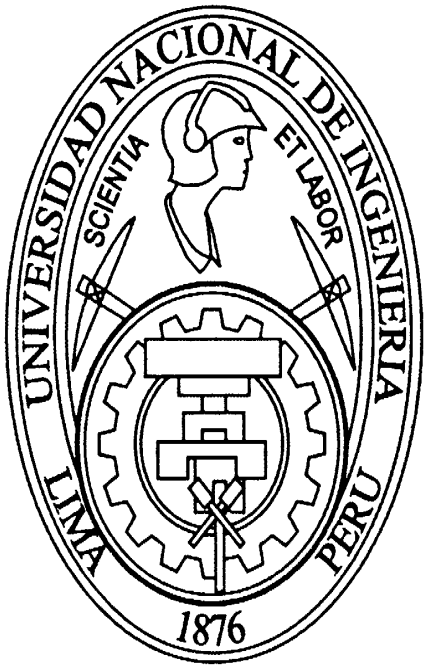
UNIVERSIDAD NACIONAL DE INGENIERÍA
FACULTAD DE CIENCIAS
ESCUELA PROFESIONAL DE MATEMÁTICA



Polinomios, Raíces y Algunas Aplicaciones en una Variable

por

Nerio Hermes Juscamayta Tineo

Tesis para Optar
el Título Profesional de
LICENCIADO en MATEMÁTICA

Prof. William Carlos Echegaray Castillo
Asesor

UNI, noviembre del 2009.

CIP - CATALOGO DE PUBLICACIÓN

Juscamayta Tineo, Nerio Hermes

Polinomios, Raíces y Algunas Aplicaciones en una Variable / Nerio Hermes Juscamayta Tineo. – EPM - FC - UNI, 2009.

63 p.: il.

Tésis (Licenciatura)—Universidad Nacional de Ingeniería, Facultad de Ciencias, Escuela Profesional de Matemática, Lima, 2009. Asesor: William Carlos Echegaray Castillo

A Mis hijos que son la luz de mi felicidad

Fiorella y Sebastian

Agradezco al Profesor William Carlos Echegaray Castillo por la orientación y sus sabios consejos para la culminación del presente trabajo y también deseo agradecer a Mabel Rosales por su amistad y ayuda en el tipeo del presente trabajo, y a todas aquellas personas que de una u otra forma me ayudaron a terminar este trabajo.

RESUMEN

El estudio de los polinomios tiene una connotada trascendencia, podemos en primer término decir que la aritmética de los polinomios en un cierto cuerpo es análoga a la de los enteros en cuanto a la divisibilidad, el algoritmo de la división, factorización, aparece la diferencia cuando se trata de estudiar sus raíces y su comportamiento. Los polinomios son vistos como entes matemáticos que tienen aplicaciones cuantiosas, entre ellos está, por ejemplo, hallar los valores propios de una matriz cuadrada, para resolver una ecuación diferencial lineal de orden n y de coeficientes constantes, y también ciertos fenómenos físicos y biológicos que se pueden modelar a travez de un polinomio.

El presente trabajo se divide en capítulos.

En el capítulo 1 se hace un concepto general de los polinomios.

En el capítulo 2 se enfoca el algoritmo de la división, para demostrar el teorema del resto, luego define la raíz de un polinomio. Se prueba el algoritmo de Euclides usando propiedades del máximo común divisor de polinomios.

Se define polinomios primos como polinomios irreducibles en un cierto cuerpo.

Si el polinomio tiene una cierta raíz en un determinado cuerpo $\mathbb{K}$, entonces el polinomio no necesariamente es reducible en dicho cuerpo. Se define las raíces múltiples de un polinomio y de las propiedades relacionadas con las derivadas del polinomio. Finalmente se concluye con el polinomio interpolador, para hallar los valores aproximados de ciertas funciones que no son polinomios.

En el capítulo 3 se estudia como punto de partida el teorema fundamental del álgebra, se prueba dicho teorema con conocimiento del análisis complejo, en resumen "cualquier polinomio en el anillo de los complejos de grado n, tiene n raíces", se logra dar una particularización detallada para polinomios cúbicos y cuárticos. Para polinomios de grado mayor o igual a 5, no existe una fórmula universal en radicales, esto se demuestra usando la teoría de Galois que es imposible expresar sus raíces, en general, de esta manera.

En el capítulo 4 se estudia las raíces de los polinomios en el anillo de los racionales y relaciona teoremas importantes para obtener las raíces racionales y se aplica procedimientos para identificar las raíces.

Se establece criterios para ver la irreducibilidad de polinomios en $\mathbb{Q}$. También se estudia un algoritmo para observar si un polinomio es o no irreducible en $\mathbb{Q}$, que es el algoritmo de Kronecker, que usa el polinomio interpolador.

En el capítulo 5 se estudia los polinomios en $\mathbb{R}$ y se da propiedades de las raíces en los complejos, destaca que todo polinomio en $\mathbb{R}$ se puede expresar como multiplicación de polinomios irreducibles de primero y segundo grado en $\mathbb{R}$. Se aplica el criterio de Descartes para dar el número de raíces positivas o negaticas.

Finalmente se concluye con el teorema de Sturm que permite localizar el número de raíces reales de un polinomio en un intervalo determinado de la recta numérica, luego se extiende este teorema para polinomios en $\mathbb{C}$, que nos permite indicar el número de raíces complejas que se hallan en cada cuadrante del plano complejo.

Índice general

1 POLINOMIOS Y RAÍCES

1.1. Introducción y Notaciones

1.1.1. Introducción

Cuando se plantea en términos matemáticos problemas de distintas áreas (economía, física, ingeniería, biología, etc.), alguna veces nos econtramos con el siguiente problema: El de encontrar los ceros de determinadas funciones, es decir, los valores para el cual la función se hace cero.

Después de las funciones lineales, las funciones polinomiales en una variable son las más simples. Analizar los ceros de funciones polinomiales son de gran interés al menos por la siguiente razón: no es posible resolver el problema para funciones más generales si no se logra resolver para el caso de los polinomios.

En algunas aplicaciones se trabaja con funciones reales y se trata de encontrar los ceros reales. Debido a la estructura de los números con los que trabajan las computadoras las funciones suelen tener coeficientes racionales y los ceros que se tratan de calcular serán números racionales que aproximen lo suficiente a la solución del problema.
En este estudio se trata de profundizar sobre las raíces de polinomios con coeficientes en $\mathbb{Q}$ (cuerpo de los números racionales), $\mathbb{R}$ (cuerpo de los números reales) y $\mathbb{C}$ (cuerpo de los números complejos).

Para realizar el estudio de este tema debemos conocer la teoría básica de polinomios en una variable. También se requiere nociones de análisis elemental, para el caso de funciones reales continuas y derivables.

1.1.2. Notaciones

$\mathbb{K}$ denotará un cuerpo cualquiera, pueder ser $\mathbb{Q}, \mathbb{R}$ ó $\mathbb{C}$ y $\mathbb{K}[x]$ denotará el anillo de los polinomios con coeficientes en $\mathbb{K}$, cuyos elementos son polinomios (de grado n)de la forma:

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \ , \ a_i \in \mathbb{K};\ 0 \leq i \leq n \ \text{ y } \ a_n \neq 0$$

- Si $f \neq 0$, se denotará con $gr(f)$ el grado del polinomio f, es decir, el máximo exponente n en los monomios no nulos de f.
- Se denotará con $cp(f)$ el coeficiente principal de f, es decir el coeficiente que acompaña a $x^{gr(f)}$. Si $cp(f) = 1$ se dice que f es mónico.
- La relación de divisibilidad se denota con /
  Sean $f, g \in \mathbb{K}[x]$, g/f (g divide a f)$\Leftrightarrow$ existe $q \in \mathbb{K}[x]$ tal que $f = qg$.
  En caso contrario g no divide a f y se denota por $g \nmid f$.
- Se dice que $\alpha \in \mathbb{K}$ es raíz de f si $f(\alpha) = 0$.

2 HECHOS GENERALES

Aquí se recuerdan los resultados básicos de la teoría de polinomios, que usaremos para exponer las teorías más específicas de los polinomios con coeficientes en $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$. La aritmética de los polinomios con coeficientes en un cuerpo $\mathbb{K}$ es similar a la de los enteros en cuanto a divisibilidad, algoritmo de división, factorización, etc. Surge la diferencia en cuanto se trata particularmente de estudiar las raíces de los polinomios y su comportamiento.

2.1. Algoritmo de División

Teorema 2.1. *Dados los polinomios $f, g \in \mathbb{K}[x]$, $g \neq 0$, existen dos únicos polinomios q (cociente) y r (resto) en $\mathbb{K}[x]$ tal que $f = qg + r$ con $r = 0$ ó $gr(r) < gr(g)$.*

Prueba*:*

Si $gr(f) < gr(g)$ no hay nada que probar, pues nada más tenemos que hacer $q(x) = 0$ y $r(x) = f(x)$ y ciertamente se tiene $f(x) = 0 \cdot g(x) + f(x)$.

