida. Por ejemplo $X^2-2X+1=(X-1)^2$ tiene dos veces la raíz 1 (o, mas generalmente, todo polinomio de grado 2 con discriminante igual a 0 tiene dos raíces repetidas).

Definición 16 *Sea $f\in\mathbf{K}[X]$ y $\alpha\in\mathbf{K}$ raíz de f. Se dice que :*

- *α es raíz <u>simple</u> de f si y sólo si $f(\alpha)=0$ pero $(X-\alpha)^2\not| f$, o sea $f=(X-\alpha)q$ con $q(\alpha)\neq 0$.*
  (A nivel de la factorización de f, esto significa que el factor irreducible $X-\alpha$ aparece en la factorización de f con potencia exactamente 1.)
- *α es raíz <u>múltiple</u> de f si y sólo si $(X-\alpha)^2\,|\,f$, o sea $f=(X-\alpha)^2q$.*
  (A nivel de la factorización de f, esto significa que el factor irreducible $X-\alpha$ aparece en la factorización de f con potencia estrictamente mayor que 1.)
- *α es raíz <u>de multiplicidad exactamente k</u> de f si y sólo si $(X-\alpha)^k\,|\,f$ pero $(X-\alpha)^{k+1}\not| f$, o sea $f=(X-\alpha)^kq$ con $q(\alpha)\neq 0$.*
  (A nivel de la factorización de f, esto significa que el factor irreducible $X-\alpha$ aparece en la factorización de f con potencia exactamente k.)

Ejemplo -1 es raíz doble de $(X+1)^2(X^2-4)$ y triple de $(X+1)^2(X^2-1)$.

■

Hay una relación entre la multiplicidad de una raíz y el hecho de ser raíz de la derivada f' del polinomio f (donde $(a_nX^n+a_{n-1}X^{n-1}+\cdots+a_1X+a_0)'=na_nX^{n-1}+(n-1)a_{n-1}X^{n-2}+\cdots+a_1$). Pensemos por ejemplo en una parábola $(X-\alpha)^2$: α define un mínimo y por lo tanto $f'(\alpha)=0$. Este hecho es más general :

Proposición 17 *Sea $\mathbf{K}$ un cuerpo de característica 0 (es decir $p\neq 0$ en $\mathbf{K}$ para todo p número primo), por ejemplo $\mathbf{K}=\mathbb{Q},\mathbb{R}$ ó $\mathbb{C}$, que son los casos que nos interesan aquí.*
Sea $f\in\mathbf{K}[X]$ no nulo. Notaremos con f' la derivada del polinomio f y con $f^{(i)}$ la derivada $i-$ésima de f, para todo $i\in\mathbb{N}$.

1. *α es raíz múltiple de $f\iff\alpha$ es simultáneamente raíz de f y de f'.*
   (Equivalentemente, α es raíz simple de $f\iff f(\alpha)=0$ y $f'(\alpha)\neq 0$.)
2. *α es raíz de multiplicidad exactamente k de f $(k\geq 1)\iff\alpha$ es raíz de f y además es raíz de multiplicidad exactamente $k-1$ de f'.*
3. *α es raíz de multiplicidad exactamente k de f $(k\geq 1)\iff f(\alpha)=f'(\alpha)=\cdots=f^{(k-1)}(\alpha)=0$ y $f^{(k)}(\alpha)\neq 0$.*

(Para un cuerpo $\mathbf{K}$ de característica positiva p, el segundo y tercer inciso tienen que ser reemplazadas por implicaciones un poco más débiles, que pueden deducirse observando lo que es válido en la demostración de (2).)

Prueba.–

1. $(\Longrightarrow)$ $f=(X-\alpha)^2q$, luego $f'=2(X-\alpha)q+(X-\alpha)^2q'=(X-\alpha)(2q+(X-\alpha)q')$ y se verifica $f(\alpha)=f'(\alpha)=0$.

   $(\Longleftarrow)$ Como α es raíz de f, se puede escribir $f=(X-\alpha)q$, y se quiere mostrar entonces que $q(\alpha)=0$, o sea $X-\alpha\,|\,q$, para así probar que $(X-\alpha)^2\,|\,f$:

   Se tiene $f'=q+(X-\alpha)q'$ y la condición $f'(\alpha)=0$ implica inmediatamente que $q(\alpha)=0$.

2. ($\Longrightarrow$) $f = (X-\alpha)^k q$ con $q(\alpha) \neq 0$, luego $f' = k(X-\alpha)^{k-1}q + (X-\alpha)^k q' = (X-\alpha)^{k-1}(kq + (X-\alpha)q')$ y, tomando $h := kq + (X-\alpha)q'$, se verifica que $f' = (X-\alpha)^{k-1}h$ con $h(\alpha) \neq 0$ (pues $q(\alpha) \neq 0$ y en un cuerpo de característica 0, $k \neq 0$).

   ($\Longleftarrow$) Como α es raíz de f, tiene una cierta multiplicidad $r \geq 1$ como raíz. Se pretende probar que $r = k$:

   Sea $f = (X-\alpha)^r q$ con $q(\alpha) \neq 0$. Luego $f' = (X-\alpha)^{r-1}(rq + (X-\alpha)q')$. Si definimos $h := rq + (X-\alpha)q'$, resulta que $f' = (X-\alpha)^{r-1}h$ con $h(\alpha) \neq 0$, por consiguiente α es raíz de multiplicidad exactamente $r-1$ de f', pero por hipótesis, esa multiplicidad es $k-1$, por lo tanto $r-1 = k-1$, es decir $r = k$.

3. Para hacerlo formalmente, se usa inducción en la multiplicidad k de α como raíz de f.

   - $\underline{k = 1}$: Es una consecuencia inmediata del inciso (1) : α es raíz simple de $f \iff \alpha$ es raíz de f y no es raíz de f'.
   - $\underline{k > 1}$: Por (2), α es raíz de multiplicidad k de $f \iff f(\alpha) = 0$ y α es raíz de multiplicidad $k-1$ de f'.

     Por hipótesis inductiva, α es raíz de multiplicidad $k-1$ de $f' \iff f'(\alpha) = (f')'(\alpha) = \cdots = (f')^{(k-2)}(\alpha) = 0$ y $(f')^{(k-1)}(\alpha) \neq 0$. Se concluye observando que $(f')^{(j)} = f^{(j+1)}$.

■

2.5 Cantidad de raíces

Un polinomio f no nulo de grado n no puede tener demasiadas raíces, aún contadas con multiplicidad :

Teorema 18 *Sea $f \in \mathbf{K}[X]$ no nulo de grado n. Entonces f tiene a lo sumo n raíces en $\mathbf{K}$ contadas cada una con su multiplicidad.*

Prueba.– La haremos por inducción en el grado n de f :

- $\underline{n = 0}$: f polinomio constante no nulo no tiene ninguna raíz.
- $\underline{n > 0}$: Si f no tiene ninguna raíz en $\mathbf{K}$, no hay nada que probar. Si tiene por lo menos una raíz α, entonces $f = (X-\alpha)q$ y q es un polinomio de grado $n-1$ que por hipótesis inductiva tiene a lo sumo $n-1$ raíces en $\mathbf{K}$. Por lo tanto, f tiene a lo sumo n raíces en $\mathbf{K}$.

■

Observación 19 *Sea $f \in \mathbf{K}[X]$, y sean $\alpha_1, \ldots . \alpha_m \in \mathbf{K}$ raíces distintas de f de multiplicidad $k_1, \ldots, k_m$ respectivamente, entonces :*

$$(X-\alpha_1)^{k_1}(X-\alpha_2)^{k_2} \ldots (X-\alpha_m)^{k_m} \mid f$$

(Esto es debido a que $(X-\alpha_1)^{k_1} \mid f, \ldots, (X-\alpha_m)^{k_m} \mid f$, y al ser los polinomios de la izquierda coprimos dos a dos (ya que no tienen ningún factor irreducible en común), su producto también divide a f.)

2.6 Polinomio interpolador

En esta sección, supondremos que el cuerpo $\mathbf{K}$ tiene característica 0, por ejemplo $\mathbf{K} = \mathbb{Q}$, $\mathbb{R}$ ó $\mathbb{C}$.
El objetivo es mostrar que existe siempre, y es único, un polinomio de grado $\leq n$ que pasa por $(n+1)$ puntos prefijados del plano $\mathbf{K}^2$ con distintas abcisas. Por ejemplo, en $\mathbb{R}^2$ hay una única recta que pasa por dos puntos, hay una única parábola que pasa por tres puntos con distintas abcisas, a menos que estén alineados, y entonces en lugar de una parábola, pasa una recta, etc.
Este resultado se puede probar de distintas maneras, por ejemplo mediante resultados sencillos de álgebra lineal, usando el conocido determinante de Vandermonde, o aplicando la fórmula de interpolación de Newton (ver por ej. [7]) o, como se expondrá aquí, mediante el polinomio interpolador de Lagrange.
Cabe señalar que si las condiciones iniciales no son sobre $(n+1)$ puntos con distintas abcisas, pero sobre el valor del polinomio y sus n primeras derivadas en un punto $x_0 \in \mathbf{K}$, se recupera el polinomio de Taylor $f(X) = \sum_{k=0}^{n} \frac{f^{(k)}(x_0)}{k!}(X - x_0)^k$.
Y si las condiciones son mezcladas, sobre distintos puntos y sus derivadas, se puede plantear y resolver un sistema lineal dado por las condiciones, o también combinar los polinomios de Taylor y Lagrange.

Teorema 20 (Interpolación de Lagrange) *Sea* $\mathbf{K}$ *un cuerpo de característica cero, y sean* $x_0, \ldots, x_n$ $n+1$ *puntos distintos de* $\mathbf{K}$. *Para cada elección* $y_0, \ldots, y_n$ *de* $n+1$ *puntos cualesquiera de* $\mathbf{K}$ *existe exactamente un polinomio* $f \in \mathbf{K}[X]$ *de grado* $\leq n$ *(si no es nulo) que verifica simultáneamente las condiciones*

$$\begin{cases} f(x_0) &= y_0 \\ f(x_1) &= y_1 \\ & \vdots \\ f(x_n) &= y_n \end{cases}$$

Prueba.–

- Existencia del polinomio interpolador

  La idea es construír uno a uno polinomios f_j $(0 \leq j \leq n)$ de grado $\leq n$ que cumplen las condiciones más sencillas $f_j(x_j) = 1$ y $f_j(x_i) = 0$ si $i \neq j$. Así los polinomios $y_j f_j$ verficarán que $(y_j f_j)(x_j) = y_j$ y $(y_j f_j)(x_i) = 0$ si $i \neq j$, y finalmente el polinomio $f := y_0 f_0 + \cdots + y_n f_n$ cumplirá todos los requisitos, pues $(y_0 f_0 + \cdots + y_n f_n)(x_j) = y_0 f_0(x_j) + \cdots + y_j f_j(x_j) + \cdots + y_n f_n(x_j) = y_j$ para todo $0 \leq j \leq n$.

  Construyamos por ejemplo f_0, los demás se construyen análogamente :

  Las condiciones son : $f_0(x_0) = 1$, $f_0(x_1) = \cdots = f_0(x_n) = 0$. O sea f_0 tiene las n raíces distintas $x_1, \ldots, x_n$. Podemos plantear entonces f_0 como el polinomio de grado n :
  $f_0 = c(X - x_1)\ldots(X - x_n)$ donde $c \in \mathbf{K}$ es una constante a determinar.

  Ahora la condición $f_0(x_0) = 1$ implica que
  $$c = [(x_0 - x_1)\ldots(x_0 - x_n)]^{-1}$$

  De la misma manera se obtiene para cada j :

  $$f_j = \frac{(X - x_0)\ldots(X - x_{j-1})(X - x_{j+1})\ldots(X - x_n)}{(x_j - x_0)\ldots(x_j - x_{j-1})(x_j - x_{j+1})\ldots(x_j - x_n)} = \prod_{\substack{0 \leq i \leq n \\ i \neq j}} \frac{X - x_i}{x_j - x_i}$$

(se observa que el denominador es siempre no nulo pues los x_i son todos distintos)

Finalmente, se define f en la forma :

$$f = y_0 f_0 + \cdots + y_n f_n = \sum_{0 \le j \le n} y_j \prod_{\substack{0 \le i \le n \\ i \ne j}} \frac{X - x_i}{x_j - x_i}$$

Este polinomio f verifica por construcción las condiciones $f(x_j) = y_j$ además de tener grado $\le n$ pues cada sumando tiene grado n (pueden ocurrir eventualmente cancelaciones de manera que se obtiene un polinomio de grado $< n$).

- Unicidad del polinomio interpolador

  Supongamos que existen f y g no nulos de grado $\le n$ que verifican las $n+1$ condiciones $f(x_j) = y_j = g(x_j)$ $(0 \le j \le n)$. Por lo tanto el polinomio $h := f - g$ verifica las $n+1$ condiciones $h(x_j) = 0$, o sea tiene $n+1$ raíces distintas.

  Pero por otro lado, dado que f y g son polinomios de grado $\le n$ (si no nulos), el polinomio h es o bien nulo o bien de grado $\le n$ también. Si fuera no nulo, no podría poseer $n+1$ raíces distintas, por consiguiente tiene que ser el polinomio nulo o sea $f = g$.

■

Ejemplo Calculemos el único polinomio de grado ≤ 3 que verifica las condiciones $f(0) = 1$, $f(1) = 0$, $f(-1) = 4$ y $f(2) = 1$.
Este es :

$$\begin{aligned} f &= 1\frac{(X-1)(X-(-1))(X-2)}{(0-1)(0-(-1))(0-2)} + 0\frac{(X-0)(X-(-1))(X-2)}{(1-0)(1-(-1))(1-2)} + \\ &\quad +4\frac{(X-0)(X-1)(X-2)}{(-1-0)(-1-1)(-1-2)} + 1\frac{(X-0)(X-1))(X-(-1))}{(2-0)(2-1)(2-(-1))} \\ &= \frac{(X-1)(X+1)(X-2)}{2} + 4\frac{X(X-1)(X-2)}{-6} + \frac{X(X-1)(X+1)}{6} \\ &= \frac{1}{2}(X^3 - 2X^2 - X + 2) - \frac{2}{3}(X^3 - 3X^2 + 2X) + 16(X^3 - X) \\ &= X^2 - 2X + 1 \end{aligned}$$

■

Este sencillo ejemplo muestra por un lado que es mejor no acordarse la fórmula de memoria, sino ser capaz de reconstruirla, y por otro lado que por más que se trate de un polinomio de grado chico, la cantidad de cuentas necesarias para obtener de esa manera el polinomio interpolador de Lagrange es muy elevada !

3 Polinomios en $\mathbb{C}[X]$

3.1 Teorema Fundamental del Algebra

Este teorema es debido a Gauss (1777-1855) quién dió de él cinco demostraciones distintas. Actualmente, existen decenas de demostraciones, algunas usan Análisis Complejo, otras Teoría de Cuerpos o Topología, todas fuera del alcance de estas notas. Pero cabe mencionar que no se conoce demostración que no use en alguna medida resultados elementales de análisis, en particular el Teorema de Bolzano, que dice que si una función continua definida de $\mathbb{R}$ en $\mathbb{R}$ cambia de signo en los extremos de un intervalo, entonces tiene un cero en el interior del intervalo.