Ahora supongamos que $f(x) = a_0 + a_1x + \cdots + a_mx^m$ y $g(x) = b_0 + b_1x + \cdots + b_nx^n$, con $a_m \neq 0$, $b_n \neq 0$ y $m \geq n$.
Sea $f_1(x) = f(x) - \dfrac{a_m}{b_n}x^{m-n}g(x)$, entonces $gr(f_1) = m - 1$.
Por inducción sobre el grado de f podemos suponer que $f_1(x) = t_1(x)g(x) + r(x)$ donde $r(x) = 0$ ó $gr(r) < gr(g)$, entonces $f(x) - \dfrac{a_m}{b_n}x^{m-n}g(x) = t_1(x)g(x) + r(x)$, lo cual nos dá $f(x) = \left[\dfrac{a_m}{b_n}x^{m-n} + t_1(x)\right] g(x) + r(x)$.
Si ponemos $t(x) = \dfrac{a_m}{b_n}x^{m-n} + t_1(x)$, tendremos que $f(x) = t(x)g(x) + r(x)$, donde $t, r \in \mathbb{K}[x]$ y $r(x) = 0$ ó $gr(r) < gr(g)$ lo que prueba el teorema. ■

Proposición 2.1 (Teorema del resto)**.** *Dado $f \in \mathbb{K}[x]$ y $\alpha \in \mathbb{K}$, se tiene*

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

Prueba*:*

Por el Teorema 1 podemos suponer que $f(x) = q(x)(x-\alpha) + R(x)$, donde $R = 0$ ó $gr(R) < 1$ (estamos tomando $g(x) = x - \alpha$) Si $R(x) = 0$ entonces se tiene $f(x) = q(x)\cdot(x-\alpha) \Rightarrow f(\alpha) = 0 \Rightarrow f(x) = q(x)\cdot(x-\alpha)+0 = q(x)(x-\alpha)+f(\alpha)$ (se cumple).

Si $gr(R) < 1 \Rightarrow gr(R) = 0$ implica que $R(x) = R \in \mathbb{K}$ $f(x) = q(x)\cdot(x-\alpha) + R$, evaluando para $x = \alpha$: $f(\alpha) = 0 + R \Rightarrow R = f(\alpha)$, luego $f(x) = q(x)(x-\alpha) + f(\alpha)$ Lo cual prueba la proposición. ■

Consecuencia 1

$\alpha \in \mathbb{K}$ es raíz de $f \Leftrightarrow f(\alpha) = 0 \Leftrightarrow (x-\alpha)/f \Leftrightarrow f(x) = (x-\alpha)\,q(x)$ para algún $q \in \mathbb{K}[x]$.

Ejemplos:

- f constante: $f(x) = c\,,\ c \in \mathbb{K}$.

  Luego o bien $c = 0$ y todo $\alpha \in \mathbb{K}$ es raíz de f, o bien $c \neq 0$ y f no tiene ninguna raíz en $\mathbb{K}$.

- f de grado 1: $f(x) = ax + b$; $a, b \in \mathbb{K}$, $a \neq 0$ entonces f tiene una raíz en $\mathbb{K}$ a saber $x = -\dfrac{b}{a}$.

- f es de grado 2:

  $f(x) = ax^2 + bx + c$, $\ a \neq 0\,,\ b\,,\ c \in \mathbb{K}$ suponiendo aquí que $2 \neq 0$ en $\mathbb{K}$ (característica de $\mathbb{K}$ es distinto de 2) luego

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

definimos el discriminante de f como $\Delta = b^2 - 4ac$. Así si existe un $\beta \in \mathbb{K}$ tal que $\beta^2 = \Delta$, se tiene

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

y se obtiene por raíces: $r_1 = \dfrac{-b+\beta}{2a}$ y $r_2 = \dfrac{-b-\beta}{2a}$.

- Cuando $\mathbb{K} = \mathbb{C}$, siempre existe $\beta \in \mathbb{C}$ tal que $\beta^2 = \Delta$, luego todo polinomio de grado 2 tiene 2 raíces en $\mathbb{C}$ (pueden ser distintas o repetidas cuando $\beta = 0$).

Cuando $\mathbb{K} = \mathbb{R}$, existe $\beta = \sqrt{\Delta}$ si y solo si $\Delta \geq 0$, luego si $\Delta \geq 0$ entonces el polinomio tiene dos raíces reales (distintos o repetidos si $\beta = 0$). Por otra parte existen polinomios en $\mathbb{R}[x]$ de grado 2 que no tienen raíces reales como $2x^2 + 4 = 0$.

Cuando $\mathbb{K} = \mathbb{Q}$, si Δ tiene una raíz cuadrada en $\mathbb{Q}$, entonces el polinomio tiene dos raíces racionales pero también existen polinomios de grado 2 en $\mathbb{Q}$ con raíces irracionales, como $x^2 - 8 = 0$, cuyas raíces son $r_1 = 2\sqrt{2}$ y $r_2 = -2\sqrt{2}$; $\quad r_1, r_2 \in \mathbb{I}$.

Lo que prueba este ejemplo de los polinomios de grado 2 en un cuerpo $\mathbb{K}$ de características distinto de 2 es una condición suficiente: si existe $\beta \in \mathbb{K}$ tal que $\beta^2 = b^2 - 4ac$, entonces $P(x) = ax^2 + bx + c$, $a \neq 0$ tiene dos raíces en $\mathbb{K}$. Falta aún investigar la reciproca. Posteriormente se verá que esta condición es necesaria y suficiente, es decir existe $\beta \in \mathbb{K}$ tal que $\beta^2 = b^2 - 4ac$ si y solo si $P(x) = ax^2 + bx + c$ tiene dos raíces en $\mathbb{K}$.

2.2. Máximo Común Divisor

Definición 2.1. *Sean $f, g \in \mathbb{K}[x]$ no nulos. El máximo común divisor entre f y g denotado por $mcd(f, g)$ es el (único) polinomio mónico $h \in \mathbb{K}[x]$ que verifica simultáneamente las dos condiciones siguientes:*

1. h/f y h/g
2. Si $\overline{h} \in \mathbb{K}[x]$ verifica $\overline{h}/f$ y $\overline{h}/g$, entonces $\overline{h}/h$

   Ejemplo: Sean $f, g \in \mathbb{K}[x], g \neq 0$.

   i) Sea $c \in \mathbb{K}\backslash\{0\} \rightarrow mcd(c, g) = 1$.

   ii) Si $g/f \rightarrow mcd(f, g) = \dfrac{g}{cp(g)}$.

Este último es evidente, pues como g/g y g/f y para cualquier otro divisor $\overline{g}$ de g y f se tiene que $\overline{g}/g \wedge \overline{g}/f$ se tiene que $mcd(f, g) = \dfrac{g}{cp(g)}$ (debe ser mónico).

El lema siguiente nos permitirá deducir un algoritmo para calcular el máximo común divisor de dos polinomios f y g.

Lema 2.1. *Sean $f, g \in \mathbb{K}[x]$, $g \neq 0$ y sean $q, r \in \mathbb{K}[x]$ con $f = qg + r$, entonces $mcd(f, g) = mcd(g, r)$.*

Prueba

Sea $d(x) = mcd(f, g)(x)$ y $d_0(x) = mcd(g, r)(x)$.

$d(x)/f(x)$ y $d(x)/g(x) \Rightarrow d(x)/\,[f(x) - q(x)g(x)]$.

Como $f(x) - q(x)g(x) = r(x) \rightarrow d(x)/r(x) \Rightarrow d(x)/d_0(x)$, por definición de d_0.

Recíprocamente $d_0/g(x)$ y $d_0/r(x) \Rightarrow d_0(x)/\,[q(x)g(x) + r(x)] \Rightarrow d_0(x)/f(x)$, además $d_0(x)/g(x) \Rightarrow d_0(x)/d(x)$.

$d_0(x)/d(x)$ y $d(x)/d_0(x) \therefore d(x) = d_0(x)$. ■

Observación 2.1 (Algoritmo de Euclides)**.** *Sean* $f, g \in \mathbb{K}[x]\backslash\{0\}$*, con* $gr(f) \geq gr(g)$*. Entonces* $mcd(f, g)$ *es el último resto* r_k *no nulo (dividido por su coeficiente principal para volverlo mónico) que aparece en la sucesión de divisiones siguientes:*

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

Del Lema anterior resulta

$mcd(f, g) = mcd(g, r_1) = mcd(r_1, r_2) = \ldots = mcd(r_{k-2}, r_{k-1}) = mcd(r_{k-1}, r_k) = r_k$, pues r_k / r_{k-1}.

Se toma $mcd(f, g) = \dfrac{r_k}{cp(r_k)}$.

A continuación despejamos r_k de la penúltima igualdad, y siguiendo hacia arriba despejamos sucesivamente $r_{k-1}, r_{k-2}, \ldots, r_2, r_1$ y se logra escribir r_k en la forma $r_k = s'f + t'g$ finalmente, dividiendo toda la expresión por $cp(r_k)$, se obtiene $s, t \in \mathbb{K}[x]$ tales que $mcd(f, g) = sf + tg$.

Ejemplo 2.1. *Sean los polinomios*

$$f(x) = x^5 + x^4 + 1 \quad y \quad g(x) = 2x^4 - x^3 - 2x^2 + 3x - 1.$$

Vamos a determinar $mcd(f, g)$*.*

SOLUCIÓN

$$f(x) = \left(\frac{1}{2}x + \frac{3}{4}\right) g(x) + r_1(x), \quad con \quad r_1(x) = \frac{7}{4}x^3 - \frac{7}{4}x + \frac{7}{4};$$

$$g(x) = \left(\frac{8}{7}x - \frac{4}{7}\right) r_1(x), \text{ con } q_2(x) = \frac{8}{7}x - \frac{4}{7} \text{ y } r_2(x) = 0.$$