Teorema 21 (Teorema Fundamental del Algebra) *Sea $f \in \mathbb{C}[X]$ un polinomio no nulo con coeficientes complejos de grado n mayor o igual que 1. Entonces f tiene por lo menos una raíz en $\mathbb{C}$, o equivalentemente, f tiene exactamente n raíces contadas con su multiplicidad.*
Esto significa que la factorización de $f \in \mathbb{C}[X]$ es siempre de la forma :

$$f = c\,(X-\alpha_1)^{k_1} \dots (X-\alpha_m)^{k_m}, \quad c \in \mathbb{C} \setminus \{0\},$$

y que los únicos polinomios irreducibles en $\mathbb{C}[X]$ son los de grado 1.

Más ejemplos

- f de grado 3 : (Scipione del Ferro 1515, Tartaglia 1535, Cardano 1545)

  $$f = aX^3 + bX^2 + cX + d \ \in \mathbb{C}[X]\,,\ a \neq 0\,.$$

  Haciendo el cambio de variables $Y = X - \frac{b}{3a}$, se pasa a buscar las raíces del polinomio :

  $$g = Y^3 + pY + q$$

  Buscando las soluciones de la forma $Y = U + V$, con $U^3 + V^3 = -q$ y $U^3V^3 = -\frac{p^3}{27}$, se observa que U^3 y V^3 son las raíces del polinomio (resolvente) :

  $$Z^2 + qZ - \tfrac{p^3}{27}\,.$$

  Se obtienen finalmente las tres soluciones complejas de g entre las 6 expresiones :

  $$U+V = \left(-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}\right)^{1/3} + \left(-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}\right)^{1/3}$$

  (pues hay 3 elecciones posibles para cada raíz cúbica en $\mathbb{C}$.)

  Para determinar las tres raíces de g, se eligen las raíces cúbicas de tal manera que $UV = -p/3$.

- f de grado 4 : (Ferrari)

  $$f + X^4 + pX^2 + qX + r$$

  Las 4 raíces son del tipo $\alpha = \frac{1}{2}(\pm\sqrt{-\beta} \pm \sqrt{-\gamma} \pm \sqrt{-\delta})$, donde $\beta,\ \gamma,\ \delta$ son las tres raíces del polinomio (resolvente) :

  $$Z^3 - 2pZ^2 + (p^2 - 4r)Z + q^2$$

  La condición aquí para elegir las 4 raíces complejas entre las 8 posibles expresiones es $(\pm\sqrt{-\beta})(\pm\sqrt{-\gamma})(\pm\sqrt{-\delta}) = -q$.

■

Hasta ahora se obtuvieron las raíces complejas de polinomios $f \in \mathbb{C}[X]$ de grado ≤ 4, por medio de fórmulas que se obtienen a partir de los coeficientes del polinomio f mediante las operaciones $+,\ -,\ \cdot,\ /$ y $\sqrt{\ }$, $\sqrt[3]{\ }$ etc.
La pregunta natural es entonces : ¿ Existirá para cada polinomio f de grado arbitrario una fórmula para las raíces que involucre los coeficientes de f y las operaciones $+,\ -,\ \cdot,\ /$ y $\sqrt[k]{\ }$ para algunos $k \in \mathbb{N}$?
La respuesta es NO :

Teorema 22 (Abel, 1802-1829) *No hay una fórmula que describa las raíces de un polinomio general cualquiera f de grado ≥ 5 a partir de sus coeficientes y de las operaciones elementales descritas más arriba.*

Galois (1811-1832) caracterizó cuáles eran los polinomios de grado ≥ 5 para los cuales existe tal fórmula, aunque no es facilmente deducible de los coeficientes del polinomio, sino que tiene que ver con cierto grupo asociado con dicho polinomio.

3.2 Ubicación de las raíces

A pesar de no poder obtener en general las raíces de un polinomio $f \in \mathbb{C}[X]$ por medio de una fórmula, uno puede exhibir una cota M para el módulo de las raíces, que depende de los coeficientes de f :

Proposición 23 (Cota de Cauchy, 1789-1857) *Sea* $f = a_n X^n + \cdots + a_0 \in \mathbb{C}[X]$, *con* $n \geq 1$, $a_n \neq 0$.
Sea $M := 1 + \left|\frac{a_{n-1}}{a_n}\right| + \cdots + \left|\frac{a_0}{a_n}\right|$. *Entonces toda raíz* $\alpha \in \mathbb{C}$ *de* f *verifica que* $|\alpha| < M$.

Prueba.–

- Si $|\alpha| < 1$, no hay nada que probar pues $1 \leq M$ por definición.
- Para $|\alpha| \geq 1$, se observa que

$$\begin{aligned} f(\alpha) = 0 &\iff a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 = 0 \\ &\iff a_n\left(\alpha^n + \frac{a_{n-1}}{a_n}\alpha^{n-1} + \cdots + \frac{a_0}{a_n}\right) = 0 \\ &\iff \alpha^n + \frac{a_{n-1}}{a_n}\alpha^{n-1} + \cdots + \frac{a_0}{a_n} = 0 \end{aligned}$$

  Por lo tanto,

$$\begin{aligned} \alpha^n &= -\left(\frac{a_{n-1}}{a_n}\alpha^{n-1} + \cdots + \frac{a_0}{a_n}\right) \\ \Longrightarrow \quad |\alpha|^n &= \left|\frac{a_{n-1}}{a_n}\alpha^{n-1} + \cdots + \frac{a_0}{a_n}\right| \\ &\leq \left|\frac{a_{n-1}}{a_n}\right||\alpha|^{n-1} + \cdots + \left|\frac{a_0}{a_n}\right| \\ &\leq |\alpha|^{n-1}\left(\left|\frac{a_{n-1}}{a_n}\right| + \cdots + \left|\frac{a_0}{a_n}\right|\right) \end{aligned}$$

  pues para $|\alpha| \geq 1$, se tiene $|\alpha|^{n-1} \geq |\alpha|^k$ para todo k, $1 \leq k \leq n$.
  Así se concluye que $|\alpha| \leq \left|\frac{a_{n-1}}{a_n}\right| + \cdots + \left|\frac{a_0}{a_n}\right|$ y por lo tanto, $|\alpha| < M$.

■

Existen otras cotas M para el módulo de las raíces más precisas, aunque más dificiles de obtener. Estas se pueden consultar por ejemplo en [5].

4 Polinomios en $\mathbb{Q}[X]$

4.1 Revisión de resultados

- Un polinomo en $\mathbb{Q}[X]$ de grado $n \geq 1$ tiene a lo sumo n raíces contadas con multiplicidad.
- Sea $f \in \mathbb{Q}[X]$ de grado ≥ 2. Si f tiene una raíz, entonces f es reducible.
- $f \in \mathbb{Q}[X]$ reducible no implica que f tiene raíces en $\mathbb{Q}$. Por ejemplo el polinomio $(X^2-2)^n$ es reducible y sin raíces racionales.
- $f \in \mathbb{Q}[X]$ de grado 2 ó 3 es reducible si y sólo si tiene una raíz en $\mathbb{Q}$ (pues por cuestiones de grado, si es reducible tiene que tener al menos un factor de grado 1).

4.2 Cálculo de raíces en $\mathbb{Q}$

A pesar de que la situación en $\mathbb{Q}[X]$ parece mucho más complicada que en $\mathbb{C}[X]$, se puede encontrar todas las raíces racionales de un polinomio $f \in \mathbb{Q}[X]$ por medio de un algoritmo. Este hecho es una consecuencia de que todo número entero $a \in \mathbb{Z} \setminus \{0\}$ tiene un número finito de divisores posibles, que se pueden calcular.

Sea $f = a_n X_n + \cdots + a_0 \in \mathbb{Q}[X]$. Entonces existe $c \in \mathbb{Z} \setminus \{0\}$ tal que $g = cf$ tiene todos sus coeficientes enteros (por ejemplo, eligiendo c como el mínimo común múltiplo de los denominadores de los coeficientes de f), y además las raíces de f claramente coinciden con las de g.
Por ejemplo, $f = \frac{3}{2}X^5 - \frac{1}{3}X^4 + X^2 - \frac{5}{4} \in \mathbb{Q}[X]$ y $g = 12f = 18X^5 - 4X^4 + 12X^2 - 15 \in \mathbb{Z}[X]$ tienen exactamente las mismas raíces.
Por consiguiente para encontrar las raíces racionales de un polinomio en $\mathbb{Q}[X]$, nos podemos restringir a estudiar como encontrar las raíces racionales de un polinomio en $\mathbb{Z}[X]$.

Lema 24 (Gauss) *Sea $f = a_n X^n + \cdots + a_0 \in \mathbb{Z}[X]$ con $a_n,\ a_0 \neq 0$. Entonces, si $\frac{\alpha}{\beta} \in \mathbb{Q}$ es una raíz racional de f, con α y $\beta \in \mathbb{Z}$ coprimos, obligatoriamente resulta que $\alpha \,|\, a_0$ y $\beta \,|\, a_n$.*

Prueba.–

$$\begin{aligned} f\left(\frac{\alpha}{\beta}\right) = 0 &\iff a_n \left(\frac{\alpha}{\beta}\right)^n + a_{n-1}\left(\frac{\alpha}{\beta}\right)^{n-1} + \cdots + a_1\left(\frac{\alpha}{\beta}\right) + a_0 = 0 \\ &\iff \frac{a_n\alpha^n + a_{n-1}\alpha^{n-1}\beta + \cdots + a_1\alpha\beta^{n-1} + a_0\beta^n}{\beta^n} = 0 \\ &\iff a_n\alpha^n + a_{n-1}\alpha^{n-1}\beta + \cdots + a_1\alpha\beta^{n-1} + a_0\beta^n = 0 \end{aligned}$$

Luego, $\alpha\left(a_n\alpha^{n-1} + \cdots + a_1\beta^{n-1}\right) = -a_0\beta^n$.
Por lo tanto, $\alpha \,|\, -a_0\beta^n$, pero al ser α y β enteros coprimos, α no tiene ningún factor en común con β^n, o sea $\alpha \,|\, a_0$.
De la misma manera, $\beta\left(a_{n-1}\alpha^{n-1} + \cdots + a_0\beta^{n-1}\right) = -a_n\alpha^n$ implica que $\beta \,|\, -a_n\alpha^n$ pero al ser coprimo con α, resulta $\beta \,|\, a_n$.

■

Aplicación (Algoritmo para calcular las raíces racionales de un polinomio entero) En las condiciones del teorema anterior, el Lema de Gauss implica que si se construye el conjunto (finito) $\mathcal{N}$ de los divisores positivos y negativos de a_0 y el conjunto $\mathcal{D}$ de los de a_n, las raíces del polinomio f se encuentran en el conjunto de todas las fracciones coprimas $\frac{\alpha}{\beta}$, eligiendo α en $\mathcal{N}$ y β en $\mathcal{D}$. Chequeando para cada fracción $\frac{\alpha}{\beta}$ así construída si $f(\frac{\alpha}{\beta}) = 0$, se obtienen todas las raíces racionales de f.
Simplemente hay que tener un poco de cuidado en que este procedimiento no aclara la multiplicidad de cada raíz.

Ejemplo Hallemos las raíces racionales del polinomio racional

$$f = X^8 + \frac{8}{3}X^7 + \frac{1}{3}X^6 - \frac{14}{3}X^5 - \frac{14}{3}X^4 - \frac{4}{3}X^3.$$

Limpiando los denominadores de f se obtiene el polinomio entero g con las mismas raíces :

$$g = 3X^8 + 8X^7 + X^6 - 14X^5 - 14X^4 - 4X^3 = X^3(3X^5 + 8X^4 + X^3 - 14X^2 - 14X - 4)$$

Claramente, 0 es raíz de multiplicidad 3 de g (y de f), y las restantes raíces racionales son las de

$$h = 3X^5 + 8X^4 + X^3 - 14X^2 - 14X - 4$$

Aquí, $a_0 = -4$ y $a_n = 3$.
Los divisores de a_0 son $\pm 1, \pm 2, \pm 4$ y los divisores de a_n son $\pm 1, \pm 3$, luego las raíces racionales se buscan en el conjunto :

$$\{\pm 1, \pm 2, \pm 4, \pm\frac{1}{3}, \pm\frac{2}{3}, \pm\frac{4}{3}\}$$

Chequeando uno obtiene que $h(-1) = 0$ y $h(-2/3) = 0$.
Así, las raíces racionales distintas de h son -1 y $-2/3$, Para conocer con qué multiplicidad, se puede o bien dividir h por $(X+1)(X+\frac{2}{3})$ y volver a evaluar el cociente en -1 y $-2/3$. O bien también se puede derivar h :
$h' = 15X^4 + 32X^3 + 3X^2 - 28X - 14$ y se tiene que $h'(-1) = 0$ mientras que $h'(-2/3) \neq 0$.
O sea -1 es raíz de multiplicidad ≥ 2 y $-2/3$ es raíz simple.
Volviendo a derivar h : $h'' = 60X^3 + 96X + 6X - 28$ y $h''(-1) \neq 0$.
Se concluye que -1 es raíz doble de h.
Finalmente la factorización de h en $\mathbb{Q}[X]$ es :

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

Y dado que $f = \frac{1}{3}X^3\, h$, resulta la siguiente factorización de f en $\mathbb{Q}[X]$:

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

■

Observación 25 *El Lema de Gauss provee un algoritmo para calcular todas las raíces racionales de un polinomio racional, pero se ve claramente que éste es extremadamente costoso, pues hay que evaluar el polinomio de entrada en un gran número de fracciones $\frac{\alpha}{\beta}$ (la cantidad de fracciones está relacionada con la cantidad de divisores de a_0 y a_n).*

4.3 Irreducibilidad en $\mathbb{Q}[X]$

El objetivo de este párrafo es dar un criterio que permite probar la irreducibilidad de ciertos polinomios en $\mathbb{Q}[X]$, y mostrar que existen polinomios irreducibles de cualquier grado. Para ello necesitaremos previamente relacionar factorizaciones en $\mathbb{Q}[X]$ con factorizaciones en $\mathbb{Z}[X]$.
Dado que $f \in \mathbb{Q}[X]$ es reducible si y sólo si cf es reducible, para todo $c \in \mathbb{Q} \setminus \{0\}$, se pueden limpiar denominadores y restringirse a analizar la reducibilidad en $\mathbb{Q}[X]$ de polinomios con coeficientes enteros.

Definición 26 *Sea $f = a_n X^n + \cdots + a_0 \in \mathbb{Z}[X]$ un polinomio no nulo con coeficientes enteros. Se define el contenido de f como el máximo común divisor de los coeficientes de f ; es decir el contenido de f es el número entero*

$$\text{cont}(f) := \text{mcd}(a_0; \ldots; a_n)$$

En caso en que $\text{cont}(f) = 1$ se dice que el polinomio f es primitivo.

Observemos que por la definición de contenido, resulta inmediatamente que si $f \in \mathbb{Z}[X]$ y $c \in \mathbb{Z} \setminus \{0\}$, entonces $\text{cont}(cf) = c\,\text{cont}(f)$, y que $f = \text{cont}(f)\,\overline{f}$ donde $\overline{f} \in \mathbb{Z}[X]$ es un polinomio primitivo.

Lema 27 (Gauss) *Sean* $f,\ g \in \mathbb{Z}[X]$, *entonces*

1. *Si* f *y* g *son polinomios primitivos, entonces* $f\,g$ *también lo es.*
2. $\text{cont}(fg) = \text{cont}(f)\text{cont}(g)$

Prueba.–

1. Sean f y g primitivos e investiguemos si existe algún primo p que pueda dividir a $\text{cont}(fg)$:
   Pongamos $f = a_n X^n + \cdots + a_0$ y $g = b_m X^m + \cdots + b_0$.
   Al ser f y g primitivos, $p \not| \text{cont}(f)$ y $p \not| \text{cont}(g)$. Por lo tanto, existen a_i y b_j no divisibles por el primo p. Sean $i_0 := \min\{\, i \,/\, p \not| a_i \,\}$ y $j_0 := \min\{\, j \,/\, p \not| b_j \,\}$
   y estudiemos el coeficiente $c_{i_0+j_0}$ del producto fg:
   $$c_{i_0+j_0} = a_{i_0+j_0}b_0 + \cdots + a_{i_0+1}b_{j_0-1} + a_{i_0}b_{j_0} + a_{i_0-1}b_{j_0+1} + \cdots + a_0 b_{i_0+j_0}$$
   Por la definición de i_0 y j_0, se observa que $p \,|\, a_0, \ldots, p \,|\, a_{i_0-1}$ y $p \,|\, b_0, \ldots, p \,|\, b_{j_0-1}$, es decir p divide a todos los términos de la derecha de la igualdad salvo eventualmente $a_{i_0}b_{j_0}$. Además $p \not| a_{i_0}$ y $p \not| b_{i_0}$, por lo tanto, dado que p es primo, $p \not| a_{i_0}b_{j_0}$. En definitiva, $p \not| c_{i_0+j_0}$ (pues sino tendría que dividir a $a_{i_0}b_{j_0}$), o sea $p \not| \text{cont}(fg)$.
   Se probó que no puede existir ningún primo p que divida al contenido de fg y por consiguiente, $\text{cont}(fg) = 1$ como se quería mostrar.
2. Sean $f = \text{cont}(f)\,\overline{f}$ y $g = \text{cont}(g)\,\overline{g}$, con $\overline{f},\ \overline{g} \in \mathbb{Z}[X]$ primitivos.
   Se tiene $fg = \text{cont}(f)\text{cont}(g)\overline{f}\,\overline{g}$. Luego, $\text{cont}(fg) = \text{cont}\left(\text{cont}(f)\text{cont}(g)\,\overline{f}\,\overline{g}\right) =$
   $= \text{cont}(f)\text{cont}(g)\,\text{cont}(\overline{f}\,\overline{g})$. Pero por (1), $\text{cont}(\overline{f}\,\overline{g}) = 1$ con lo que concluye la prueba.

■

El paso siguiente es mostrar que si un polinomio entero se escribe como el producto de dos polinomios racionales, entonces también se puede reescribir como el producto de dos polinomios enteros :

Teorema 28 *Sea* $f \in \mathbb{Z}[X]$ *y supongamos que existen polinomios* $g,\ h \in \mathbb{Q}[X]$ *tales que* $f = gh$. *Entonces existen polinomios* $\tilde{g}\,,\ \tilde{h}$ *que verifican simultáneamente :*

- $\tilde{g},\ \tilde{h}\ \in \mathbb{Z}[X]$
- $f = \tilde{g}\tilde{h}$
- $\text{gr}(\tilde{g}) = \text{gr}(g)$ *y* $\text{gr}(\tilde{h}) = \text{gr}(h)$

Prueba.– Para simplificar las notaciones, observemos primero que alcanza con probar el resultado para un polinomio $f \in \mathbb{Z}[X]$ primitivo, ya que $\text{cont}(f) \in \mathbb{Z}$ se puede poner en factor.
Supongamos entonces que f es primitivo. La idea ahora es simplemente que dado que f es un polinomio entero que se escribe como producto de dos polinomios racionales g y h , debe haber una forma de redistribuir los denominadores de g y h de manera que se cancelen :
En efecto, sean $b, c \in \mathbb{Z} \setminus \{0\}$ tales que $b\,g$ y $c\,h$ pertenezcan a $\mathbb{Z}[X]$, entonces :
$bc\,f = (b\,g)\,(c\,h)$, y por consiguiente $b\,c = \text{cont}(bc\,f) = \text{cont}((b\,g)\,(c\,h)) = \text{cont}(b\,g)\,\text{cont}(c\,h)$
(recordemos que $\text{cont}(b\,g) \neq b\,\text{cont}(g)$ porque g no es en principio un polinomio con coeficientes enteros, y lo mismo para $c\,h$)

Luego, si escribimos $b\,g = \mathrm{cont}(b\,g)\overline{b\,g}$ y $c\,h = \mathrm{cont}(c\,h)\overline{c\,h}$, con $\overline{b\,g}$, $\overline{c\,h} \in \mathbb{Z}[X]$ primitivos, se tiene que $f = \overline{b\,g}\,\overline{c\,h}$ y por lo tanto alcanza con definir :

$$\tilde{g} = \overline{b\,g} \qquad \text{y} \qquad \tilde{h} = \overline{c\,h}.$$

Es inmediato verificar que éstos polinomios verifican las condiciones del teorema.

■

Finalmente, estamos en condiciones de probar el siguiente criterio de irreducibilidad para polinomios enteros :

Teorema 29 (Criterio de irreducibilidad de Eisenstein)
Sea $f \in \mathbb{Z}[X]$, $f = a_n X^n + \cdots + a_0$ *tal que existe un primo* p *que verifica* $p \not| a_n$, $p \,|\, a_i$ *para* $0 \le i \le n-1$ *y* $p^2 \not| a_0$, *entonces* f *es irreducible en* $\mathbb{Q}[X]$.

Prueba.– Supongamos que f es reducible en $\mathbb{Q}[X]$, es decir que existen $g, h \in \mathbb{Q}[X]$ tal que $f = g\,h$ y $1 \le \mathrm{gr}(g) < \mathrm{gr}(f)$. Por el teorema anterior, podemos suponer que g y h son polinomios con coeficientes enteros.
Pongamos $g = b_d X^d + \cdots + b_0$ y $h = c_e X^e + \cdots + c_0 \in \mathbb{Z}[X]$, donde $1 \le d, e < n$.
Dado que $f = g\,h$, las hipótesis implican que $p \,|\, b_0 c_0$ pero $p^2 \not| b_0 c_0$. Por lo tanto p divide a uno de los factores exactamente. Sin pérdida de generalidad, podemos suponer que $p \,|\, b_0$ y $p \not| c_0$.
Probaremos inductivamente que en tal caso, p divide a todos los coeficientes de g :
Para $1 \le i \le \mathrm{gr}(g) - 1$, supongamos que $p \,|\, b_0$, $p \,|\, b_1$, $\ldots$, $p \,|\, b_i$ y veamos que entonces $p \,|\, b_{i+1}$:
La igualdad $f = g\,h$ implica que $a_{i+1} = b_0 c_{i+1} + \cdots + b_i c_1 + b_{i+1} c_0$.
Por hipótesis inductiva, p divide a todos los primeros factores de la derecha de la igualdad, y por otro lado, dado que $i + 1 \le \mathrm{gr}(g) < \mathrm{gr}(f)$, se tiene por la hipótesis del teorema que $p \,|\, a_{i+1}$. Por lo tanto $p \,|\, b_{i+1} c_0$. Pero $p \not| c_0$, en consecuencia $p \,|\, b_{i+1}$ como se quería probar.
Así, $p \,|\, \mathrm{cont}(g)$, y por lo tanto $p \,|\, \mathrm{cont}(g)\,\mathrm{cont}(h) = \mathrm{cont}(g\,h) = \mathrm{cont}(f)$, lo que contradice el hecho que $p \not| a_n$. La contradicción proviene de suponer que f es reducible.

■

Corolario 30 *Existen polinomios irreducibles de cualquier grado en* $\mathbb{Q}[X]$. *Por ejemplo el polinomio* $X^n - 2$ *es irreducible en* $\mathbb{Q}[X]$ *para todo* $n \in \mathbb{N}$.

4.4 Factorización en $\mathbb{Q}[X]$

Como hemos visto en la sección anterior, para factorizar un polinomio en $\mathbb{Q}[X]$, dado que las constantes no influyen, alcanza con considerar el polinomio en $\mathbb{Z}[X]$ obtenido limpiando los denominadores. Y para factorizar en $\mathbb{Q}[X]$ un polinomio con coeficientes enteros, se puede intentar reducirlo paso a paso hasta obtener todos factores irreducibles, pero siempre trabajando con factores en $\mathbb{Z}[X]$ (Teorema 28).
Un algoritmo clásico, debido a Kronecker(1823,1891), y muy sencillo teóricamente (aunque terriblemente costoso de implementar computacionalmente) que permite factorizar en $\mathbb{Q}[X]$ un polinomio con coeficientes enteros se basa en la idea siguiente :

Si $f \in \mathbb{Z}[X]$ es reducible en $\mathbb{Q}[X]$ entonces existen g, $h \in \mathbb{Z}[X]$ de grados estrictamente menores que el de f de manera que $f = gh$, y podemos suponer sin pérdida de generalidad que $\mathrm{gr}(g) \le \mathrm{gr}(f)/2$.
Ahora, si $g \in \mathbb{Z}[X]$ tiene grado $\le \mathrm{gr}(f)/2$, por el Teorema 20 de interpolación, queda exactamente determinado por su valor en $[\mathrm{gr}(f)/2] + 1$ puntos (donde $[\mathrm{gr}(f)/2]$ denota la parte entera, i.e. el mayor entero, $\le \mathrm{gr}(f)/2$). Por otro lado, para todo $k \in \mathbb{Z}$ se verifica $f(k) = g(k)h(k)$, o sea que $g(k) \,|\, f(k)$.

El algoritmo es por lo tanto el siguiente :

Algoritmo de factorización de Kronecker

- Se evalúa el polinomio f en $m := [\mathrm{gr}(f)/2] + 1$ puntos enteros $k_1, \ldots, k_m$, obteniendo $r_1 = f(k_1), \ldots, r_m = f(k_m)$.
- Se computan todos los divisores positivos y negativos de cada uno de los valores $r_1, \ldots, r_m$ obtenidos.
- Para cada elección de m divisores $d_1, \ldots, d_m$, se chequea si el polinomio g que interpola $(k_1, d_1), \ldots, (k_m, d_m)$ es efectivamente un factor del polinomio f.
- Si no lo es, se pasa a otra elección de divisores, mientras que si lo es, se repite el procedimiento con g y $\frac{f}{g}$.
- Si para ninguna elección de divisores se obtiene que $g \mid f$ eso significa que el polinomio f es irreducible.

Ejemplo Sea $f = X^5 - X^3 + X^2 - 2X - 2$
Si f es es reducible tiene un factor $g \in \mathbb{Z}[X]$ de grado ≤ 2, que será determinado por su valor en tres puntos.
(Observemos que por el Lema de Gauss (Lema 27), las posibles raíces racionales de f son ± 2, pero $f(\pm 2) \neq 0$, por lo tanto f no tiene raíces racionales, o sea $\mathrm{gr}(g) = 2$.)
Elijamos por ejemplo los puntos de interpolación $k_1 = 0$, $k_2 = 1$ y $k_3 = -1$: se tiene $f(0) = -2$, $f(1) = -3$ y $f(-1) = 1$, por lo tanto $g(0) \in \{\pm 1, \pm 2\}$, $g(1) \in \{\pm 1, \pm 3\}$ y $g(-1) \in \{\pm 1\}$. Esto indica que tenemos en principio que calcular 32 posibles polinomios g y chequear si son efectivamente divisores de f.

- Por ejemplo, si elegimos para g los puntos de interpolación $(0,1), (1,1)$ y $(-1,1)$, obtenemos claramente el polinomio $g = 1$ que no aporta ningún factor esencial para la factorización de f.
- Eligiendo los puntos $(0,1), (1,1)$ y $(-1,-1)$ se obtiene el polinomio de interpolación :

$$\begin{aligned} g &= 1\frac{(X-1)(X+1)}{(-1)(1)} + 1\frac{X(X+1)}{(1)(1+1)} - 1\frac{X(X-1)}{(-1)(-1-1)} \\ &= -(X^2-1) + \frac{X^2+X}{2} - \frac{X^2-X}{2} \\ &= -X^2 + X + 1 \end{aligned}$$

  Y este polinomio g no divide f pues al dividir da resto $2X + 1$.

- Finalmente, al ir chequeando todas las posibles ternas, se llega a los puntos de interpolación $(0,-2), (1,-1)$ y $(-1,-1)$ que arrojan el polinomio

$$\begin{aligned} g &= -2\frac{(X-1)(X+1)}{(-1)(1)} - 1\frac{X(X+1)}{(1)(1+1)} - 1\frac{X(X-1)}{(-1)(-1-1)} \\ &= 2(X^2-1) - \frac{X^2+X}{2} - \frac{X^2-X}{2} \\ &= X^2 - 2 \end{aligned}$$

  y se verifica que $X^2 - 2 \mid f$, con cociente $X^3 + X + 1$.

Ahora bien, X^2-2 y X^3+X+1 son ambos irreducibles pues f no tiene raíces en $\mathbb{Q}$. Así, la factorización de f en $\mathbb{Q}[X]$ es la siguiente :

$$X^5-X^3+X^2-2X-2=(X^2-2)(X^3+X+1)$$

■

Se observa que este algoritmo puede ser extremadamente lento ya que por más que los valores de $f(k_i)$ sean lo más simples posibles, tienen cada uno por lo menos 2 divisores (correspondientes a ± 1) y por lo menos tendremos que calcular y chequear $2^{[\mathrm{gr}(f)/2]+1}$ polinomios g.
Hubo posteriormente grandes mejoras en cuanto a la velocidad de los algoritmos de factorización en $\mathbb{Q}[X]$.
El primero de ellos, debido a H.Zassenhaus ([8], 1969), se basa esencialmente en un algoritmo de E.Berlekamp para factorizar rápidamente polinomios en cuerpos finitos ([1], 1967). El algoritmo requiere en promedio un número de operaciones del orden de $\mathrm{gr}(f)^c$, donde c es una constante calculada, aunque en el peor de los casos puede necesitar un número exponencial en $\mathrm{gr}(f)$ operaciones como en el algoritmo expuesto más arriba.
El algoritmo más eficiente en la actualidad (por lo menos en teoría), conocido como algoritmo L^3, es debido a A.K.Lenstra, H.Lenstra y L.Lovász ([4], 1982), y establece exactamente lo siguiente :

Teorema 31 *(L^3) Sea $f=a_nX^n+\cdots+a_0\in\mathbb{Z}[X]$ un polinomio primitivo, y sea H una cota superior para los módulos de los coeficientes a_i. Entonces, se puede factorizar f en $\mathbb{Q}[X]$ realizando del orden de $n^{12}+n^9(\log_2 H)^3$ operaciones "bit" (es decir los números se representan en base 2, y se cuenta una operación cada vez que se suma,resta, multiplica o divide un bit "0" ó "1").*

Este es el primer algoritmo polinomial que existe para factorizar en $\mathbb{Q}[X]$ polinomios racionales, donde polinomial significa que si el polinomio de entrada se mide a través de su grado n y del tamaño de sus coeficientes en representación binaria $\log_2 H$, la cantidad total de operaciones a realizar es un polinomio en n y $\log_2 H$, y no del tipo 2^n como lo era hasta entonces.
La descripción y la demostración de los algoritmos de Berlekamp y L^3 quedan fuera de nuestro alcance, y utilizan fundamentalmente en el primer caso la reducción a factorizar polinomios módulo p para p primo, y en el segundo caso la teoría de látices o reticulados en $\mathbb{Z}^n$.