Luego

$$mcd(f,g) = \frac{r_1(x)}{cp\,(r_1)} = x^3 - x + 1.$$

Podemos ver que $\quad r_1(x) = f(x) - \left(\frac{1}{2}x + \frac{3}{4}\right) g(x) \Rightarrow$

$$mcd(f,g) = \frac{r_1(x)}{\frac{7}{4}} = \frac{4}{7}f(x) - \frac{4}{7}\left(\frac{1}{2}x + \frac{3}{4}\right) g(x)$$

$$mcd(f,g) = \frac{4}{7}f(x) + \left(-\frac{2}{7}x - \frac{3}{7}\right) g(x).$$

Aqui encontramos los polinomios $S(x) = \frac{4}{7}$, $t(x) = -\frac{2}{7}x - \frac{3}{7}$

tal que $mcd(f,g) = sf(x) + tg(x)$. □

Corolario 2.1. *Si d es el máximo común divisor de los polinomios f y g,entonces es posible encontrar polinomios u y v tal que:*

$$d(x) = f(x)u(x) + g(x)v(x).$$

Prueba

Por el algoritmo de Euclides, se tiene la sucesión de las siguientes divisiones:

$$\begin{aligned}
f(x) &= g(x)q_1(x) + r_1(x), && gr(r_1) < gr(g)\\
g(x) &= r_1(x)q_2(x) + r_2(x), && gr(r_2) < gr(r_1)\\
r_1(x) &= r_2(x)q_3(x) + r_3(x), && gr(r_3) < gr(r_2)\\
&\vdots\\
r_{k-3}(x) &= r_{k-2}(x)q_{k-1}(x) + r_{k-1}(x), && gr(r_{k-1}) < gr(r_{k-2})\\
r_{k-2}(x) &= r_{k-1}(x)q_k(x) + r_k(x), && gr(r_k) < gr(r_{k-1})\\
r_{k-1}(x) &= r_k(x)q_{k+1}(x),
\end{aligned}$$

Si tomamos en consideración que $r_k(x) = d(x)$ y ponemos $u_1(x) = 1, v_1(x) = -q_k(x)$, entonces en la penúltima igualdad de la sucesión de la divisiones, obtenemos

$$d(x) = r_{k-2}u_1(x) + r_{k-1}(x)v_1(x)$$

sustituyendo la expresión $r_{k-1}(x)$ en términos de $r_{k-3}(x)$ y $r_{k-2}(x)$ en la antepenúltima igualdad, se obtiene

$$d(x) = r_{k-3}u_2(x) + r_{k-2}(x)v_2(x)$$

donde $u_2(x) = v_1(x)$, $v_2(x) = u_1(x) - v_1(x)q_{k-1}(x)$, continuando el proceso en forma sucesiva obtenemos:

$$d(x) = f(x)u(x) + g(x)v(x).$$

■

Ejemplo 2.2. *Hallaremos los polinomios u y v el cual satisface la propiedad para $f(x) = x^3 - x^2 + 3x - 10$, $g(x) = x^3 + 6x^2 - 9x - 14$.*

SOLUCIÓN

Aplicamos el Algoritmo de Euclides a dichos polinomios, obteniéndose: $f(x) = g(x)+(-7x^2+12x+4)$, $g(x) = (-7x^2 + 12x + 4)\left(-\frac{1}{7}x - \frac{54}{49}\right) + \frac{235}{49}(x - 2)$, como $-7x^2 + 12x + 4 = (x - 2)(-7x - 2)$, con ello obtenemos que $mcd(f, g) = x - 2$ y que

$$u(x) = \frac{7}{235}x + \frac{54}{235} \quad \text{y} \quad v(x) = -\frac{7}{235}x - \frac{5}{235}$$

y $x - 2 = f(x)u(x) + g(x)v(x)$. □

Aplicando la demostración del corolario (2.1) para polinomios primos relativos, se obtiene el siguiente resultado:

los polinomios f y g son primos relativos, si es posible encontrar polinomios u y v

tal que

$$f(x)u(x) + g(x)v(x) = 1$$

2.2.1. POLINOMIOS PRIMOS ENTRE SI

Definición 2.2. *Dos polinomios f y $g \in \mathbb{K}[x]$ son primos entre si (coprimos) si verifican $mcd(f,g) = 1$, o sea ningún polinomio de grado ≥ 1 divide simultáneamente a f y g; o en forma equivalente si existen polinomios $s,t \in \mathbb{K}[x]$ tales que $1 = sf+tg$.*

Proposición 2.2. *Sean $f,g,h \in \mathbb{K}[x]$, entonces:*

1. *f/h, g/h y f,g primos entre si $\Rightarrow fg/h$*
2. *f/gh y f,g primos entre si $\Rightarrow f/h$*

Prueba

Como f y g primos entre si $\Rightarrow mcd(f,g) = 1 \Rightarrow \exists \quad s,t \in \mathbb{K}[x]$ tal que $1 = sf + tg \quad$ luego $\; h = sfh + tgh \qquad (*)$

1. $\Rightarrow \dfrac{h}{fg} = \dfrac{sh}{g} + \dfrac{th}{f} = sq_1 + tq_2, \quad q_1, q_2 \in \mathbb{K}[x] \therefore fg/h.$
2. Es claro que f divide a cada sumando de $(*) \therefore f/h$

Proposición 2.3. *Sean $f,g \in \mathbb{K}[x]$ entonces $\dfrac{f}{mcd(f,g)}$ y $\dfrac{g}{mcd(f,g)}$ son coprimos.*

Prueba

Sea $mcd(f,g) = d$, como $d/f \Rightarrow \ni \quad p \in \mathbb{K}[x] : f = pd$

Asimismo $d/g \Rightarrow \exists \quad q \in \mathbb{K}[x] : g = qd$

Además por propiedad existen $s,t \in \mathbb{K}[x]$ tal que $d = sf + tg \;\Rightarrow d = spd + tqd \Rightarrow$ $1 = sp + tq$ de aqui $mcd(p,q) = mcd\left(\frac{f}{d}, \frac{g}{d}\right) = 1$.

luego $\frac{f}{d}$ y $\frac{g}{d}$ son primos entre si. ■

2.3. Factorización de Polinomios

Definición 2.3. *Sea $f \in \mathbb{K}[x]$, no constante $(gr(f) \geq 1)$. Se dice que f es irreducible si y solo si no existe ningún $g \in \mathbb{K}[x]$ con $1 \leq gr(g) < gr(f)$ además g/f, o en forma equivalente, no existen polinomios $g, h \in \mathbb{K}[x]$(no constantes) ambos de grados estrictamente menor que el de f tal que $f = gh$. De lo contrario, se dice que f es reducible, esto es cuando existe $g \in \mathbb{K}[x]$ no constante y de grado estrictamente menor que el de f tal que g/f.*

Ejemplo 2.3.

1. *$4x^2 - 1$ es reducible en $\mathbb{Q}[x], \mathbb{R}[x]$ y $\mathbb{C}[x]$ pues $2x + 1/4x^2 - 1$ y $1 = gr(2x + 1) < gr(4x^2 - 1)$*

2. *Cualquier polonomio f de grado 1 en $\mathbb{K}[x]$ es irreducible en $\mathbb{K}[x]$, pues no existe otro polinomio g tal que $1 \leq gr(g) < gr(f) = 1$*

3. *$x^4 + 2$ es irreducible en $\mathbb{Q}[x]$ y $\mathbb{R}[x]$ de lo contrario sería el producto de 4 polinomios de grado 1 y por tanto tendría raíces en $\mathbb{Q}$ o en $\mathbb{R}$.*
   Pero podemos ver que $x^4 + 2$ es reducible en $\mathbb{C}$ pues
   $x^4 + 2 = (x^2 + \sqrt{2}i)(x^2 - \sqrt{2}i) = \left(x + \frac{1}{\sqrt[4]{2}} - \frac{1}{\sqrt[4]{2}}i\right)\left(x - \frac{1}{\sqrt[4]{2}} + \frac{1}{\sqrt[4]{2}}i\right)\left(x - \frac{1}{\sqrt[4]{2}} - \frac{1}{\sqrt[4]{2}}i\right)\left(x + \frac{1}{\sqrt[4]{2}} + \frac{1}{\sqrt[4]{2}}i\right)$
   luego es reducible en $\mathbb{C}[x]$ y tiene 4 raíces en $\mathbb{C}$ a saber
   $-\frac{1}{\sqrt[4]{2}} + \frac{1}{\sqrt[4]{2}}i\ ;\ \frac{1}{\sqrt[4]{2}} - \frac{1}{\sqrt[4]{2}}i\ ;\ -\frac{1}{\sqrt[4]{2}} - \frac{1}{\sqrt[4]{2}}i$ y $\frac{1}{\sqrt[4]{2}} + \frac{1}{\sqrt[4]{2}}i$

4. *El polinomio $x^4 + 4x^2 + 3$ es reducible en $\mathbb{Q}[x]$ o $\mathbb{R}[x]$, pues se expresa como $(x^2 + 3)(x^2 + 1)$ sin embargo no tiene raíces en estos cuerpos.*

5. *Todo polinomio $f \in \mathbb{K}[x]$ de grado no menor a dos que tiene una raíz $\alpha \in \mathbb{K}$ es reducible, pues $(x - \alpha)/f$ con $1 = gr(x - \alpha) < gr(f)$. La recíproca por lo general es falsa, f puede ser reducible sin tener ninguna raíz en $\mathbb{K}$ (al menos para $\mathbb{K} = \mathbb{Q}$ ó $\mathbb{R}$).*

PROPIEDAD 2.1 (PRIMALIDAD DE LOS POLINOMIOS IRREDUCIBLES)**.** *Sean $f, g, h \in \mathbb{K}[x]$, con f irreducible, entonces:*

1. $mcd(f,g) = \dfrac{f}{cp(f)}$ *si* f/g *y* $mcd(f,g) = 1$ *si* $f \nmid g$
2. $f/gh \Rightarrow f/g$ *ó* f/h

Prueba

1. i) Si f/g entonces $\exists\, q \in \mathbb{K}[x] : g = qf$ por teorema (2.1) $\exists\, s, t \in \mathbb{K}[x]$ y $mcd(f,g) = sf + tg \Rightarrow mcd(f,g) = mcd(f, qf) = sf + tqf \Rightarrow mcd(f,g) = f \cdot (s \cdot 1 + tq) = f\ mcd(1,q) = f$.
   Por definición: $mcd(f,g) = \dfrac{f}{p(f)}$

   ii) Si $f \nmid g$, entonces g no contiene como factor a f, (dado que f es irreducible) luego f y g son coprimos, en consecuencia $mcd(f,g) = 1$

2. Si $g(x) = 0$ o bien $h(x) = 0$ el resultado es obvio. Si ninguno es idénticamente nulo, supongamos que $f(x) \nmid g(x)$ debemos probar que $f(x)/h(x)$. La suposición que $f(x) \nmid g(x)$ implica que $mcd(f,g) = 1$ y de aquí existen los polinomios $r, s \in \mathbb{K}[x]$ tal que
$$1 = rf + sg \Rightarrow h = hfr + shg.$$

Ahora bien f es un divisor del segundo miembro de esta igualdad debido a que f/gh. Luego f/h. ■

Teorema 2.2. *(Teorema fundamental de la aritmética) Sea $\mathbb{K}$ un cuerpo, y sea $f \in \mathbb{K}[x]$ un polinomio no constante, luego existen únicos polinomios irreducibles mónicos distintos $g_1, \ldots, g_m \in \mathbb{K}[x]$ de manera que $f = cg_1^{k_1}, g_2^{k_2} \ldots g_m^{k_m}$, donde $c \in \mathbb{K}\backslash\{0\}$ y $k_1, \ldots, k_m \in \mathbb{N}$.*

Prueba

Si f es primo en $\mathbb{K}[x]$ no hay nada que probar pues $f(x) = cf_1(x)$ donde $c \in \mathbb{K}\backslash\{0\}$ y $f_1 \in \mathbb{K}[x]$ es mónico irreducible.

Si f no es primo en $\mathbb{K}[x]$ (reducible) entonces f se puede factorizar como un producto de polinomios mónicos distintos $g_1, g_2 \dots g_\ell \in \mathbb{K}[x]$ de manera que $f(x) = cg_1(x), g_2(x) \dots g_\ell(x)$, pero entre estos factores g_i pueden existir factores que se repiten, entonces se estará expresando los que se repiten, a algunas potencias enteras, por lo tanto la forma general que puede adoptar f es:

$$f(x) = cg_1^{k_1}(x), g_2^{k_2}(x) \dots g_m^{k_m}(x) \quad , \quad m \leq \ell$$

donde $c \in \mathbb{K}\backslash\{0\}$ y $k_1, k_2, \dots, k_m \in \mathbb{N}$.
Claramente la unicidad de los factores irreducibles g_i se dá , salvo al orden de los factores, c resulta ser el coeficiente principal de f.

Ejemplo 2.4. *El polinomio* $F(x) = (x^2 + 4)^2(x^2 - 3)$ *está expresado en factores irreducibles en* $\mathbb{Q}[x]$ *pero su factorización en* $\mathbb{R}[x]$ *es* $(x^2 + 4)^2(x + \sqrt{3})(x - \sqrt{3})$*, y su factorización en* $\mathbb{C}[x]$ *es* $(x + 2i)^2(x - 2i)^2(x + \sqrt{3})(x - \sqrt{3})$. □

Observación 2.2. *Si* $f \in \mathbb{K}[x]$ *tiene una raíz* $\alpha \in \mathbb{K}$*, entonces el polinomio* $(x - \alpha)$ *es uno de los factores irreducibles de* f*, pues* $f(x) = (x - \alpha)q(x)$ *y para factorizar* f *alcanza con factorizar* q*.*

Ahora viendo para los polinomios de grado 2: podemos mostrar que si $f(x) = ax^2 + bx + c$, tiene una raiz en $\mathbb{K}$ (con características $\mathbb{K} \neq 2$) entonces $b^2 - 4ac$ es un cuadrado en $\mathbb{K}$, con esto concluimos la demostración de la afirmación: "existe $\beta \in \mathbb{K}$ tal que $\beta^2 = b^2 - 4ac$ si y solo si el polinomio $f(x) = ax^2 + bx + c$ tiene dos raíces en $\mathbb{K}$".

Sea $f(x) = ax^2 + bx + c$, tiene una raíz $\alpha_1 \in \mathbb{K}$, entonces por la observación anterior, $x - \alpha_1$ aparece en la factorización de f, por consiguiente el otro factor mónico es $(x - \alpha_2)$, y f se puede escribir

$$f(x) = a(x - \alpha_1)(x - \alpha_2) = ax^2 - a(\alpha_1 + \alpha_2)x + \alpha_1\alpha_2 a.$$

Igualando coeficientes se obtiene:
$b = -a(\alpha_1 + \alpha_2)$, $c = a\alpha_1\alpha_2$, $b^2 - 4ac = a^2(\alpha_1 + \alpha_2)^2 - 4a^2\alpha_1\alpha_2 = a^2(\alpha_1^2 + 2\alpha_1\alpha_2 + \alpha_2^2 - 4\alpha_1\alpha_2) = \alpha^2(\alpha_1 - \alpha_2)^2$ y resulta ser un cuadrado en $\mathbb{K}$.

Finalmente podemos escribir el máximo común divisor de dos polinomios f y g en términos de sus factores irreducibles mónicos de sus factorizaciones.

Observación 2.3. *Sean $f, g \in \mathbb{K}[x]$, entonces $mcd(f, g)$ es el producto de los factores irreducibles mónicos que aparecen en común en los factorizaciones de f y g, elevados a la mínima potencia con que aparecen.*

Ejemplo 2.5. $f(x) = 5x^2(x-2)^3(x+1)$.

$g(x) = 2x^2(x-2)^2(x-1)$.

$\Rightarrow mcd(f, g) = x^2(x-2)^2$.

La observación precedente puede parecer a simple vista un algoritmo para calcular el *mcd* entre dos polinomios, incluso más simple que el algoritmo de Euclides, pero realmente no es así, pues no se conocen métodos genéricos para factorizar polinomios, por lo menos en que $\mathbb{K}$ sea $\mathbb{R}$ ó $\mathbb{C}$.

2.4. Raíces Multiples

Los polinomios pueden tener raíces repetidas. Como por ejemplo, $P(x) = x^2 - 4x + 4 = (x-2)^2$ tiene dos veces la raíz 2 (todo polinomio de grado 2 con discriminante cero tiene las raíces repetidas).

Definición 2.4. *Sea $f \in \mathbb{K}[x]$ y $\alpha \in \mathbb{K}$ raíz de f, se dice que:*

- *α es raíz simple de f si y solo si $f(\alpha) = 0$ pero $(x-\alpha)^2 \nmid f(x)$ o sea $f(x) = (x-\alpha)q(x)$ con $q(\alpha) \neq 0$*

- α *es raíz doble de* f *si y solo si* $(x-\alpha)^2/f$*, o sea* $f(x)=(x-\alpha)^2q(x)$ *con* $q(\alpha)\neq 0$

- α *es raíz de multiplicidad* k *de* f *si y solo si* $(x-\alpha)^k/f(x)$ *pero* $(x-\alpha)^{k+1}\nmid f$*, o sea* $f(x)=(x-\alpha)^kq(x)$ *con* $q(\alpha)\neq 0$

Ejemplo 2.6. *Sea* $f(x)=2x^2(x+1)(x^2-1)^3=2x^2(x+1)^4(x-1)^3$

"0" es raíz doble, -1 *es raíz cuadruple y* 1 *es raíz triple de* f*.*

Ahora veremos que existe una relación entre la multiplicidad de una raíz y el hecho de ser raíz de la derivada f' del polinomio f.

Proposición 2.4. *Sea* $\mathbb{K}$ *un cuerpo de característica* 0 *(es decir* $p\neq 0$ *en* $\mathbb{K}$ *para todo* p *número primo), por ejemplo* $\mathbb{K}=\mathbb{Q}$, $\mathbb{R}$ *ó* $\mathbb{C}$*, que son los casos que nos interesan.*

Sea $f\in\mathbb{K}[x]$ *no nulo. Denotaremos con* f' *la derivada del polinomio* f *y con* $f^{(i)}$ *la* i*-ésima derivada de* f*, para todo* $i\in\mathbb{N}$*, no olvidemos también que* $f^{(0)}=f$*.*

1. α *es raíz doble de* $f\Leftrightarrow\alpha$ *es simultáneamente raíz de* f *y de* f'*. (Equivalentemente,* α *es raíz simple de* $f\Leftrightarrow f(\alpha)=0$ *y* $f'(\alpha)\neq 0$*)*

2. α *es raíz de múltiplicidad* k *de* f $(k\geq 2)\Leftrightarrow\alpha$ *es raíz de* f *y además es raíz de multiplicidad* $(k-1)$ *de* f'

3. α *es raíz de multiplicidad exactamente* k *de* f $(k\geq 1)\Leftrightarrow$
   $f(\alpha)=f'(\alpha)=\ldots=f^{(k-1)}_{(\alpha)}=0$ *y* $f^{(k)}_{(\alpha)}\neq 0$

Prueba

1. $\Rightarrow) f(x)=(x-\alpha)^2q(x)$, luego $f'(x)=2(x-\alpha)q(x)+(x-\alpha)^2q'(x)$.
   $f'(x)=(x-\alpha)[2q(x)+(x-\alpha)q'(x)]$ y se verifica que $f(\alpha)=f'(\alpha)=0$

$\Leftarrow$) como α es raíz de f, se puede escribir $f(x) = (x-\alpha)q(x)$, debemos mostrar entonces que $q(\alpha) = 0$, osea que $(x-\alpha)^2/f$:
como $f'(x) = (x-\alpha)q'(x) + q(x)$ y por condición $f'(\alpha) = 0$ implica en forma inmediata que $q(\alpha) = 0$.

2. $\Rightarrow$)$f(x) = (x-\alpha)^k q(x)$ con $q(\alpha) \neq 0$, de donde
$f'(x) = k(x-\alpha)^{k-1}q(x)+(x-\alpha)^k q'(x) = (x-\alpha)^{k-1}[kq(x)+(x-\alpha)q'(x)]$,
tomando $h(x) = kq(x) + (x-\alpha)q'(x)$, se verifica que
$f'(x) = (x-\alpha)^{k-1}h(x)$ con $h(\alpha) \neq 0$ (pues $q(\alpha) \neq 0$ y en un cuerpo de características 0).