5 Polinomios en $\mathbb{R}[X]$

5.1 Revisión de resultados

- Un polinomio en $\mathbb{R}[X]$ de grado $n\geq 1$ tiene a lo sumo n raíces contadas con multiplicidad.
- Sea $f\in\mathbb{R}[X]$ de grado ≥ 2. Si f tiene una raíz, entonces f es reducible.
- $f\in\mathbb{R}[X]$ reducible no implica que f tenga raíces en $\mathbb{R}$. Por ejemplo el polinomio $(X^2+1)^n$ es reducible y sin raíces reales.
- $f\in\mathbb{R}[X]$ de grado 2 ó 3 es reducible si y sólo si tiene una raíz en $\mathbb{R}$ (pues por cuestiones de grado, si es reducible tiene que tener al menos un factor de grado 1).

Pero se puede probar que en $\mathbb{R}[X]$ no existen polinomios irreducibles de cualquier grado :

5.2 Polinomios irreducibles en $\mathbb{R}[X]$

Proposición 32 *Todo polinomio en $\mathbb{R}[X]$ de grado impar tiene al menos una raíz real*

Prueba.– Sea $f = a^n X^n + \cdots + a_0 \in \mathbb{R}[X]$, con n impar.
Si $a_n > 0$, entonces :

$$\lim_{x\to+\infty} f(x) = +\infty \qquad \text{y} \qquad \lim_{x\to-\infty} f(x) = -\infty$$

Y si $a_n < 0$ se tiene :

$$\lim_{x\to+\infty} f(x) = -\infty \qquad \text{y} \qquad \lim_{x\to-\infty} f(x) = +\infty$$

En ambos casos los signos son opuestos, y por lo tanto, por el Teorema de Bolzano (y dado que $f : \mathbb{R} \to \mathbb{R}$ define una función continua), debe existir $\alpha \in \mathbb{R}$ tal que $f(\alpha) = 0$

■

Pero se puede ser más explícito y precisar mejor cuántas raíces reales puede tener f.

Teorema 33 *Sea $f \in \mathbb{R}[X]$, y sea $z \in \mathbb{C} \setminus \mathbb{R}$ un número complejo no real. Entonces*

1. $f(z) = 0 \iff f(\overline{z}) = 0$
2. *z es raíz de multiplicidad k de f $\iff$ $\overline{z}$ es raíz de multiplicidad k de f.*

Prueba.–

1. Sea $f = a_n X^n + \cdots + a_0 \in \mathbb{R}[X]$, entonces

$$\begin{aligned} f(z) = 0 &\iff a_n z^n + \cdots + a_1 z + a_0 = 0 \\ &\iff \overline{a_n z^n + \cdots + a_1 z + a_0} = 0 \\ &\iff \overline{a_n}\,\overline{z}^n + \cdots + \overline{a_1}\,\overline{z} + \overline{a_0} = 0 \\ &\iff a_n \overline{z}^n + \cdots + a_1 \overline{z} + a_0 = 0 \\ &\iff f(\overline{z}) = 0 \end{aligned}$$

   (pues para todo i, $\overline{a_i} = a_i$ por ser a_i real).

2. z raíz de multiplicidad k de $f \iff f(z) = f'(z) = \cdots = f^{(k-1)}(z) = 0$ y $f^{(k)}(z) \neq 0$
   Pero $f', \ldots, f^{(k-1)}$, $f^{(k)}$ también son polinomios en $\mathbb{R}[X]$ y por lo tanto, por (1):
   $f(z) = \cdots = f^{(k-1)}(z) = 0$ y $f^{(k)}(z) \neq 0 \iff f(\overline{z}) = \cdots = f^{(k-1)}(\overline{z}) = 0$ y $f^{(k)}(\overline{z}) \neq 0$
   $\iff$ $\overline{z}$ raíz de multiplicidad k de f

■

El teorema anterior significa que las raíces complejas no reales de un polinomio real f vienen de a pares de complejos conjugados, o sea que un polinomio real f de grado n, que tiene exactamente n raíces complejas contadas con multiplicidad, tiene un número par de ellas que son complejas no reales y el resto son reales. Por ejemplo, un polinomio real de grado impar tiene un número impar de raíces reales.

La Observación siguiente nos permitirá caracterizar los polinomios irreducibles de $\mathbb{R}[X]$:

Observación 34 *Sean $z, \overline{z}$ números complejos conjugados, entonces el polinomio $(X-z)(X-\overline{z})$ es un polinomo real (pues $(X-z)(X-\overline{z}) = X^2 - 2\mathrm{Re}(z) + |z|^2 \in \mathbb{R}[X]$).*

Proposición 35 (Polinomios irreducibles en $\mathbb{R}[X]$) *Los polinomios irreducibles en* $\mathbb{R}[X]$ *son exactamente los de grado 1 y aquéllos de grado 2 con discriminante negativo.*

Prueba.– Claramente los polinomios de grado 1 y los de grado 2 con discriminante negativo son irreducibles.
Recíprocamente, si f tiene grado impar > 1 tiene por lo menos una raíz y por lo tanto es reducible.
Si f es de grado 2, es reducible si y solo si tiene discriminante ≥ 0.
Si f tiene grado par ≥ 4, o bien tiene alguna raíz real y en tal caso es reducible, o bien todas sus raíces son complejas no reales y vienen de a pares conjugados, por lo tanto si z es una de esas raíces, el polinomio real $(X - z)(X - \overline{z})$ divide a f en $\mathbb{R}[X]$ y f resulta reducible también.

■

Corolario 36 (Factorización en $\mathbb{R}[X]$) *La factorización en irreducibles de un polinomio* $f \in \mathbb{R}[X]$ *es siempre de la forma :*

$$f = c(X - \alpha_1)^{k_1} \dots (X - \alpha_r)^{k_r} (X^2 + \beta_1 X + \gamma_1)^{j_1} \dots (X^2 + \beta_s X + \gamma_s)^{j_s}$$

con r *ó* s *eventualmente nulos,* $k_i, j_\ell \geq 1$ $(1 \leq i \leq r, 1 \leq \ell \leq s)$ *y* ${\beta_\ell}^2 - 4\gamma_\ell < 0$.

5.3 Cantidad de raíces reales de un polinomio en $\mathbb{R}[X]$

Sabemos que $f \in \mathbb{R}[X]$ de grado $n \geq 1$ tiene exactamente n raíces complejas (contadas con multiplicidad). También sabemos que si $\text{gr}(f) \geq 5$, no existe una fórmula general para describir las raíces. ¿ Cuántas de estas raíces serán reales ? No existe para raíces reales un criterio como el Lema de Gauss (Lema 27) para raíces racionales. Pero sin embargo existe un algoritmo que permite contar con exactitud la cantidad de raíces reales del polinomio f en un intervalo (Teorema de Sturm, 1836). Antes veremos un criterio más sencillo, debido a Descartes (1596-1650), que permite acotar la cantidad de raíces reales de f. Para ello necesitamos introducir la notación siguiente :

Notación 37 *Sea* $f = a_n X^n + \dots + a_0 \in \mathbb{R}[X]$.

- $Z_+(f)$ *:= cantidad de raíces reales estrictamente positivas de* f *(contadas con multiplicidad).*
- $Z_-(f)$ *:= cantidad de raíces reales estrictamente negativas de* f *(contadas con multiplicidad).*
- $V(f) = V(a_n, \dots, a_0) :=$ *número de cambios de signo en la sucesión ordenada* $(a_n, \dots, a_0)$, *salteando los ceros.*

Por ejemplo, si $f = 3X^6 + 2X^5 - X^3 + X^2 - 7$, entonces $V(f) = V(3, 2, 0, -1, 1, 0, -1) = 3$ pues se cuenta 1 al pasar de 2 a -1, 1 por pasar de -1 a 1 y nuevamente 1 por pasar de 1 a -7.
Si $g = 3X^4 + X^2 + 2$, $V(g) = 0$ y si $h = X^3 - X^2 + X - 1$, $V(h) = 3$.

Proposición 38 (Regla de los signos de Descartes)
Sea $f = a_n X^n + \dots + a_0 \in \mathbb{R}[X]$, *entonces :*

1. $Z_+(f) \leq V(f)$
2. $V(f) - Z_+(f)$ *es siempre un número par.*
3. $Z_-(f) \leq V(f(-X)) = V((-1)^n a_n, (-1)^{n-1} a_{n-1}, \dots, a_0)$ *y* $V(f(-X)) - Z_-(f)$ *es siempre un número par.*
4. *Si se sabe que* f *tiene todas sus raíces en* $\mathbb{R}$, *entonces* $Z_+(f) = V(f)$ *y* $Z_-(f) = V(f(-X))$

Observación Descartes enunció esta regla, basándose posiblemente en observaciones empíricas y demostraciones parciales para polinomios de grado 1 y 2, y polinomios con todos los coeficientes positivos por ejemplo donde es claro. El resultado fue probado luego con total generalidad por Gauss.
El inciso (4), que no es tan conocido y empezó a ser comentado y usado hacia 1980, resulta útil cuando uno sabe de antemano que un polinomio real tiene todas sus raíces reales, por ejemplo cuando se trata del polinomio característico de una matriz real simétrica. En ese caso, la regla de los signos de Descartes permite calcular la signatura de la matriz sin factorizar el polinomio característico.

Prueba.– Demostraremos aquí completamente el inciso (1), que se basa en el :

Teorema de Rolle *Sea* $f : \mathbb{R} \longrightarrow \mathbb{R}$ *continua y derivable, y* $\alpha < \beta \in \mathbb{R}$ *tales que* $f(\alpha) = f(\beta) = 0$, *entonces existe* γ, $\alpha < \gamma < \beta$ *tal que* $f'(\gamma) = 0$.

Para obtener (2), se usa la misma demostración que para (1) pero usando la siguiente versión más fuerte del Teorema de Rolle : si $f \in \mathbb{R}[X]$, entonces entre dos raíces reales consecutivas de f hay un número impar de raíces de f'.

Para (3), se observa que si $\alpha \in \mathbb{R}$, $\alpha < 0$, es raíz de f, entonces $-\alpha > 0$ es raíz del polinomio $f(-X)$. O sea contar las raíces negativas de f se reduce a contar las raíces positivas de $f(-X)$.

El inciso (4) se obtiene agregando la siguiente observación (que se puede probar por inducción en $\mathrm{gr}(f)$) : siempre vale $V(f) + V(f(-X)) \leq n$. Luego, si f tiene n raíces reales, que podemos suponer no nulas, la única posibilidad es que se cumplan las igualdades en los dos primeros incisos.

Pasemos ahora a probar el inciso (1) :

La demostración se hace por inducción en $\mathrm{gr}(f) = n$:

– Si $n = 1$, $f = aX + b$ y $Z_+(f) = 1 \Longleftrightarrow ab < 0 \Longleftrightarrow V(f) = 1$.

– Si $n > 1$, sin pérdida de generalidad, podemos suponer que :

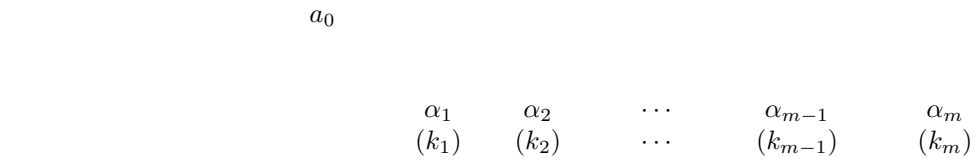
$$f = a_n X^n + \cdots + a_j X^j + a_0 \text{ con } a_n \neq 0,\ a_j \neq 0\ (n \geq n-1 \geq \cdots \geq j) \text{ y } a_0 > 0$$

quitando la raíz 0 tantas veces como aparece y eventualmente cambiando f por $-f$ (ya que estos cambios no modifican ni $Z_+(f)$ ni $V(f)$).

Luego $f' = na_n X^{n-1} + \cdots + ja_j X^{j-1}$ y se tienen dos posibilidades : o bien $a_j < 0$ y en ese caso $V(f) = V(f') + 1$, o bien $a_j > 0$ y en ese caso $V(f) = V(f')$.
Analizaremos cada caso por separado :

- Caso $a_j < 0$ y $V(f) = V(f') + 1$

  Dibujemos el gráfico de f (en su parte positiva) marcando las raíces positivas $\alpha_1, \ldots, \alpha_m$ con sus respectivas multiplicidades $k_1, \ldots, k_m$.



  Se tiene $Z_+(f) = k_1 + \cdots + k_m$, y $\alpha_1, \ldots, \alpha_m$ son raíces de f' con multiplicidades $k_1 - 1, \ldots, k_m - 1$.

Por el Teorema de Rolle, existen además (por lo menos) $\beta_1, \ldots, \beta_{m-1}$ raíces de f' con $\alpha_1 < \beta_1 < \alpha_2, \ldots, \alpha_{m-1} < \beta_{m-1} < \alpha_m$.

Así, $Z_+(f') \geq (k_1 - 1) + \cdots + (k_m - 1) + (m-1) = k_1 + \cdots + k_m - 1 = Z_+(f) - 1$.

Pero por hipótesis inductiva, $Z_+(f') \leq V(f')$ y estamos en el caso en que $V(f') = V(f) - 1$.

Por lo tanto, resumiendo, $Z_+(f) - 1 \leq Z_+(f') \leq V(f') = V(f) - 1$, es decir $Z_+(f) \leq V(f)$ como se quería probar.

- Caso $a_j > 0$ y $V(f) = V(f')$

  Haciendo el mismo analisis, se obtiene $Z_+(f') \geq Z_+(f) - 1$, pero en este caso $V(f') = V(f)$. Usando la hipótesis inductiva, se podría concluir que $Z_+(f) \leq V(f) + 1$ que no es lo que se busca.

  Si pudiéramos mostrar que en realidad en este caso, $Z_+(f') \geq Z_+(f)$, entonces tendríamos las desigualdades $Z_+(f) \leq Z_+(f') \leq V(f') = V(f)$, como queremos probar. O sea, nos falta una raíz positiva de f' !

  Observemos que $a_0 = f(0) > 0$, y $a_j > 0$ implica que a la derecha de 0 la función f crece :

$$\lim_{x \to 0^+} f(x) = \lim_{x \to 0^+} a_0 + a_j x^j (1 + \frac{a_{j+1}}{a_j} x + \cdots + \frac{a_n}{a_j} x^{n-j}) = {a_0}^+ \text{ pues } a_j > 0$$

  Pero luego, la función f tiene que decrecer pues $f(\alpha_1) = 0$, por lo tanto f tiene un máximo en el intervalo $(0, \alpha_1)$, es decir existe $\beta \in (0, \alpha_1)$ tal que $f'(\beta) = 0$.

  Así, $Z_+(f') \geq (Z_+(f) - 1) + 1 = Z_+(f)$ y por lo tanto $Z_+(f) \leq Z_+(f') \leq V(f') = V(f)$ como se quería probar.

■

Aplicaciones

- El polinomio $X^n - 1$ tiene a lo sumo 1 raíz real positiva pues $V(f) = 1$, pero al ser $V(f) - Z_+(f)$ par, tiene exactamente 1 raíz real positiva. Y tiene 1 raíz real negativa en función de si n es par o impar.
- Más generalmente, si $f \in \mathbb{R}[X]$ es un polinomio tal que $V(f) = 1$, entonces, al ser $V(f) - Z_+(f)$ siempre par, tiene que valer que $Z_+(f) = 1$.
- Sea $f \in \mathbb{R}[X]$ un polinomio de grado n con exactamente k monomios no nulos. Entonces f tiene a lo sumo $k - 1$ raíces reales positivas y $k - 1$ raíces reales negativas.
- Sea $f = X^5 - 3X^4 + 1$. $V(f) = 2$, por lo tanto f tiene 0 o 2 raíces reales positivas. Pero como además $f(0) = 1$ y $f(1) = -1$, f tiene seguro una raíz real en el intervalo $(0, 1)$, por lo tanto f tiene 2 raíces reales positivas, y f tiene exactamente 1 raíz real negativa (pues $f(-X) = -X^5 - 3X^4 + 1$), y 2 raíces complejas no reales conjugadas.

Pasaremos ahora al Teorema de Sturm que permite determinar exactamente el número de raíces reales de un polinomio real f en un intervalo (a, b). Para ello necesitaremos asociar al polinomio f un polinomio $\overline{f}$ con las mismas raíces complejas que f, pero todas de multiplicidad 1.

Proposición 39 *Sea $f \in \mathbb{R}[X]$, $\text{gr}(f) \geq 1$. Entonces el polinomio $\overline{f} := \frac{f}{\text{mcd}(f; f')} \in \mathbb{R}[X]$ tiene las mismas raíces complejas que f, pero todas de multiplicidad 1. ($\overline{f}$ se llama el polinomio libre de cuadrados asociado a f.)*

Prueba.– Sea $f = c(X-\alpha_1)^{k_1}\dots(X-\alpha_m)^{k_m}$ la factorización de f en $\mathbb{C}[X]$.
Sabemos por la Proposición 17 que si α_i es raíz de multiplicidad exactamente k_i de f, entonces es raíz de multiplicidad exactamente $k_i - 1$ de f', y por lo tanto :

$$f' = (X-\alpha_1)^{k_1-1}\dots(X-\alpha_m)^{k_m-1}g(X) \quad \text{con} \quad g(\alpha_i) \neq 0 \ (1 \leq i \leq m).$$

(También se puede hacer la cuenta derivando f.)
Luego $\operatorname{mcd}(f;f') = (X-\alpha_1)^{k_1-1}\dots(X-\alpha_m)^{k_m-1} \in \mathbb{R}[X]$ y $\overline{f} = \frac{f}{\operatorname{mcd}(f;f')} = c(X-\alpha_1)\dots(X-\alpha_m) \in \mathbb{R}[X]$ verifica lo enunciado.

■

Observación 40 *Se puede calcular* $\operatorname{mcd}(f;f')$ *sin conocer la factorización de* $f \in \mathbb{C}[X]$*, aplicando por ejemplo el algoritmo de Euclides (repidiendo sucesivas veces el algoritmo de división), y por lo tanto para cada* $f \in \mathbb{R}[X]$ *determinar el polinomio* $\overline{f}$ *libre de cuadrados asociado a* f*.*

Definición 41 (Sucesión de Sturm) *Sea* $f \in \mathbb{R}[X]$ *un polinomio sin raíces múltiples en* $\mathbb{C}$*. Sean* $a,\ b \in \mathbb{R}$*,* $a < b$ *tales que* $f(a) \neq 0$ *y* $f(b) \neq 0$*. Se define la siguiente sucesión de polinomios (Sucesión de Sturm de* f*) :*

- $f_0 := f$*,*
- $f_1 := f'$*,*
- *para todo* $i \geq 1$*, se efectúa el algoritmo de división* $f_{i-1} = q_i f_i + r_i$ *con* $\operatorname{gr}(r_i) < \operatorname{gr}(f_i)$ *y se define* $f_{i+1} = -r_i$*.*
- *Se termina cuando se llega a* $f_s :=$ *constante (observemos que dado que esta sucesión coincide salvo eventualmente signos con la sucesión de restos que se obtiene aplicando el Algoritmo de Euclides —para calcular el máximo común divisor— a* f *y* f'*, la hipotesis que* f *no tenga raíces múltiples en* $\mathbb{C}$ *garantiza que se llega siempre a* f_s *igual a una constante no nula).*

Se define también, siguiendo el espíritu de la Notación 37 :

- $Z_{(a,b)}(f)$ *:=cantidad de raíces reales de* f *en el intervalo* (a,b)*.*
- $Z(f) := Z_{(-\infty,+\infty)}(f)$ *:=cantidad total de raíces reales de* f*.*
- $\forall c \in \mathbb{R}$*,* $V(c) := V(f_0(c), f_1(c), \dots, f_s(c)) =$ *número de variaciones de signos en la sucesión ordenada* $(f_0(c), f_1(c), \dots, f_s(c))$*.*

Teorema 42 (Sturm, 1836) *Sea* $f \in \mathbb{R}[X]$ *un polinomio sin raíces múltiples. Sean* $a,\ b \in \mathbb{R}$*,* $a < b$ *tales que* $f(a) \neq 0$ *y* $f(b) \neq 0$*. Entonces,* $Z_{(a,b)}(f) = V(a) - V(b)$*.*

Antes de demostrar este resultado, hagamos algunos ejemplos :

Ejemplo Sea $f = X^3 - 5X^2 + 8X - 8$.

Por la regla de los signos de Descartes, se deduce que f tiene 1 o 3 raíces reales positivas y ninguna raíz real negativa.
Se tiene $f' = 3X^2 - 10X + 8$

(Observemos que f' tiene exactamente 2 raíces reales positivas, $3/2$ y 2, pero ésto no nos permite decidir si f tiene 1 o 3 raíces reales)

Calculemos la Sucesión de Sturm de f, aún sin saber que f no tiene raíces múltiples.
$f_0 := f = X^3 - 5X^2 + 8X - 8$
$f_1 := f' = 3X^2 - 10X + 8$
$f_2 := \frac{2}{9}X + \frac{32}{9}$ pues $f_0 = (\frac{1}{3}X - \frac{5}{9})f_1 + (-\frac{2}{9}X - \frac{32}{9})$.
$f_3 := -936$ pues $f_1 = (\frac{27}{2}X - 261)f_2 + 936$.

Dado que llegamos a que f_3 es una constante no nula, deducimos inmediatamente que f no tiene raíces múltiples en $\mathbb{C}$ (recordando que la sucesión de Sturm es, salvo eventualmente un signo, la del algoritmo de Euclides para calcular $\mathrm{mcd}(f; f')$) y estamos en condiciones de aplicar el Teorema de Sturm.

- Sea por ejemplo $a = 0$ y $b = 1$. Se tiene $V(a) = V(0) = V(-8, 8, \frac{32}{9}, -936) = 2$ y $V(b) = V(1) = V(-4, 1, \frac{34}{9}, -936) = 2$

  Por lo tanto, $Z_{(0,1)}(f) = V(0) - V(1) = 2 - 2 = 0$ y f no tiene ninguna raíz real en el intervalo $(0, 1)$.

- Sea ahora $a = 3$ y $b = 4$. Se tiene $V(a) = V(3) = V(-2, 5, \frac{38}{9}, -936) = 2$ y $V(b) = V(4) = V(8, 16, \frac{40}{9}, -936) = 1$

  Por lo tanto, $Z_{(3,4)}(f) = V(3) - V(4) = 2 - 1 = 1$ y f tiene exactamente 1 raíz real en el intervalo $(0, 1)$.

- También queremos saber calcular la cantidad total de raíces reales de f. Como sabemos que $M = 1+5+8+8 = 22$ es una cota superior para los módulos de las raíces de f (Proposición 23), podríamos calcular $V(-22) - V(22)$, ó también $V(-N) - V(N)$, para todo $N \geq 22$. Si elegimos entonces N suficientemente grande, es decir más grande que todas las raíces de los f_i para todo i, $0 \leq i \leq 2$:

  $$f_i(N) > 0 \Longleftrightarrow \lim_{x \to +\infty} f_i(x) = +\infty$$

  (pues en $[N, +\infty)$ no puede haber cambios de signo ya que no hay raíces de f_i, y obligatoriamente $\lim_{x\to+\infty} f_i(x) = \pm\infty$ si f no es constante).

  Pero observemos también que

  $$\lim_{x \to +\infty} f_i(x) = +\infty \Longleftrightarrow \text{ el coeficiente principal de } f_i \text{ es positivo}$$

  De la misma manera,

  $$f_i(-N) > 0 \Longleftrightarrow \lim_{x \to -\infty} f_i(x) = +\infty \Longleftrightarrow (-1)^{\mathrm{gr}(f_i)}\mathrm{cp}(f_i) > 0$$

  Así, observamos que :

  $V(-N) = V(-\infty) = V(-\infty, +\infty, -\infty, -936) = V(-, +, -, -) = 2$

  y $V(+\infty) = V(+\infty, +\infty, +\infty, -936) = V(+, +, +, -) = 1$

  Y concluimos que $Z(f) = Z_{(-N,N)}(f) = Z_{(-\infty,+\infty)}(f) = V(-\infty, +\infty) = 2 - 1 = 1$: el número total de raíces reales de f es 1.

■

Como corolario de la discusión anterior, obtenemos :

Teorema 43 (Sturm) *Sea $f \in \mathbb{R}[X]$ un polinomio sin raíces múltiples, y sea $f_0, f_1, \ldots, f_s$ la sucesión de Sturm definida en la Definición 41.*
Entonces $Z(f) = V(-\infty) - V(+\infty)$, donde :

$$V(\pm\infty) := V(\lim_{x\to\pm\infty} f_0(x), \lim_{x\to\pm\infty} f_1(x), \ldots, \lim_{x\to\pm\infty} f_s(x))$$

Ejemplo Sea $f = X^2 + bX + c \in \mathbb{R}[X]$. Vamos a reencontrar por medio del teorema de Sturm el hecho que f tiene 2 raíces reales si y sólo si $b^2 - 4c \geq 0$.
f tiene raíces simples $\iff \gcd(f; f') = 1$ donde $f' = 2X + b$.
O sea, $\gcd(f; f') = 1 \iff f(-\frac{b}{2}) \neq 0 \iff \frac{b^2}{4} - \frac{b^2}{2} + c \neq 0 \iff b^2 - 4c \neq 0$.
Es decir, si $b^2 - 4c \neq 0$, f tiene raíces simples y podemos aplicar directamente el teorema de Sturm. Mientras que si $b^2 - 4c = 0$, $\gcd(f; f') = X + b/2$ y tenemos que trabajar con el cociente $\overline{f} = X + b/2$.

- Caso $b^2 - 4c \neq 0$:

  $$f_0 = X^2 + bX + c \quad , \quad f_1 = 2X + b \quad , \quad f_2 = -c + \frac{b^2}{4} = \frac{b^2 - 4c}{4}$$

  Luego

  $$V(-\infty) = V(+\infty, -\infty, b^2 - 4c) = \begin{cases} 2 & \text{si } b^2 - 4c > 0 \\ 1 & \text{si } b^2 - 4c < 0 \end{cases}$$
  $$V(+\infty) = V(+\infty, +\infty, b^2 - 4c) = \begin{cases} 0 & \text{si } b^2 - 4c > 0 \\ 1 & \text{si } b^2 - 4c < 0 \end{cases}$$

  Es decir,

  $$Z(f) = \begin{cases} 2 & \text{si } b^2 - 4c > 0 \\ 0 & \text{si } b^2 - 4c < 0 \end{cases}$$

- Caso $b^2 - 4c = 0$:

  $$\overline{f}_0 = X + \frac{b}{2} \quad , \quad \overline{f}_1 = 1$$

  Aquí, $V(-\infty) = V(-\infty, 1) = 1$ y $V(+\infty) = V(+\infty, 1) = 0$, y $Z(\overline{f}) = 1$, es decir f tiene una raíz real doble.

■

Prueba del Teorema de Sturm.– Dado que f y f' son coprimos, y que la sucesión de Sturm coicide salvo eventualmente signos con la sucesión de restos dada por el Algoritmo de Euclides, no solamente se obtiene que $f_s \in \mathbb{R} \setminus \{0\}$, sino que para todo i, $(1 \leq i \leq s-1)$ los polinomios f_i y f_{i+1} son coprimos, y no comparten raíces en $\mathbb{C}$.
Las raíces, ordenadas consecutivamente, de todos los polinomios f_i de la sucesión de Sturm dividen el intervalo (a, b) en subintervalos I. En el interior de cada uno de esos subintervalos I el signo de cada polinomio f_i es constante (pues si hubiese un cambio de signo, habría una raíz). Por lo tanto $f_i(c)$ es de signo constante, para todo $c \in I$.
Denotemos por $\beta_1, \ldots, \beta_t$ todas las raíces de todos los polinomios f_i, ordenadas de menor a mayor, y por $c_1, \ldots, c_{t-1}$ puntos intermedios elegidos arbitrariamente :

$$a < \beta_1 < c_1 < \beta_2 < c_2 < \cdots < \beta_{t-1} < c_{t-1} < \beta_t < b$$

Podemos calcular $V(a) - V(b) = (V(a) - V(c_1)) + (V(c_1) - V(c_2)) + \cdots + (V(c_{t-1}) - V(b))$.

Notemos entonces $c_0 := a$, $c_t := b$, y analicemos $V(c_{k-1}) - V(c_k)$ para $1 \leq k \leq t$, o sea examinemos como varía V al cruzar exactamente la raíz β_k de (al menos) algún polinomio f_i :

- Si β_k es raíz de $f_0 = f$, no es raíz de $f_1 = f'$ (y f_1 no tiene ninguna raíz en $[c_{k-1}, c_k]$), luego f_1 tiene signo constante en $[c_{k-1}, c_k]$ y se tienen las siguientes posibilidades :

	c_{k-1}	β_k	c_k
f_0	$+$	0	$-$
f_1	$-$		$-$

f_0 decreciente en $[c_{k-1}, c_k]$
$\Longrightarrow f_1 = f' < 0$

	c_{k-1}	β_k	c_k
f_0	$-$	0	$+$
f_1	$+$		$+$

f_0 creciente en $[c_{k-1}, c_k]$
$\Longrightarrow f_1 = f' > 0$

  En cualquiera de los dos casos, $V(f_0(c_{k-1}), f_1(c_{k-1})) - V(f_0(c_k), f_1(c_k)) = 1 - 0 = 1$

- Si β_k es raíz de f_i $(1 \leq i \leq s-1)$, entonces $f_{i-1}(\beta_k) \neq 0$ y $f_{i+1}(\beta_k) \neq 0$ (pues $\text{mcd}(f_{i-1}; f_i) = 1 = \text{mcd}(f_i; f_{i+1})$), y por lo tanto f_{i-1} y f_{i+1} tienen signo constante en $[c_{k-1}, c_k]$.