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

   Sea $f(x) = (x-\alpha)^r q(x)$, con $q(\alpha) \neq 0$. Luego
   $f'(x) = r(x-\alpha)^{r-1}q(x)+(x-\alpha)^r q'(x) = (x-\alpha)^{r-1}[rq(x)+(x-\alpha)q'(x)]$
   tomando $h(x) = rq(x) + (x-\alpha)q'(x)$.

   $f'(x) = (x-\alpha)^{r-1}h(x)$, con $h(\alpha) \neq 0$, pues $q(\alpha) \neq 0$, por consiguiente α es raíz de multiplicidad $r-1$ de f', pero por hipótesis, la multiplicidad de f' es $k-1$, por lo tanto $r-1 = k-1 \ \therefore \ r = k$.

3. Podemos probarlo formalmente, usando la induccion en la multiplicidad k de α como raíz de f.

   a) Si $k = 1$: es inmediato ver que α es raíz simple de $f \Leftrightarrow \alpha$ es raíz de f y no raíz de $f' \Rightarrow f(\alpha) = 0$

   b) Si $k > 1$: Por $(2), \alpha$ es raíz de multiplicidad k de $f \Leftrightarrow f(\alpha) = 0$ y α es raíz de multiplicidad $k-1$ de f'.
   Por hipótesis inductiva, α es raíz de multiplicidad $k-1$ de $f' \Leftrightarrow \ f'(\alpha) = (f')'(\alpha) = f"(\alpha) = (f''')'(\alpha) = f'''(\alpha) = \ldots = (f')^{k-2}(\alpha) = f^{k-1}(\alpha) = 0$ y $(f')^{k-1}(\alpha) \neq 0$

■

2.5. Cantidad de Raíces

Un polinomio no nulo de grado n no puede tener un número ilimitado de raíces, aún contados con sus multiplicidades.

Teorema 2.3. *Sea $f \in \mathbb{K}[x]$ no nulo de grado n. Entonces f tiene a lo sumo n raíces en $\mathbb{K}$ contados cada raíz con su multiplicidad.*

Prueba

Haciendo la prueba por inducción sobre el grado n de f.

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

■

Observación 2.4. *Sea $f \in \mathbb{K}[x]$ y sean $\alpha_1, \ldots, \alpha_m \in \mathbb{K}$ raíces distintas de f de multiplicidad $k_1, \ldots, k_m$ respectivamente, entonces:*

$$(x - \alpha_1)^{k_1}(x - \alpha_2)^{k_2} \ldots (x - \alpha_m)^{k_m} / f.$$

(Esto es debido a que $(x - \alpha_1)^{k_1}/f, \ldots, (x - \alpha_m)^{k_m}/f$, y al ser los polinomios de la izquierda primos entre si dos a dos (no tiene ningún factor irreducible en común), su producto también divide a f.

2.6. Polinomio Interpolador

Aqui supondremos que el cuerpo tiene característica 0, como $\mathbb{K} = \mathbb{Q}, \mathbb{R}$ ó $\mathbb{C}$.

Nuestro propósito es mostrar que siempre existe, y es único, un polinomio de grado $\leq n$ que pasa por $(n+1)$ puntos prefijados del plano $\mathbb{K}^2$ con distintas abscisas. Así en $\mathbb{R}^2$ hay una única recta que pasa por dos puntos distintos, hay una única parábola que pasa por tres puntos con distintas abscisas a menos que estén alineados, en ese caso en lugar de parábola pasa una recta, etc.
Podemos probarlo de distintas maneras, usando resultados sencillos de algebra lineal, usando el determinante de Vandermonde, ó aplicando la fórmula de interpolación de Newton, ó 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 abscisas, pero sobre el valor del polinomio y sus n primeras derivadas en un punto $x_0 \in \mathbb{K}$, se obtiene 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 2.4. *(Interpolación de Lagrange) Sea $\mathbb{K}$ un cuerpo de característica cero, y, sean $x_0, x_1, \ldots, x_n$; $n+1$ puntos distintos de $\mathbb{K}$. Para cada elección $y_0, y_1, \ldots, y_n$ de $n+1$ puntos cualesquiera de $\mathbb{K}$ existe un único polinomio $f \in \mathbb{K}[x]$ de $gr(f) \leq n$ que verifica simultáneamente las condiciones.*

$$f(x_0) = y_0, f(x_1) = y_1, \cdots f(x_n) = y_n.$$

Prueba

1. **Existencia del polinomio interpolador**

   Construimos los polinomios f_j $(0 \leq j \leq n)$ de grado $\leq n$ que cumplen las condiciones $f_j(x_j) = 1$ y $f_j(x_i) = 0$, si $i \neq j$. Así los polinomios $y_j f_j$

verificarán 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 se puede expresar como $f = y_0 f_0 + \ldots + y_n f_n$ cumplirá que $f(x_j) = (y_0 f_0 + \ldots + y_n f_n)_{(x_j)} = y_0 f_0(x_j) + \ldots + y_n f_n(x_j) = y_j$ para todo $0 \leq j \leq n$, construyamos por ejemplo f_0, los demás se construyen en forma similar.

$f_0(x_0) = 1, \qquad f_0(x_1) = f_0(x_2) = \ldots = f_0(x_n) = 0$, o sea f tiene n raíces distintas $x_1, \ldots, x_n$. Se puede plantear entonces f_0 como el polinomio de grado n: $f_0(x) = c(x - x_1) \ldots (x - x_n)$, puede determinar la constante c como $f_0(x_0) = 1 \Rightarrow c = [(x_0 - x_1) \ldots (x_0 - x_n)]^{-1}$.

$$\Rightarrow f_0(x) = \frac{(x - x_1) \ldots (x - x_n)}{(x_0 - x_1) \ldots (x_0 - x_n)} = \prod_{\substack{0 \leq i \leq n \\ i \neq 0}} \frac{(x - x_i)}{(x_0 - x_i)}.$$

De igual forma se obtiene para cada j

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

Finalmente, se define f en la forma:

$$f(x) = y_0 f_0(x) + \ldots + y_n f_n(x) = \sum_{0 \leq j \leq n} y_j \prod_{\substack{0 \leq i \leq n \\ i \neq j}} \frac{x - x_i}{x_j - x_i}$$

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

2. **Unicidad del polinomio interpolador**

Supongamos que existen polinomios f y g no nulos de grado $\leq n$ que verifican las $n + 1$ condiciones $f(x_j) = y_j = g(x_j) \quad (0 \leq j \leq n)$.

Definamos el polinomio $h = f - g$, cuyo $gr(h) \leq n$ y además verifica las $n+1$ condiciones $h(x_j) = f(x_j) - g(x_j) = 0$, para todo j, es decir, h

tiene $n+1$ raíces distintas. Luego el único polinomio que satisface estas condiciones es el polinomio nulo, es decir, $h \equiv 0$, por tanto, $f = g$.

■

Nota 2.1. *Interpolar significa estimar un valor desconocido de una función en un punto, tomando una media ponderada de sus valores conocidos en puntos cercanos al dado. Cuando las ordenadas y_k vienen dadas por $y_k = f(x_k)$, el proceso de utilizar $P(x)$ para aproximar $f(x)$ en un intervalo $[x_k, x_{k+1}]$ se conoce con el nombre de interpolación*

Ejemplo 2.7. *Calcular el polinomio de grado ≤ 4 que verifica las condiciones*

$$f(-1) = 0, f(0) = 1, \quad f(2) = -2, f(3) = 2, f(-2) = 4.$$

SOLUCIÓN

Usando la interpolación de Lagrange:

$$\begin{aligned} f(x) &= 0 \cdot \frac{(x-0)(x-2)(x-3)(x+2)}{(-1-0)(-1-2)(-1-3)(-1+2)} + \\ & 1 \cdot \frac{(x+1)(x-2)(x-3)(x+2)}{(0+1)(0-2)(0-3)(0+2)} + \\ & -2\frac{(x+1)(x-0)(x-3)(x+2)}{(2+1)(2-0)(2-3)(2+2)} + \\ & 2\frac{(x+1)(x-0)(x-2)(x+2)}{(3+1)(3-0)(3-2)(3+2)} + \\ & 4\frac{(x+1)(x-0)(x-2)(x-3)}{(-2+1)(-2-0)(-2-2)(-2-3)} \end{aligned}$$

$$\Rightarrow f(x) = \frac{1}{12}(x+1)(x-2)(x-3)(x+2) + \frac{1}{12}x(x+1)(x-3)(x+2)$$

$$+\frac{1}{30}x(x+1)(x-2)(x+2) + \frac{1}{10}x(x+1)(x-2)(x-3)$$

$$\therefore f(x) = \frac{1}{30}(x+1)(9x^3 - 25x^2 - 11x + 30) \qquad \square$$

Ejemplo 2.8. *El polinomio interpolador de Lagrange cuadrático en los puntos* (x_0, y_0) , (x_1, y_1) *y* (x_2, y_2) *es:*

$$P_2(x) = y_0\frac{(x-x_1)(x-x_2)}{(x_0-x_1)(x_0-x_2)} + y_1\frac{(x-x_0)(x-x_2)}{(x_1-x_0)(x_1-x_2)} +$$

$$y_2\frac{(x-x_0)(x-x_1)}{(x_2-x_0)(x_2-x_1)}$$

$\square$

3 POLINOMIOS EN $\mathbb{C}[X]$

3.1. Teorema Fundamental del Álgebra

Este Teorema fue dado por Gauss (1777-1855) quien dio cinco demostraciones distintas. En la actualidad, existe decenas de demostraciones. Cabe mencionar que las demostraciones que se usan citan en alguna medida resultados elementales de análisis.