  Además, por la construcción de la sucesión de Sturm :
  $$f_{i-1} = q_i f_i - f_{i+1}$$
  Luego, $f_{i-1}(\beta_k) = -f_{i+1}(\beta_k)$, o sea son de signo opuesto. Por consiguiente se tienen las siguientes posibilidades :

	c_{k-1}	β_k	c_k
f_{i-1}	$-$		$-$
f_i	$?$	0	$?$
f_{i+1}	$+$		$+$

	c_{k-1}	β_k	c_k
f_{i-1}	$+$		$+$
f_i	$?$	0	$?$
f_{i+1}	$-$		$-$

  E independientemente de los signos de $f_i(c_{k-1}$ y $f_i(c_k)$, resulta que :

  $V(f_{i-1}(c_{k-1}), f_i(c_{k-1}), f_{i+1}(c_{k-1})) = 1 = V(f_{i-1}(c_k), f_i(c_k), f_{i+1}(c_k))$.

  Así, $V(f_{i-1}(c_{k-1}), f_i(c_{k-1}), f_{i+1}(c_{k-1})) - V(f_{i-1}(c_k), f_i(c_k), f_{i+1}(c_k)) = 0$.

- Para los índices i tales que $f_i(\beta_k) \neq 0$ y $f_{i+1}(\beta_k) \neq 0$, f_i y f_{i+1} tienen signo constante en $[c_{k-1}, c_k]$, e independientemente de cuales son, se tiene $V(f_i(c_{k-1}), f_{i+1}(c_{k-1})) - V(f_i(c_k), f_{i+1}(c_k)) = 0$

Ahora :

$$V(c_{k-1}) - V(c_k) := V(f_0(c_{k-1}), f_1(c_{k-1}), \ldots, f_s(c_{k-1})) - V(f_0(c_k), f_1(c_k), \ldots, f_s(c_k))$$

y hemos observado que cada diferencia parcial

$$V(f_{i-1}(c_{k-1}), f_i(c_{k-1}), f_{i+1}(c_{k-1})) - V(f_{i-1}(c_k), f_i(c_k), f_{i+1}(c_k))$$
$$\text{ó } V(f_i(c_{k-1}), f_{i+1}(c_{k-1})) - V(f_i(c_k), f_{i+1}(c_k))$$

es siempre nula, a menos que se trate de f_0, f_1 y justamente entre c_{k-1} y c_k se encuentre una raíz β_k de f_0, en cuyo caso da 1. Por lo tanto, $V(c_{k-1}) - V(c_k)$ computa 1 cada vez que se pasa una raíz de f. Esto permite concluir que $Z_{(a,b)}(f) = V(a) - V(b)$.

■

Nota El algoritmo dado por el Teorema de Sturm permite luego calcular exactamente la cantidad de raíces reales de un polinomio libre de cuadrados f. Mas aún, permite por dicotomía, aproximarlas tanto como uno quiere (hallando intervalos pequeños donde se encuentra exactamente una raíz de f, y luego achicándolos cada vez más). Pero el costo de este algoritmo es muy elevado, y se observa además que en las sucesivas divisiones para construir las sucesiones de Sturm, aparecen números cada vez más complicados, aún cuando se empieza con un polinomio simple en $\mathbb{Z}[X]$.

Ultimo ejemplo (Polinomios de grado 3) En este ejemplo, utilizaremos todo la discusión de este párrafo para determinar cuántas raíces reales tiene el polinomio $X^3 + pX + q$ en función de los parámetros $p,\ q \in \mathbb{R}$.

$$f = X^3 + pX + q,\ p, q \in \mathbb{R}$$

El polinomio f tiene 1 ó 3 raíces reales. Vamos a distinguir los casos posibles según los signos posibles de p y q, aplicando la regla de los signos de Descartes (Proposición 38) y el Teorema de Sturm (Teorema 42).

- Caso $p = 0$:
  - Si $q = 0$, f tiene la raíz 0 con multiplicidad 3.
  - Si $q > 0$, $V(f) = 0$ y $V(f(-X)) = V(-, 0, 0, +) = 1$, por lo tanto, por la regla de los signos de Descartes, f tiene exactamente 1 raíz real negativa.
  - Si $q < 0$, $V(f) = 1$ y $V(f(-X)) = 0$, por lo tanto f tiene exactamente 1 raíz real positiva.
- Caso $q = 0$: en este caso $f = X(X^2 + p)$ tiene como única raíz real el 0 si $p > 0$ y 3 raíces reales distintas si $p < 0$.
- Caso $p > 0,\ q \neq 0$:

  En este caso, $V(f) = V(+, 0, +, q)$ y $V(f(-X) = V(-X^3 - pX + q) = V(-, 0, -, q)$. Apliquemos nuevamente la regla de los signos de Descartes : si $q > 0$, f tiene exactamente 1 raíz real negativa, y si $q < 0$, f tiene exactamente 1 raíz real positiva. Por lo tanto, en todos los casos, si $p > 0$ f tiene exactamente 1 raíz real.
- Caso $p < 0,\ q \neq 0$:

  En este caso, $V(f) = V(+, 0, -, q)$ y $V(f(-X) = V(-X^3 - pX + q) = V(-, 0, +, q)$.
  - Si $q > 0$, $V(f) = 2$ y $V(f(-X) = 1$: f tiene exactamente 1 raíz real negativa y hay que determinar si tiene 0 ó 2 raíces reales positivas.
  - Si $q < 0$, $V(f) = 1$ y $V(f(-X)) = 2$: f tiene exactamente 1 raíz real positiva y hay que determinar si tiene 0 ó 2 raíces reales negativas.

  Vamos a terminar la discusión aplicando el Teorema de Sturm al polinomio f. Calculando la sucesión de Sturm, se obtiene :

$$f_0 = X^3 + pX + q \quad , \quad f_1 = 3X^2 + p \quad , \quad f_2 = -\frac{2p}{3}X - q \quad , \quad f_3 = \frac{-4p^3 - 27q^2}{4p^2}.$$

  Así , f es libre de cuadrados si y sólo si $4p^3 + 27q^2 \neq 0$, y en ese caso podemos aplicar directamente el teorema.

– Caso $4p^3 + 27q^2 \neq 0$:

$$V(-\infty) = V(-,+,-,-4p^3-27q^2) = \begin{cases} 3 & \text{si } -4p^3-27q^2 > 0 \\ 2 & \text{si } -4p^3-27q^2 < 0 \end{cases}$$

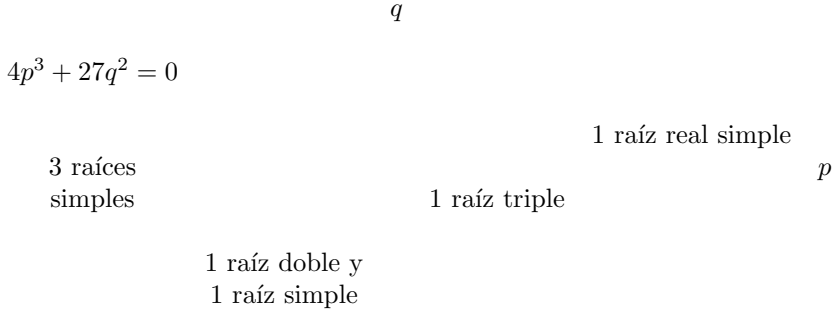
$$V(+\infty) = V(+,+,+,-4p^3-27q^2) = \begin{cases} 0 & \text{si } -4p^3-27q^2 > 0 \\ 1 & \text{si } -4p^3-27q^2 < 0 \end{cases}$$

Luego,

$$Z(f) = V(-\infty) - V(+\infty) = \begin{cases} 3 & \text{si } -4p^3-27q^2 > 0 \\ 1 & \text{si } -4p^3-27q^2 < 0 \end{cases}$$

– Caso $4p^3 + 27q^2 = 0$: En este caso, $\text{mcd}(f; f') = X + \frac{3q}{2p}$, y se verifica facilmente que las raíces de f son todas reales : $-\frac{3q}{2p}$ es raíz doble y $\frac{3q}{p}$ es raíz simple.

En todos los casos, notamos que f tiene tres raíces reales si y solo si el *Discriminante de* f : $-4p^3 - 27q^2$ es mayor o igual que 0 (ésta condición implica claramente $p \leq 0$). Podemos resumir la situación en el gráfico siguiente :



5.4 Aproximación de raíces reales

Como vimos antes, no hay en general una forma de calcular exactamente las raíces de un polinomio de $\mathbb{R}[X]$ de grado ≥ 5. Sin embargo, muchos problemas de la vida real requieren de todos modos calcular las raíces de alguna forma (o al menos aproximarlas suficientemente bien). Más aún, muchas veces las traducciones matemáticas de los problemas de la vida real son en realidad aproximaciones numéricas al problema real (debido a los errores de mediciones, por ejemplo, o a los truncamientos que ocurren cuando uno lleva un problema a la computadora), y por lo tanto, por más que uno pudiera obtener una solución exacta de este problema aproximado, sería en el mejor de los casos solo una solución aproximada del problema real.
Así que resulta imprescindible estudiar ciertos algoritmos que permiten aproximar las raíces de los polinomios reales. Este tema pertenece en principio a un área fundamental y muy compleja de la Matemática que se llama el Análisis Numérico.

Cabe mencionar que el algoritmo de Sturm que se ha expuesto para encajonar una raíz real de un polinomio tiene la desventaja de ser demasiado lento para aplicarlo en problemas concretos que generalmente necesitan ser resueltos casi instantáneamente.

A continuación se expondrán básicamente tres métodos : el más natural e intuitivo, que es el método de la bisección, una variación de éste que es el método de la secante y el conocido método de Newton-Raphson. Todos son válidos más generalmente para funciones $f : \mathbb{R} \longrightarrow \mathbb{R}$ continuas y suficientemente derivables, pero suelen ser más sencillos para polinomios.

5.4.1 Los métodos de la bisección y de la secante

Sean $a,\, b \in \mathbb{R},\ a < b$ y $f : \mathbb{R} \longrightarrow \mathbb{R}$ una función continua en $[a, b]$. Supongamos que $f(a)f(b) < 0$ (es decir el signo de $f(a)$ es el opuesto del signo de $f(b)$). Entonces, por el teorema de Bolzano, existe $\alpha \in (a, b)$ tal que $f(\alpha) = 0$.

El método de bisección
Consideremos $\frac{a+b}{2}$.

- Si $f(\frac{a+b}{2}) = 0$, entonces $\alpha = \frac{a+b}{2}$.
- Si $f(\frac{a+b}{2}) \neq 0$, o bien $f(a)f(\frac{a+b}{2}) < 0$ ó bien (excluyentemente) $f(\frac{a+b}{2})f(b) < 0$.

  En el primer caso se define $a_1 := a$ y $b_1 := \frac{a+b}{2}$, y en el segundo caso se define $a_1 := \frac{a+b}{2}$ y $b_1 := b$.
- Se continúa el procedimiento a partir de $a_1,\, b_1$: Definidos $a_n,\, b_n$ se define $a_{n+1} := a_n$, $b_{n+1} := \frac{a_n+b_n}{2}$ si $f(a_n)f(\frac{a_n+b_n}{2}) < 0$ y $a_{n+1} := \frac{a_n+b_n}{2}$, $b_{n+1} := b_n$ si $f(\frac{a_n+b_n}{2})f(b_n) < 0$ (salvo eventualmente si se cae en un cero de f, en cuyo caso se termina).

Al cabo de n pasos, se determina un intervalo $[a_n, b_n]$ que contiene un cero α de la función f. Además se observa que $\alpha - a_n \leq b_n - a_n \leq \frac{b-a}{2^n}$, por lo tanto si suponemos que $b - a = 1$ (o sea iniciamos el procedimiento con un intervalo de longitud 1), al considerar la sucesión $(a_n)_{n\in\mathbb{N}}$ se obtiene una cifra decimal significativa aproximadamente cada $3,3$ pasos.

Ejemplo Para determinar $\sqrt{2}$, sea $f = X^2 - 2$. tomando $a := 1$ y $b := 2$.

Se observa que $f(1) = -1$ y $f(2) = 2$. Así se determinan las sucesiones :

$$a_1 := 1; b_1 := 1,5 \quad ; \quad a_2 := 1,25; b_2 := 1,5 \quad ; \quad a_3 := 1,375; b_3 = 1,5$$

$$a_4 := 1,375; b_4 = 1,4375 \quad ; \quad a_5 := 1,40625; b_5 := 1,4375$$

$$a_6 := 1,40625; b_6 := 1,420875 \quad ; \quad a_7 := 1,4135625; b_7 := 1,420875$$

y se observa que al cabo de 7 pasos se tienen solamente 2 decimales significativos de $\sqrt{2}$.

El método de la secante
Es parecido al método de la bisección, pero en lugar de trabajar con el punto medio de cada intervalo para determinar el punto siguiente, se traza la secante entre $(a, f(a))$ y $(b, f(b))$ y se trabaja con su intersección con el eje de las abcisas :
La recta secante entre $(a, f(a))$ y $(b, f(b))$ tiene por ecuación :

$$y = \frac{f(b) - f(a)}{b - a}(x - a) + f(a)$$

y su intersección con el eje de las absicas está dado por :

$$x = \frac{f(b)a - f(a)b}{f(b) - f(a)}.$$

- Si $f(x) = 0$, entonces $\alpha = x$.
- Si $f(x) \neq 0$, o bien $f(a)f(x) < 0$ ó bien (excluyentemente) $f(x)f(b) < 0$.

  En el primer caso se define $a_1 := a$ y $b_1 := x$, y en el segundo caso se define $a_1 := x$ y $b_1 := b$ y se continúa el procedimiento con a_1, b_1.

Este método siempre converge a un cero α de la función f pero es dificil evaluar la rapidez de convergencia, ya que a priori no se puede acotar el intervalo $b_n - a_n$ al cabo de n pasos, salvo por $b-a$. Sin embargo, basándose en el hecho que si $|f(b)|$ es por ejemplo muy grande con respecto a $|f(a)|$, hay más chances para que α esté mas cerca de a, en muchos casos este método converge más rápido que el método de la bisección.

Ejemplo Retomemos el ejemplo anterior de la función $f(x) = x^2 - 2$ para determinar $\sqrt{2}$, con los puntos iniciales $a := 1, b := 2$.