Teorema 3.1 (Teorema Fundamental del Álgebra)**.** *Sea $f \in \mathbb{C}[x]$ un polinomio no nulo de grado n mayor o igual a 1. Entonces f tiene por lo menos una raíz en $\mathbb{C}$, o equivalentemente, f tiene exactamente n raíces contadas con sus multiplicidades.*

Esto significa que la factorización de $f \in \mathbb{C}[x]$ toma la forma:
$f(x) = c(x-\alpha_1)^{k_1} \dots (x-\alpha_m)^{k_m}, c \in \mathbb{C}\backslash\{0\}$ *y que los únicos polinomios irreducibles en $\mathbb{C}[X]$ son los de grado 1.*

Prueba

$$\text{Sea } f \in \mathbb{C}[x], f(x) = a_0 + \sum_{i=1}^{n} a_i x^i / a_n \neq 0.$$

Será suficiente probar que $f(x)$ tiene al menos una raíz en $\mathbb{C}$.

Supongamos que $f(x) \neq 0$ para todo $x \in \mathbb{C}$

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

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

$$\Rightarrow \frac{1}{x} = \frac{f(x)}{xf(x)} = \frac{xQ(x)}{xf(x)} + \frac{a_0}{xf(x)} = \frac{Q(x)}{f(x)} + \frac{a_0}{xf(x)}$$

como $\dfrac{Q(x)}{f(x)}$ es analítica en $\mathbb{C}$, entonces por el teorema de Cauchy-Goursat

$\int_\gamma \frac{Q(x)}{f(x)} = 0$, $\forall\, \gamma$ contorno simple cerrado, en $\mathbb{C}$, sea

$$\gamma : |x| = \gamma \Rightarrow \int_\gamma \frac{dx}{x} = \int_\gamma \frac{Q(x)}{f(x)}dx + \int_\gamma \frac{a_0}{xf(x)}dx \tag{3.1}$$

Pero $\int_\gamma \frac{Q(x)}{f(x)}dx = 0$ y $\int_\gamma \frac{dx}{x} = 2\pi i$, aplicando $\int_\gamma \frac{f(x)}{x-a}dx = 2\pi i f(a)$.

En (3.1):

$$2\pi i = 0 + \int_\gamma \frac{a_0}{xf(x)}dx \Rightarrow \int_\gamma \frac{a_0}{xf(x)}dx = 2\pi i \tag{3.2}$$

Por otro lado

$$\frac{f(x)}{a_n x^n} = 1 + \frac{a_{n-1}}{a_n}x^{-1} + \ldots + \frac{a_0}{a_n}x^{-n}$$

$\lim\limits_{|x|=r\to\infty} \frac{f(x)}{a_n x^n} = 1$, cuando r grande $\left|\frac{f(x)}{a_n x^n}\right| > \frac{1}{2} \Rightarrow \frac{1}{|f(x)|} < \frac{2}{|a_n|\ |x|^n}$

$\Rightarrow \frac{1}{|f(x)|} < \frac{2}{|a_n| r^n}$

$\Rightarrow$ de (3.2):
$|2\pi i| = \left|\int_\gamma \frac{a_0}{xf(x)}dx\right| \leq \int_\gamma \frac{|a_0|}{|x|\ |f(x)|}|dx| < \frac{|a_0|\cdot 2}{r|a_n|r^n}\int_\gamma dx = \frac{2|a_0|2\pi r}{|a_n|r^{n+1}} = \frac{4|a_0|\pi}{|a_n|r^n}; 2\pi < \frac{4\pi|a_0|}{|a_n|r^n}$

si $r \to \infty \Rightarrow 2\pi < 0 (\Rightarrow \Leftarrow)$ $\quad \therefore f(x)$ tiene al menos una raíz.

Aplicaciones del Teorema Fundamental del Álgebra:

1. Si tenemos la ecuación cúbica:

$$y^3 + ay^2 + by + c = 0 \tag{3.3}$$

con coeficientes complejos.

Haciendo el sguiente cambio de variable

$$y = x - \frac{a}{3} \tag{3.4}$$

obtenemos la siguiente ecuación

$$x^3 + px + q = 0. \tag{3.5}$$

Con las raíces de (3.5), podemos encontrar las raíces de (3.3) usando (3.4).

Sabemos por el teorema fundamental (3.1) que (3.5) tiene tres raíces. Sea x_0 una de esas raíces, enseguida introducimos la variable auxiliar u y consideremos el polinomio

$$f(u) = u^2 - x_0 u - \frac{p}{3}$$

con coeficientes complejos, y sean sus raíces α y β, por las fórmulas de Vieta tenemos:

$$\alpha + \beta = x_0 \tag{3.6}$$

$$\alpha\beta = -\frac{p}{3}. \tag{3.7}$$

Sustituyendo x_0 en (3.5), se obtiene:

$$(\alpha + \beta)^3 + p(\alpha + \beta) + q = 0,$$

de donde

$$\alpha^3 + \beta^3 + (3\alpha\beta + p)(\alpha + \beta) + q = 0.$$

De (3.7) se sigue que $3\alpha\beta + p = 0$, con lo cual se obtiene

$$\alpha^3 + \beta^3 = -q, \tag{3.8}$$

por otro lado de (3.7) también obtenemos:

$$\alpha^3\beta^3 = -\frac{p^3}{27}. \tag{3.9}$$

De (3.8) y (3.9) se observa que α^3 y β^3 son las raíces de la ecuación:

$$z^2 + qz - \frac{p^3}{27} = 0 \tag{3.10}$$

al resolverlo tendremos:

$$z = -\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$$

entonces

$$\alpha = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}, \qquad \beta = \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} \tag{3.11}$$

así, llegamos a la fórmula de Cardano, que expresa las raíces de la (3.5), luego

$$x_0 = \alpha + \beta = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}.$$

Puesto que la raíz cúbica tiene 3 valores en el campo de los complejos, la fórmula (3.11) da 3 valores para α y 3 para β. Sin embargo usando las fórmulas de Cardano, no se puede combinar un valor de α con un valor de β.

Para un valor de α tenemos que tomar solamente un valor de los tres de β el cual satisface la condición (3.7).

Si α_1 es uno de esos tres valores de la raíz de α, los otros valores pueden ser obtenidos multiplicando α_1 por las raíces cúbicas ϵ y ϵ^2 de la unidad:

$$\alpha_2 = \alpha_1\epsilon, \qquad \alpha_3 = \alpha_1\epsilon^2.$$

Denotando por β_1 uno de los tres valores de la raíz de β correspondientes al valor de α_1 de la raíz de α en la ecuación (3.7), esto es, $\alpha_1\beta_1 = -\frac{p}{3}$, los otros valores para

β son

$$\beta_2 = \beta_1\epsilon, \qquad \beta_3 = \beta_1\epsilon^2.$$

Desde que $\epsilon^3 = 1$, se tiene

$$\alpha_2\beta_3 = \alpha_1\epsilon\beta_1\epsilon^2 = \alpha_1\beta_1\epsilon^3 = \alpha_1\beta_1 = -\frac{p}{3}.$$

Ello muestra que el valor α_2 de la raíz α es asociado con el valor β_3 de la raíz de β; similarmente, el valor de α_3 le corresponde el valor de β_2.

Así las tres raíces de la ecuación (3.5 pueden ser escritos como sigue:

$$\begin{cases} x_1 &= \alpha_1 + \beta_1 \\ x_2 &= \alpha_2 + \beta_3 = \alpha_1\epsilon + \beta_1\epsilon^2 \\ x_3 &= \alpha_3 + \beta_2 = \alpha_1\epsilon^2 + \beta_1\epsilon \end{cases}$$

Ejemplo 3.1. *Resolver* $x^3 + 3\sqrt[3]{3}x - 2 = 0$

SOLUCIÓN

Esta ecuación corresponde a la forma reducida, identificando:

$p = 3\sqrt[3]{3}, \quad q = -2.$

se plantea el sistema $\begin{cases} u^3 + v^3 &= 2 \\ u^3v^3 &= -3 \end{cases}$

u^3 *y* v^3 *son raíces de la ecuación:*

$$r^2 - 2r - 3 = 0 \quad \Rightarrow r = \frac{2 \pm \sqrt{4+12}}{2} = 1 \pm 2$$

$$\Rightarrow u = \sqrt[3]{3} \quad , \quad v = -1$$

una raíz es :$x_1 = \sqrt[3]{3} - 1$ *las otras raíces son* $x_2 = \sqrt[3]{3}w - w^2$ *y* $x_3 = \sqrt[3]{3}w^2 - w$

2. Ecuación de cuarto grado

La solución de la ecuación cuártica

$$y^4 + ay^3 + by^2 + cy + d = 0 \tag{3.12}$$

con coeficientes complejos se reduce a la solución de alguna ecuación cúbica auxiliar. Esto es logrado por un procedimiento debido a Ferrari, primero la sustitución
$y = x - \frac{a}{4}$ reduce la ecuación (3.12) a la forma

$$x^4 + px^2 + qx + r = 0. \tag{3.13}$$

El miembro izquierdo de esta ecuación es idénticamente transformado con la ayuda de un parámetro auxiliar α:

$$x^4 + px^2 + \frac{p^2}{4} + qx + r - \frac{p^2}{4} = 0$$

obteniéndose

$$\left(x^2 + \frac{p}{2}\right)^2 + 2\alpha\left(x^2 + \frac{p}{2}\right) + \alpha^2 + qx + r - \frac{p^2}{4} - 2\alpha\left(x^2 + \frac{p}{2}\right) - \alpha^2 = 0.$$

Así

$$\left(x^2 + \frac{p}{2} + \alpha\right)^2 - \left[2\alpha x^2 - qx + \left(\alpha^2 + p\alpha - r + \frac{p^2}{4}\right)\right] = 0 \tag{3.14}$$

Ahora elegimos α y completar el cuadrado en el corchete, esto requiere que debe tener raíz doble, es decir, se debe tener la ecuación

$$q^2 - 8\alpha\left(\alpha^2 + p\alpha - r + \frac{p^2}{4}\right) = 0. \tag{3.15}$$

La ecuación (3.15) es una ecuación cúbica en la variable α con coeficientes complejos. Como sabemos, esta ecuación tiene tres raíces complejas.
Sea α_0 una de las raíces, ello es expresado por la fórmula de Cardano, con ayuda de radicales en términos de la ecuación (3.13).
Dado esto elegimos de valor para α, el polinomio en el corchete (3.14) tiene la raíz

doble $\frac{q}{4\alpha_0}$, y así esta ecuación toma la forma

$$\left(x^2+\frac{p}{2}+\alpha_0\right)^2-2\alpha_0\left(x-\frac{q}{4\alpha_0}\right)^2=0$$

que da origen a dos ecuaciones cuadráticas:

$$\left.\begin{array}{rcl} x^2-\sqrt{2\alpha_0}x+\left(\frac{p}{2}+\alpha_0+\frac{q}{2\sqrt{2\alpha_0}}\right) & = & 0 \\ x^2+\sqrt{2\alpha_0}x+\left(\frac{p}{2}+\alpha_0-\frac{q}{2\sqrt{2\alpha_0}}\right) & = & 0 \end{array}\right\} \tag{3.16}$$

las raíces de (3.16) servirán como raíces de (3.14).