Se obtienen las sucesiones :

$$a_1 := 4/3 = 1,\overline{3}; b_1 := 2 \quad ; \quad a_2 := 7/5 = 1,4; b_2 := 2 \quad ; \quad a_3 := 72/51 = 1,411\ldots; b_2 := 2$$

5.4.2 El método de Newton-Raphson

En algún sentido es parecido al método de la secante, pero trabaja con la recta tangente a la función en el punto $(x_0, f(x_0))$.
Haremos primero una presentación informal del método sin especificar demasiado las condiciones, y después se estudiarán condiciones que garanticen la convergencia del método.
Sea $f : \mathbb{R} \longrightarrow \mathbb{R}$ continua y derivable, y sea $x_0 \in \mathbb{R}$ tal que $f'(x_0) \neq 0$.
La recta tangente a la función en el punto $(x_0, f(x_0))$ tiene por ecuación :

$$y = f'(x_0)(x - x_0) + f(x_0)$$

y corta el eje de las abcisas en el punto :

$$x_1 := x_0 - \frac{f(x_0)}{f'(x_0)}.$$

Repitiendo el procedimiento (y suponiendo que $f'(x_1) \neq 0$, etc.) se define :

$$x_n := x_{n-1} - \frac{f(x_{n-1})}{f'(x_{n-1})} \qquad (n \geq 1).$$

Veremos en lo que sigue como, bajo algunas condiciones, la sucesión $(x_n)_{n\in\mathbb{N}_0}$ converge rápidamente a un cero α de la función f.

Ejemplo Sea $f = X^2 - 2$, y elijamos $x_0 := 2$.

En este caso, $f' = 2X$. Calculemos la función de recurrencia g :

$$g = X - \frac{f(X)}{f'(X)} = X - \frac{X^2-2}{2X} = \frac{X}{2} + \frac{1}{X}$$

Así, $x_1 := x_0/2 + 1/x_0 = 3/2 = 1,5$, $x_2 := 3/4 + 2/3 = 17/12 = 1,41\overline{6}$, $x_3 := 577/408 = 1,414210\ldots$ y se observa que en cada paso se agrega un dígito significativo.

Para poder dar condiciones suficientes para la convergencia de la sucesión de Newton, nos reduciremos al problema relacionado de la búsqueda de un punto fijo de una función :

5.4.3 Búsqueda de punto fijo y convergencia

Definición 44 *Sea $g : \mathbb{R} \longrightarrow \mathbb{R}$ una función. Se dice que $\alpha \in \mathbb{R}$ es un <u>punto fijo</u> de g si $g(\alpha) = \alpha$.*

Es inmediato observar que buscar un cero α de la función $f(x)$ en el intervalo $[a, b]$ es equivalente a buscar un punto fijo α de la función $g(x) := x - f(x)/f'(x)$ (asegurándose la condición $f'(x) \neq 0$ $\forall x \in [a, b]$).
Y, de la misma manera, estudiar si la sucesión de Newton definida por $x_0 \in \mathbb{R}$ arbitrario y $x_n := x_{n-1} - f(x_{n-1})/f'(x_{n-1})$ $(n \geq 1)$ converge a un cero α de f se reduce a estudiar si la sucesión $(x_n)_{n\in\mathbb{N}_0}$ definida por x_0 y $x_n := g(x_{n-1}))$ $(n \geq 1)$ converge a un punto fijo α de g (siempre que $x_n \in [a, b]$ para todo n).

Observación 45 *Sean $a < b \in \mathbb{R}$ y sea $g : [a, b] \longrightarrow [a, b]$ una función continua. Entonces g tiene un punto fijo en el intervalo $[a, b]$.*

Prueba.– Si $g(a) = a$ o $g(b) = b$, ya está. Si no, $g(a) > a$ y $g(b) < b$. Por lo tanto la función $h(x) := x - g(x)$ verifica que $h(b) > 0$ y $h(a) < 0$, y por el teorema de Bolzano, se concluye que existe $\alpha \in (a, b)$ tal que $h(\alpha) = 0$, es decir $g(\alpha) = \alpha$.

■

Notemos aquí la importancia del hecho que el intervalo $[a, b]$ sea finito. En efecto, si consideráramos la función $g(x) = x + 1$ (pensando por ejemplo en $a = -\infty$ y $b = +\infty$) la afirmación de que existe un punto fijo es falsa.
Por lo tanto en la práctica, se requiere hallar un intervalo finito de estabilidad de la función g : o sea, si g está definida de $\mathbb{R}$ en $\mathbb{R}$, un intervalo finito $[a, b]$ tal que $g([a, b]) \subseteq [a, b]$. Este es

uno de los problemas mayores al cual nos enfrentamos al tratar de conseguir un punto fijo de una función.

Gráficamente, buscar un punto fijo de g es buscar la intersección del gráfico de g con la recta $y = x$, y determinar si la sucesión dada por x_0, $x_n := g(x_{n-1})$ $(n \geq 1)$ converge a un punto fijo α de g se puede visualizar en los ejemplos siguientes :

Gráfico 1 : $x_n \longrightarrow \alpha$

Gráfico 2 : $x_n \not\longrightarrow \alpha$

Gráfico 3 : $x_n \longrightarrow \alpha$

Gráfico 4 : $x_n \not\longrightarrow \alpha$

Aquí se ve claramente la necesidad de que $|\, x_n - \alpha \,| < |\, x_{n-1} - \alpha \,|$ $(n \geq 1)$, o sea que $|g(x_{n-1}) - g(\alpha)\,| < |\, x_{n-1} - \alpha \,|$ $(n \geq 1)$.
Luego sería bueno conseguir un intervalo $[a, b] \in \mathbb{R}$ tal que $(x_n)_{n\in\mathbb{N}_0} \subset [a, b]$ en el cual se cumpla la condición $|\, g(x) - g(y)\,| < |\, x - y \,|$ (para todo $x, y \in [a, b]$).
Esto motiva la definición siguiente, aunque para garantizar la convergencia, pediremos una condición un poco más fuerte :

Definición 46 *Sean $a < b \in \mathbb{R}$ y $g : [a, b] \longrightarrow [a, b]$ una función continua. Se dice que g es contractiva si existe $k < 1 \in \mathbb{R}$ tal que $|\, g(x) - g(y)\,| \leq k\,|\, x - y \,|$ para todo $x, y \in [a, b]$.*

Proposición 47 *Sean $a < b \in \mathbb{R}$ y $g : [a, b] \longrightarrow [a, b]$ una función continua y contractiva. Entonces la sucesión definida por $x_0 \in [a, b]$ arbitrario, y $x_n := g(x_{n-1})$ $(n \geq 1)$ converge al único punto fijo α de g en $[a, b]$.*

Prueba.–

- Veamos primero que en esas condiciones hay un único punto fijo de g en $[a, b]$.

  Ya sabemos, por la Observación 45, que hay por lo menos uno.

  Supongamos que α, $\beta \in [a, b]$ son puntos fijos de g. Entonces $|\, \alpha - \beta \,| = |\, g(\alpha) - g(\beta)\,| \leq k\,|\, \alpha - \beta \,|$ con $k < 1$. Luego, $\alpha = \beta$.

- Para probar la convergencia de la sucesión (x_n) a ese punto fijo, probemos primero que es convergente, y luego que converge a un punto fijo :

  – Se tiene $|\, x_{n+1} - x_n \,| = |\, g(x_n) - g(x_{n-1} \,| \leq k \,|\, x_n - x_{n-1} \,| \leq k^2 \,|x_{n-1} - x_{n-2} \,| \leq \cdots \leq k^n |\, x_1 - x_0 \,|$.
  Por lo tanto, para $m > n$, aplicando la desigualdad triangular y la fórmula de la serie geométrica :

$$\begin{aligned} |\, x_m - x_n \,| &\leq |\, x_m - x_{m-1} \,| + |\, x_{m-1} - x_{m-2} \,| + \cdots + |\, x_{n+1} - x_n \,| \\ &\leq (k^{m-1} + \cdots + k^n) |\, x_1 - x_0 \,| \\ &\leq k^n (k^{m-1-n} + \cdots + 1) |\, x_1 - x_0 \,| \\ &\leq k^n \left(\frac{1 - k^{m-n}}{1-k} \right) |\, x_1 - x_0 \,| \\ &< k^n \left(\frac{1}{1-k} \right) |\, x_1 - x_0 \,| \\ &< \frac{k^n}{1-k} |\, x_1 - x_0 \,| \end{aligned}$$

  La sucesión resulta de Cauchy, luego convergente.

  – Sea $\alpha := \lim_{n\to\infty} x_n$. Por la continuidad de g, se tiene :

$$g(\alpha) = \lim_{n\to\infty} g(x_n) = \lim_{n\to\infty} x_{n+1} = \alpha.$$

■

Para determinar en la práctica si una función derivable es contractiva, resulta más fácil en general utilizar el teorema del valor medio y chequear una condición sobre la derivada :

Proposición 48 *Sean $a < b \in \mathbb{R}$ y $g : [a,b] \longrightarrow [a,b]$ una función derivable. Supongamos que existe $k < 1 \in \mathbb{R}$, tal que $|\, g'(x) \,| \leq k$ para todo $x \in [a,b]$. Entonces g es contractiva.*

Prueba.– Para todo $x < y \in [a,b]$,

$$\left| \frac{g(x) - g(y)}{x - y} \right| = |g'(\xi)| \leq k < 1 \quad \text{para algún } \xi \in (x,y)$$

■

Podemos resumir los resultados obtenidos en la Proposición siguiente :

Proposición 49 *Sea g continua y derivable, $a < b \in \mathbb{R}$ y $k < 1 \in \mathbb{R}$ tales que :*

- $g([a,b]) \subseteq [a,b]$
- $|\, g'(x) \,| \leq k$ *para todo* $x \in [a,b]$

Entonces, g tiene un único punto fijo α en el intervalo $[a,b]$, y la sucesión definida por : $x_0 \in [a,b]$ arbitrario, y $x_n = g(x_{n-1})$, $n \geq 1$, converge a α .

■

Ejemplo : Verifiquemos que se cumplen efectivamente las condiciones de la Proposición 49 para la función $g = X/2 + 1/X$ correspondiente a $f = X^2 - 2$ del ejemplo anterior en el intervalo $[1,2]$:

- $1 \leq x \leq 2 \Longrightarrow 1/2 \leq x/2 \leq 1$ y $1/2 \leq 1/x \leq 1$, luego $1 \leq g(x) = x/2 + 1/x \leq 2$, o sea $g([1,2]) \subseteq [1,2]$, y $g : [1,2] \longrightarrow [1,2]$ es derivable.
- $g'(X) = 1/2 - 1/X^2$ verifica que $|\, g'(x)\,| \leq 1/2$ si $1 \leq x \leq 2$ pues $1/4 \leq 1/x^2 \leq 1$. Luego g es contractiva con $k = 1/2$.

■

Otro ejemplo Sea $f = X^3 - X - 1$, y tratemos de aproximar un cero real de f.
(Por la regla de los signos de Descartes, f tiene exactamente 1 raíz real positiva, que (por Bolzano) se encuentra además en el intervalo $(1,2)$.)

- Si elegimos $g_1 := x - f(x)/f'(x)$, como lo hemos hecho hasta ahora, se tiene :

$$g_1 = X - \frac{X^3 - X - 1}{3X^2 - 1} = \frac{2X^3 + 1}{3X^2 - 1}$$

  y puede resultar complicado verificar las condiciones de la Proposición 49.

- También podemos observar que $f(\alpha) = 0 \Longleftrightarrow \alpha = \alpha^3 - 1$, y por lo tanto intentar aproximar un punto fijo de la función $g_2 = X^3 - 1$.

  Pero aquí también nos va a resultar imposible encontrar un intervalo de estabilidad de g_2.

- Finalmente, podemos observar que $f(\alpha) = 0 \Longleftrightarrow \alpha = \sqrt[3]{\alpha + 1}$ y trabajar con $g := \sqrt[3]{X+1}$.

  - Claramente g es creciente; además $g(1) = \sqrt[3]{2} > 1$ y $g(2) = \sqrt[3]{3} < 2$, por lo tanto $g([1,2]) \subseteq [1,2]$.
  - g es derivable en $[1,2]$:

$$g' = \frac{1}{3\sqrt[3]{(X+1)^2}}$$

    y se cumple $|\, g'(x)\,| \leq 1/3$ para todo $x \in [1,2]$.

  Por lo tanto la sucesión $1,\ g(1) = \sqrt[3]{2} = 1.25992\ldots,\ g(g(1)) = \sqrt[3]{\sqrt[3]{2}+1} = 1.31229\ldots,$
  $g(g(g(1))) = 1.32235\ldots,\ 1.32426\ldots,\ 1.32463\ldots,\ldots$ converge al punto fijo α de g, o sea a la raíz positiva α de $X^3 - X - 1$.

■

Se mostró hasta ahora que cada vez que se logra determinar un intervalo de estabilidad para g donde la derivada es acotada por $k < 1$, la sucesión $x_n = g(x_{n-1})$ correspondiente converge al único punto fijo α. Reciprocamente, si α es un punto fijo de g con $g'(\alpha) < 1$, existe un intervalo de estabilidad donde el método va a funcionar :

Proposición 50 *Sea g definida en algún intervalo abierto I de $\mathbb{R}$, derivable y con derivada continua en I, y sea $\alpha \in I$ un punto fijo de g tal que $|\, g'(\alpha)\,| < 1$. Entonces existe $\varepsilon > 0$ tal que las condiciones de la Proposición 49 se cumplen en el intervalo $[\alpha - \varepsilon, \alpha + \varepsilon]$, y por lo tanto la sucesión definida por $x_0 \in [\alpha - \varepsilon, \alpha + \varepsilon]$ arbitrario, y $x_n = g(x_{n-1})$ $(n \geq 1)$ converge al punto fijo α.*

Prueba.–

- Dado que $g'(\alpha) < 1$, existe $k < 1$ tal que $g'(\alpha) < k$, y por la continuidad de g', existe $\varepsilon > 0$ tal que para todo $x \in [\alpha - \varepsilon, \alpha + \varepsilon]$ se tiene $g'(x) < k$.
- Por otro lado, sea $x \in [\alpha - \varepsilon, \alpha + \varepsilon]$, entonces, $|\, g(x) - \alpha \,| = |\, g(x) - g(\alpha) \,| = |\, g'(\xi) \,|\, |\, x - \alpha \,|$ para algún ξ en el intervalo determinado por α y x.

  Luego, $|\, g(x) - \alpha \,| < |\, x - \alpha \,| \leq \varepsilon$, es decir, $g(x) \in [\alpha - \varepsilon, \alpha + \varepsilon]$ y se tiene un intervalo de estabilidad para g.

■

Pero esta Proposición no ayuda demasiado, ya que implica acotar la derivada en el cero de la función que en principio no se conoce y se quiere calcular, y lleva finalmente a encontrar un intervalo contractivo !

5.4.4 Criterios de convergencia para el método de Newton-Raphson

Teorema 51 *Sea $f : [a, b] \longrightarrow \mathbb{R}$ dos veces derivable en $[a, b]$ con derivada segunda continua, que cumple las condiciones :*

- $f(a)f(b) < 0$
- $f'(x) \neq 0$ *para todo* $x \in [a, b]$
- $f''(x) \geq 0$ *ó* $f''(x) \leq 0$ *para todo* $x \in [a, b]$
- $\left|\frac{f(a)}{f'(a)}\right| < b - a$ *y* $\left|\frac{f(b)}{f'(b)}\right| < b - a$

Entonces, para todo $x \in [a, b]$, el método de Newton-Raphson converge al único cero α de f en $[a, b]$.