Comentario 3.1. *Los griegos conocieron el método para resolver una ecuación cuadrática, pero los métodos para resolver las ecuaciones cúbicas y cuárticas fueron descubiertos sólo en el siglo* 16*. Luego de* 3 *centurias de intentos sin éxitos para hallar fórmulas que expresan por radicales las raíces de una ecuación de quinto grado (con coeficientes literales) en términos de sus coeficientes. Esos intentos cesaron únicamente desde que Abel demostró en* 1820*, que no era posible encontrar una fórmula para una ecuación de grado* $n \geq 5$*.*
Este resultado de Abel, sin embargo no evitó la posibilidad que las raíces de un polinomio con coeficientes numéricos, deberían ser expresados de alguna forma en términos de los coeficientes por alguna combinación de radicales, o bien como usualmente se dice una ecuación resoluble por radicales. En 1930*, Galois hizo una completa investigación de las condiciones bajo el cual dada una ecuación es soluble por radicales. Mostró que para* $n \geq 5$ *ecuación de grado* n *con coeficientes enteros no era soluble por radicales. Las investigaciones de Galois ejerció una decisiva influencia en posteriores desarrollos del álgebra.*

Hasta el momento se han obtenido 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 $+, -, \cdot, /, \sqrt{}, \sqrt[3]{}$, 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 algebraicas? La respuesta es negativa.

Teorema 3.2 (Abel, 1802-1829)**.** *No hay una fórmula que describa las raíces de un polinomio general f de grado ≥ 5 a partir de sus coeficientes y de las operaciones elementales descritos anteriormente.*

Galois (1811-1832)

Sea un polinomio general de grado n sobre $\mathbb{K}[x]$, $p(x) = x^n + a_1x^{n-1} + \cdots + a_n$, se conoce:

sea $\mathbb{K}(a_1, \cdots, a_n)$ el campo de funciones racionales en las n variables $a_1, \cdots, a_n$ sobre $\mathbb{K}$, y consíderese el polinomio particular $p(x) = x^n + a_1x^{n-1} + \cdots + a_n$ sobre el campo $\mathbb{K}(a_1, \cdots, a_n)$.

Decimos que es soluble por radicales si es soluble por radicales sobre $\mathbb{K}(a_1, \cdots, a_n)$, esto expresa realmente la idea intuitiva de "mostrar una fórmula" para las raíces de $p(x)$ que implique combinaciones de raíces n-ésimas, para $n \geq 5$ Abel probó, en general, que esto no puede hacerse, (esto no excluye la posibilidad de que un polinomio dado pueda resolverse por radicales).

3.2. UBICACIÓN DE LAS RAÍCES

No obstante de no poder obtener en general las raíces de un polinomio $f \in \mathbb{C}[x]$ por medio de una fórmula, se puede exhibir una cota M para el módulo de las raíces, dependiendo de los coeficientes de f.

Proposición 3.1 (Cota de Cauchy)**.** *Sea $f(x) = a_nx^n + \ldots + a_0 \in \mathbb{C}[x]$, con $n \geq 1, a_n \neq 0$.*

Sea $M = 1 + \left|\frac{a_{n-1}}{a_n}\right| + \ldots + \left|\frac{a_0}{a_n}\right|$, luego toda raíz $\alpha \in \mathbb{C}[x]$ de f verifica que $|\alpha| < M$.

Prueba

1. Si $|\alpha| < 1$, no hay nada que probar pues $1 \leq M$ por definición.

2. Para $|\alpha| \geq 1$, se observa que $f(\alpha) = 0$

$$
\begin{aligned}
&\Leftrightarrow a_n\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_1\alpha + a_0 &&= 0\\
&\Leftrightarrow a_n\left(\alpha^n + \tfrac{a_{n-1}}{a_n}\alpha^{n-1} + \ldots + \tfrac{a_1}{a_n}\alpha + \tfrac{a_0}{a_n}\right) &&= 0\\
&\Leftrightarrow \alpha^n + \tfrac{a_{n-1}}{a_n}\alpha^{n-1} + \ldots + \tfrac{a_0}{a_n} &&= 0\\
&\Leftrightarrow \alpha^n = -\left(\tfrac{a_{n-1}}{a_n}\alpha^{n-1} + \ldots + \tfrac{a_0}{a_n}\right) &&\Leftrightarrow |\alpha|^n = \left|\tfrac{a_{n-1}}{a_n}\alpha^{n-1} + \ldots \tfrac{a_0}{a_n}\right| \leq\\
&\left|\tfrac{a_{n-1}}{a_n}\right||\alpha|^{n-1} + \ldots + \left|\tfrac{a_1}{a_n}\right||\alpha| + \left|\tfrac{a_0}{a_n}\right| &&\leq |\alpha|^{n-1}\left(\left|\tfrac{a_{n-1}}{a_n}\right| + \ldots + \left|\tfrac{a_0}{a_n}\right|\right)
\end{aligned}
$$

Pues para $|\alpha| \geq 1$, se tiene que $|\alpha|^{n-1} \geq |\alpha|^k, \quad \forall \quad 1 \leq k \leq n-1$.

De esta manera se concluye que:

$$|\alpha| \leq \left|\frac{a_{n-1}}{a_n}\right| + \ldots + \left|\frac{a_0}{a_n}\right| < M \qquad \therefore |\alpha| < M$$

■

Ejemplo 3.2. *Sea el polinomio en* $\mathbb{C}$*,*

$$f(x) = (2+i)x^5 + (2-i)x^4 - x^3 + 5ix - 4$$

En este caso $M = 1 + \left|\frac{2-i}{2+i}\right| + \left|\frac{-1}{2+i}\right| + \left|\frac{5i}{2+i}\right| + \left|\frac{-4}{2+i}\right| = 2 + 2\sqrt{5}$.
Luego tadas las raíces α *de* f *verifican* $|\alpha| < 2 + 2\sqrt{5}$. □

4 POLINOMIOS EN $\mathbb{Q}[X]$

4.1. REVISIÓN DE RESULTADOS

1. Un polinomio en $\mathbb{Q}[x]$ de grado $n \geq 1$ tiene a lo sumo n raíces en $\mathbb{Q}$ contados con su multiplicidad.

2. Sea $f \in \mathbb{Q}[x]$ de grado ≥ 2, si f tiene una raíz entonces f es reducible.

3. $f \in \mathbb{Q}[x]$ reducible no implica que f tiene raíces en $\mathbb{Q}$ por ejemplo x^2-3 es reducible y sin raíces racionales.

4. $f \in \mathbb{Q}[x]$ de grado 2 o 3 es reducible si y solo si tiene una raíz en $\mathbb{Q}$ (por cuestion de grado, si es reducible tiene que tener al menos un factor de grado 1).

4.2. CÁLCULO DE RAÍCES EN $\mathbb{Q}$

Si el polinomio $f \in \mathbb{Q}[x]$ tiene raíces en $\mathbb{Q}$, entonces se puede encontrar todas las raíces racionales por medio de un algoritmo.

Sea $f(x) = a_n x^n + \ldots + a_1 x + a_0, \quad a_n \neq 0$. Entonces existe $c \in \mathbb{Z}\backslash\{0\}$ tal que $g(x) = cf(x)$ donde g tiene todos sus coeficientes enteros (se puede elegir c como el mínimo común multiplo de los denominadores de los coeficientes de f), más aún las raíces de f claramente coinciden con los de g.

Ejemplo 4.1. $f(x) = \frac{3}{4}x^5 - \frac{1}{3}x^4 - \frac{1}{6}x^2 + \frac{2}{3} \in \mathbb{Q}[x]$
$y \quad g(x) = 12f(x) = 9x^5 - 4x^4 - 2x^2 + 8 \in \mathbb{Z}[x]$ *tienen exactamente las mismas raíces, que* f.

Como resultado para hallar las raíces racionales de un polinomio en $\mathbb{Q}[x]$, nos basta con estudiar como encontrar las raíces racionales de un polinomio en $\mathbb{Z}[x]$.