Prueba.– Demostraremos el resultado para $f(a) < 0$, $f(b) > 0$, el otro caso se demuestra de manera análoga.
Dado que $f(a) < 0$ y $f(b) > 0$, la condición $f' \neq 0$ en $[a, b]$ implica que $f' > 0$ en $[a, b]$) y que $f''(x) \geq 0$ para todo $x \in [a, b]$: o sea la función es estrictamente creciente (con derivada creciente) y convexa. Por lo tanto, tiene un único cero α en el intervalo.
La última condición garantiza que las tangentes a la curva en los puntos $(a, f(a))$ y $(b, f(b))$ intersecan el eje de las abcisas en el intervalo $[a, b]$:
Por ejemplo, la recta tangente a la curva en $(a, f(a))$ tiene por ecuación : $y = f'(a)(x-a)+f(a)$, e interseca al eje de las absicas en $x - a = -f(a)/f'(a)$, con $x > a$ (por ser $f(a) < 0$). Luego

$$x - a = |x - a| = \left|\frac{f(a)}{f'(a)}\right| < b - a$$

garantiza que $x \in [a, b]$.
Si por casualidad, $x = \alpha$, no hay nada que probar.
Probaremos ahora que si $x \in (\alpha, b]$, entonces el elemento siguiente de la sucesión de Newton definido por $g(x) := x - f(x)/f'(x)$ pertenece al intervalo (α, x) :
Se tiene $\alpha < x \leq b$, y $g' = \frac{ff''}{f'^2}$, por lo tanto $g'(x) \geq 0$ en $[\alpha, b]$, pues $f(x) > f(\alpha) = 0$ y $f'' > 0$ por hipótesis. Es decir g es creciente en $[\alpha, b]$, y estrictamente creciente en $(\alpha, b]$. Así $\alpha = g(\alpha) < g(x)$. Por otro lado, $g(x) = x - f(x)/f'(x) < x$ pues $f(x)/f'(x) > 0$ (por ser $f(x) > 0$ y $f' > 0$).
Lo que se probó entonces es que si $x_0 \in (\alpha, b]$, la sucesión $x_n := g(x_{n-1})$ ($n \geq 1$) verifica :

$$\alpha < \cdots < x_n < x_{n-1} < \cdots < x_1 < x_0 \,.$$

Es una sucesión decreciente y acotada inferiormente que por lo tanto converge, y converge obligatoriamente a un punto fijo de g, o sea a α.

Falta considerar que pasa si $x \in [a, \alpha)$. Mostraremos que en ese caso, $g(x)$ pertenece al intervalo $(\alpha, b]$ y por lo tanto uno se reduce al caso anterior a partir de $x_1 := g(x)$.
Se tiene $a \leq x < \alpha$, y en este caso $g'(x) \leq 0$ (pues $f(x) \leq f(\alpha) = 0$ y $f'' > 0$), por lo tanto g es decreciente en $[a, \alpha]$ y estrictamente decreciente en $[a, \alpha)$, o sea $\alpha = g(\alpha) < x$. Por otro lado, $g(x) \leq g(a)$ y la última condición de las hipótesis del teorema garantizaba que $g(a) \leq b$, por lo tanto $g(x) \leq b$.

■

La demostración del teorema lleva inmediatamente al siguiente resultado :

Corolario 52 *Sea $f : [a, b] \longrightarrow \mathbb{R}$ una función continua y dos veces derivable, que verifica las condiciones :*

- $f(a) < 0$ *y* $f(b) > 0$.
- $f'(x) > 0$ *y* $f''(x) \geq 0$ *para todo* $x \in [a, b]$.

Entonces, la sucesión de Newton definida por $x_0 := b$ y $x_n := x_{n-1} - f(x_{n-1})/f'(x_{n-1})$ converge al único cero real α de f en $[a, b]$.

Esto tiene un corolario interesante para el caso de un polinomio $f \in \mathbb{R}[X]$ del cual se sabe que todas sus raíces son reales (como en el caso que ya se mencionó del polinomio característico de una matriz simétrica por ejemplo) :

Corolario 53 *Sea $f \in \mathbb{R}[X]$ un polinomio mónico de grado m cuyas raíces $\alpha_1 < \alpha_2 < \cdots < \alpha_m$ son todas reales y distintas, y sea $x_0 \in \mathbb{R}$ tal que $x_0 > \alpha_m$ (la mayor de las raíces de f). Entonces la sucesión de Newton definida por $x_n := x_{n-1} - f(x_{n-1})/f'(x_{n-1})$ $(n \geq 1)$ converge a α_m.*

Prueba.– Dado que f es mónico (lo que no es restrictivo ya que las raíces de f coinciden con las de $\frac{f}{\mathrm{cp}(f)}$), se tiene que $\lim_{x \to +\infty} f(x) = +\infty$, ya que sino se puede reemplazar f por $-f$, lo que no cambia ni los ceros ni la sucesión de Newton.
En ese caso, $f(x_0) > 0$ ya que si fuera negativo, por el Teorema de Bolzano existiría otra raíz real de f mayor que α_m. Verificaremos las condiciones del Corolario 52 para $b := x_0$.

Como f tiene todas sus raíces simples, α_m no puede ser un cero doble, y para todo $x \in (\alpha_{m-1}, \alpha_m)$, se verifica $f(x) < 0$.
Más aún, como f tiene tantas raíces reales (distintas) como su grado, y entre dos raíces reales consecutivas de f siempre hay una raíz de f' (Teorema del valor intermedio), f' tiene también tantas raíces reales (distintas) como su grado y f'' también. Si llamamos β_{m-1} la mayor raíz real de f' y γ_{m-2} la mayor raíz real de f'', se tiene $\gamma_{m-2} < \beta_{m-1} < \alpha_m$.
Elijamos $a \in \mathbb{R}$ tal que $\beta_{m-1} < a < \alpha_m$, y $b := x_0$. Se tiene $f(a) < 0$, $f(b) > 0$. Además, dado que f es mónico, se observa que $\lim_{x \to +\infty} f'(x) > 0$ y $\lim_{x \to +\infty} f''(x) > 0$, por lo tanto $f'(x) > 0$ y $f''(x) > 0$ para todo $x \in [a, b]$ (pues a es mayor que la mayor de las raíces de f' y de f''). Se concluye aplicando el corolario.

■

Otro resultado clásico para la convergencia del método de Newton para polinomios (del cual no daremos demostración) es el siguiente :

Teorema 54 *Sea* $f \in \mathbb{R}[X]$ *y* $a < b \in \mathbb{R}$. *Sea* $x_0 \in [a,b]$ *tal que* $f'(x_0) \neq 0$ *y*

$$2\left|\frac{f(x_0)}{f'(x_0)^2}\right| \max_{x\in[a,b]} |f''(x)| \leq 1,$$

entonces existe una única raíz α *de* f *en el intervalo*

$$\left(x_0 - 2\left|\frac{f(x_0)}{f'(x_0)}\right|, x_0 + 2\left|\frac{f(x_0)}{f'(x_0)}\right|\right)$$

y el método de Newton inicializado en x_0 *converge a* α.

En todos los resultados mencionados, se requiere calcular el máximo de una derivada en un intervalo, y en general, para evitar cálculos se acota groseramente ese máximo.
Sin embargo, existe un resultado reciente debido a M.Shub y S.Smale ([6]) que permite reemplazar para un polinomio de grado n esa condición global por las $n-1$ condiciones puntuales siguientes :

$$\left|\frac{f(x_0)^{k-1} f^{(k)}(x_0)}{f'(x_0)^k}\right| \leq \left(\frac{1}{8}\right)^{k-1} \quad \text{para } 2 \leq k \leq n.$$

5.4.5 Rapidez de convergencia

Definición 55 *Sea* $(x_n)_{n\in\mathbb{N}_0}$ *una sucesión convergente, con límite* α.

- *Se dice que la convergencia es lineal si existe una constante* $c < 1 \in \mathbb{R}$, *tal que la sucesión* (x_n) *verifica la desigualdad :*
$$|\, x_n - \alpha \,| \leq c |\, x_{n-1} - \alpha \,|\,.$$
- *Se dice que la convergencia es de orden* $p \geq 2$ *si existe una constante* $c \in \mathbb{R}$ *tal que la sucesión* (x_n) *verifica la desigualdad :*
$$|\, x_n - \alpha \,| \leq c |\, x_{n-1} - \alpha \,|^p\,.$$
- *Si la sucesión se obtiene por un método, como los descriptos en las secciones anteriores, se dice que el método converge con orden* $p \geq 1$ *si existen* $a < \alpha < b$ *tal que para todo* $x_0 \in [a,b]$ *la sucesión construída a partir de* x_0 *converge a* α *con orden* p.

El orden de convergencia p de un método, junto con la constante c, determina la rapidez de la convergencia de la sucesión a α, o sea intuitivamente la cantidad de cifras significativas que se obtienen luego de calcular n términos de la sucesión.

La razón por la que se pide $c < 1$ en el caso $p = 1$, pero no para $p \geq 2$, es que se trata de evaluar la velocidad de convergencia de la sucesión (x_n) a α:

- En el caso $p = 1$, la desigualdad implica inductivamente que $|\, x_n - \alpha \,| \leq c^n |\, x_0 - \alpha \,| \leq c^n |\, b - a \,|$, e independientemente del valor de $|\, b - a \,|$, si c fuera ≥ 1, no se podría decir nada de la velocidad de la convergencia.
- En cambio, si $p \geq 2$, se obtiene la desigualdad

  $$|\, x_n - \alpha \,| \leq c^{1+p+\cdots+p^{n-1}} |\, x_0 - \alpha \,|^{p^n} \leq c^{\frac{p^n-1}{p-1}} |\, b - a \,|^{p^n}$$

  y eligiendo inicialmente $|\, b - a \,|$ suficientemente chico, por ejemplo, $|\, b - a \,| \leq c^{-2}$, se observa que independientemente del valor constante de c, se puede calcular la velocidad de convergencia.

Ejemplo El cálculo de $\sqrt{2}$:
En caso de usar el método de Newton-Raphson, se tenía $x_n := \frac{x_{n-1}}{2} + \frac{1}{x_{n-1}}$, para todo $x_0 \in [1,2]$.
Luego se tiene :

$$\begin{aligned}
\left| x_n - \sqrt{2} \right| &= \left| \frac{x_{n-1}}{2} + \frac{1}{x_{n-1}} - \sqrt{2} \right| \\
&= \left| \frac{{x_{n-1}}^2 + 2 - 2\sqrt{2}x_{n-1}}{2\, x_{n-1}} \right| \\
&= \frac{\left| x_{n-1} - \sqrt{2} \right|^2}{|\, 2x_{n-1}\,|} \\
&\leq \frac{1}{2} \left| x_{n-1} - \sqrt{2} \right|^2 .
\end{aligned}$$

Por lo tanto la convergencia del método es de orden ≥ 2, y resulta que $\left| x_n - \sqrt{2} \right| \leq \left(\frac{1}{2}\right)^{2^n - 1}$, por lo tanto en el paso n hay aproximadamente 2^{n-2} cifras significativas.

- **Velocidad de convergencia del método del punto fijo**

  Sea $g : [a,b] \longrightarrow [a,b]$ derivable con derivada continua, tal que, según la Definición 55, el método del punto fijo inicializado en $x_0 \in [a,b]$ arbitrario produce una sucesión que converge a α (o sea la sucesión (x_n) definida por $x_n := g(x_{n-1})$ converge a α).

  Por el Teorema del valor intermedio, se tiene $x_n - \alpha = g(x_{n-1}) - g(\alpha) = g'(\xi_{n-1})(x_{n-1} - \alpha)$ donde ξ_{n-1} se halla en el intervalo determinado por x_{n-1} y α. Luego la sucesión (ξ_n) también converge a α y, por la continuidad de g', $g'(\xi_n)$ converge a $g'(\alpha)$.

  Luego, si $|\, g'(\alpha)\,| < 1$, achicando si es necesario el intervalo $[a,b]$, se tendrá $|\, g'(\xi_n)\,| \leq c < 1$, y se deduce :

  $$|\, x_n - \alpha\,| \leq c\,|\, x_{n-1} - \alpha\,| \quad \text{con} \quad c < 1$$

  Por lo tanto en este caso (si $g'(\alpha) < 1$) el método resulta convergente de orden 1 (por lo menos).

  En el caso en que g es dos veces derivable, con derivada segunda continua, y además $g'(\alpha) = 0$, el desarrollo de Taylor alrededor de α da :

  $$|\, x_n - \alpha\,| = |\, g(x_{n-1}) - g(\alpha)\,| = \tfrac{|\, g''(\xi_{n-1})\,|}{2} |\, x_{n-1} - \alpha\,|^2$$

  y dado que $g''(\xi_n) \to g''(\alpha)$, esta sucesión resulta acotada. Por lo tanto, el método del punto fijo es de orden por lo menos 2.

- **Velocidad de convergencia del método de Newton**

  Sea $f : [a,b] \to [a,b]$ derivable tres veces con derivada tercera continua, con $f'(x) \neq 0$ para todo $x \in [a,b]$ y tal que el método de Newton inicializado en cualquier $x_0 \in [a,b]$ converge al cero α de f en el intervalo.

  Aplicando la discusión del método del punto fijo, se observa que $g(x) = x - \frac{f(x)}{f'(x)}$ implica $g'(x) = \frac{f(x)f''(x)}{(f'(x))^2}$. Por lo tanto $g'(\alpha) = 0$ y el método de Newton converge con orden por lo menos 2.

En el caso en que α es un cero no simple de f, se puede hacer una variante del método de Newton, pero se obtiene convergencia lineal a lo sumo :

Consideremos por ejemplo $f(X) = X^2$, y $x_0 = 1$. Definiendo la sucesión de Newton, se tiene $g(x) = x - \frac{f(x)}{f'(x)} = x - \frac{x^2}{2x} = \frac{x}{2}$ y por lo tanto $x_n = g(x_{n-1}) = \frac{1}{2^n}$. Aquí el método de Newton coincide con el método de la bisección y la convergencia es lineal.

References

[1] E.Berlekamp. *Factoring polynomials over large finite fields*, Math. Comp. 24 (1970) 713–735.

[2] E.Gentile. *Notas de Algebra*, Eudeba.

[3] S.Lang. *Algebra*, Addison-Wesley (1965).

[4] A.K.Lenstra, H.W.Lenstra, L.Lovász. *Factoring polynomials with rational coefficients*, Math. Ann. 261 (1982) 515–534.

[5] M.Mignotte. *Mathématiques pour le calcul formel*, Presses Universitaires de France (1989).

[6] M.Shub, S.Smale. *Computational Complexity : On the Geometry of Polynomial and Theory of Cost, I*, Annales Scientifiques de l'Ecole Normale Supérieure (4) 18 (1985) 107–142.

[7] B.L.van der Waerden. *Modern Algebra*, Frederick Ungar Publishing Co. NY (1953).

[8] H.Zassenhaus. *On Hensel Factorization I.*, J. Number Theory 1 (1969) 291–311.