Lema 4.1 (Gauss)**.** *Sea* $f(x) = a_n x^n + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$ *con* $a_n, a_0 \neq 0$*. Entonces, si* $\alpha/\beta \in \mathbb{Q}$ *es una raíz racional de* f*, con* $\alpha, \beta \in \mathbb{Z}$ *primos entre si, entonces* α/a_0 *y* β/a_n*.*

Prueba

Por hipótesis:
$f\left(\frac{\alpha}{\beta}\right) = 0 \Leftrightarrow a_n \left(\frac{\alpha}{\beta}\right)^n + a_{n-1}\left(\frac{\alpha}{\beta}\right)^{n-1} + \ldots + a_1\left(\frac{\alpha}{\beta}\right) + a_0 = 0.$

$\Leftrightarrow a_n\alpha^n + a_{n-1}\alpha^{n-1}\beta + \ldots + a_1\alpha\beta^{n-1} + a_0\beta^n = 0.$

De donde:

$$\alpha(a_n\alpha^{n-1} + a_{n-1}\alpha^{n-2}\beta + \ldots + a_1\beta^{n-1}) = -a_0\beta^n.$$

Por lo tanto $\alpha/-a_0\beta^n$, pero como α y β son primos entre si, α y β^n no tienen ningún factor en común, o sea lo único que queda es que α/a_0.
Del mismo modo:

$$\beta(a_{n-1}\alpha^{n-1} + \ldots + a_1\alpha\beta^{n-2} + a_0\beta^{n-1}) = -a_n\alpha^n$$

implica que $\beta/-a_n\alpha^n$, pero al ser primos con α, resulta β/a_n.

Aplicación (Algoritmo que permite encontrar las raíces racionales de un polinomio en $\mathbb{Z}[X]$).

En las condiciones del Lema de Gauss implica que si se construye el conjunto N de los divisores positivos y negativos de a_0 y el conjunto D de los de a_n las raíces del polinomio f se encuentra en el conjunto de las fracciones α/β, eligiendo

α en N y β en D. Verificando para cada fracción α/β asi construida si $f\left(\frac{\alpha}{\beta}\right) = 0$, se obtienen las raíces racionales.

Con este criterio no se aclara la multiplicidad de cada raíz. Para evaluar cada fracción en el polinomio f se debe usar la división sintética de Ruffini, si el resto es cero entonces se toma como raíz, si es diferente de cero se descarta.

Ejemplo 4.2. *Hallemos las raíces racionales del polinomio:*

$$f(x) = x^7 - \frac{7}{2}x^6 + 7x^5 - 12x^4 + 12x^3 - \frac{9}{2}x^2$$

SOLUCIÓN

Quitando denominadores podemos definir:

$$g(x) = 2f(x) = 2x^7 - 7x^6 + 14x^5 - 24x^4 + 24x^3 - 9x^2$$

$$g(x) = x^2(2x^5 - 7x^4 + 14x^3 - 24x^2 + 24x - 9)$$

Vemos que 0 *es raíz de multiplicidad* 2 *de* g*(y de* f*) y las restantes raíces son del polinomio* h*:*

$$h(x) = 2x^5 - 7x^4 + 14x^3 - 24x^2 + 24x - 9$$

Aquí, $a_0 = -9$, $a_n = 2$*; luego las raíces racionales se busca en el conjunto.*

$$\pm\left\{\frac{\textit{divisores de } 9}{\textit{divisores de } 2}\right\} = \pm\left\{\frac{1,3,9}{1,2}\right\} = \pm 1, \pm\frac{1}{2}\,; \pm 3\,; \pm 9\,; \pm\frac{9}{2}$$

veamos que $h(1) = 0$

$x = 1$:

	2	*-7*	*14*	*-24*	*24*	*-9*
1		*2*	*-5*	*9*	*-15*	*9*
	2	*-5*	*9*	*-15*	*9*	*0*

$x = 1$:

	2	-5	9	-15	9
1		2	-3	6	-9
	2	-3	6	-9	0
$\frac{3}{2}$		3	0	9	
	2	0	6	0	

$$\Rightarrow h(x) = (x-1)^2\left(x - \frac{3}{2}\right)(2x^2+6) = (x-1)^2(2x-3)(x^2+3)$$

$$\therefore f(x) = x^2(x-1)^2\left(x - \frac{3}{2}\right)(x^2+3)$$

□

Observación 4.1. *El Lema de Gauss nos provee un algoritmo para calcular las raíces racionales de un polinomio en $\mathbb{Q}[x]$, pero podemos notar que es bastante laborioso (la cantidad de fracciones está relacionada con la cantidad de divisores de a_0 y a_n)*

4.3. IRREDUCIBILIDAD EN $\mathbb{Q}[x]$

En este párrafo debemos dar un criterio que permite probar la irreducibilidad de determinados polinomios en $\mathbb{Q}[x]$, y mostrar que existen polinomios irreducibles de cualquier grado. Debemos relacionar factorizaciones en $\mathbb{Q}[X]$ con factorizaciones en $\mathbb{Z}[x]$.

Dado $f \in \mathbb{Q}[x]$ es reducible si y solo si cf es reducible para todo $c \in \mathbb{Q}\backslash\{0\}$, se pueden suprimir denominadores y restringirse a analizar la reducibilidad en $\mathbb{Q}[x]$ de polinomios con coeficientes enteros.

Definición 4.1. *Sea* $f(x) = a_n x^n + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$ *un polinomio con coeficientes enteros. Se define el contenido de* f *como el máximo común divisor de los coeficientes de* f *o sea el contenido de* f *es el número entero:*

$$con\,t(f) = mcd(a_0, \ldots, a_n)$$

En el caso que $con\,t(f) = 1$, se dice que el polinomio f es primitivo.
Debemos ver que por la definición de contenido, resulta inmediato que si $f \in \mathbb{Z}[x]$ y $c \in \mathbb{Z}\backslash\{0\}$, entonces $con\,t(cf) = c\ cont\,(f)$ y además $f = con\,t(f)\overline{f}$ donde $\overline{f} \in \mathbb{Z}[x]$ es un polinomio primitivo.

Lema 4.2. *(Gauss) Sean* $f, g \in \mathbb{Z}[x]$*, entonces*

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

Prueba

1. Sea $f(x) = a_0 + a_1 x + \ldots + a_n x^n$ y $g(x) = b_0 + b_1 x + \ldots + b_m x^m$, supongamos que el lema fuera falso; entonces todos los coeficientes de $f(x)\ g(x)$ serían divisibles por algun entero mayor que 1, de donde, por algún primo p como $f(x)$ es primitivo, p no divide a alguno de los coeficientes a_i. Sea a_j el primer coeficiente de $f(x)$ al que p no divide. Análogamente, sea b_k el primer coeficiente de $g(x)$ al que p no divide. En $f(x)\ g(x)$ el coeficiente de x^{j+k}, c_{j+k}, es:
$$\begin{aligned} c_{j+k} = \quad & a_j b_k + (a_{j+1} b_{k-1} + a_{j+2} b_{k-2} + \ldots + a_{j+k} b_0) + \\ & (a_{j-1} b_{k+1} + a_{j-2} b_{k+2} + \ldots + a_0 b_{j+k}) \end{aligned} \qquad (\alpha)$$
Por nuestra elección de b_k , $p/b_{k-1}, b_{k-2}, \ldots$, de modo que $p/(a_{j+1} b_{k-1} + a_{j+2} b_{k-2} + \ldots + a_{j+k} b_0)$. Análogamente, por nuestra elección de a_j, $p/a_{j-1}, a_{j-2}, \ldots$, de modo que

$p/(a_{j-1}b_{k+1} + a_{j-2}b_{k+2} + \ldots + a_0 b_{k+j})$.

Por hipotesis, p/c_{j+k} luego (α) , $p/a_j b_k$, lo que es imposible pués $p \nmid a_j$ y $p \nmid b_k$, con lo cual concluye la prueba.

2. Como $f = cont(f) \cdot \overline{f}$ y $g = cont(g)\overline{g}$, donde $\overline{f}, \overline{g} \in \mathbb{Z}[x]$ son primitivos.

   Tenemos que

$$\begin{aligned} fg &= cont(f)cont(g)\overline{f} \cdot \overline{g} \\ \Rightarrow cont(fg) &= cont(cont(f)cont(g)\overline{f}\,\overline{g}) \\ &= cont(f)cont(g)cont(\overline{f}\,\overline{g}) \end{aligned}$$

   Pero por (1):

$$\begin{aligned} cont(\overline{f}\,\overline{g}) &= 1 \\ \Rightarrow cont(fg) &= cont(f)cont(g) \end{aligned}$$

■

El Lema siguiente nos muestra que si un polinomio entero se escribe como el producto de dos polinomios racionales, entonces se puede también escribir como el producto de dos polinomios enteros.

Teorema 4.1 (LEMA DE de GAUSS)**.** *Si el polinomio primitivo $f(x)$ puede factorizar como el producto de dos polinomios de coeficientes racionales, entonces puede factorizarse como el producto de dos polinomios de coeficientes enteros.*

Prueba

Supongamos que $f(x) = g(x)h(x)$ donde $g(x)$ y $h(x)$ tienen coeficientes racionales. Quitando denominadores y sacando los factores comunes podemos escribir entonces $f(x) = \left(\frac{a}{b}\right) u(x)v(x)$ donde a y b son enteros y donde tanto $u(x)$ como $v(x)$ tienen coeficientes enteros y son primitivos. Luego $bf(x) = au(x)v(x)$. El contenido del primer miembro es b, ya que $f(x)$ es primitivo; como $u(x)$ y $v(x)$ son primitivos, según el lema anterior $u(x)v(x)$ es primitivo, luego el contenido del segundo miembro es a. Por lo tanto $a = b$ y $f(x) = u(x)v(x)$ donde $u(x)$ y $v(x)$ tienen coeficientes enteros. Con lo que queda demostrado el teorema.

Teorema 4.2 (Criterio de irreducibilidad de Eisenstein)**.** *Sea* $f(x) \in \mathbb{Z}[x]$, $f(x) = a_n x^n + \ldots + a_1 x + a_0, \quad a_n \neq 0$ *tal que existe un primo* p *que verifica* $p \nmid a_n$, p/a_{n-1}, $p/a_{n-2}, \ldots, p/a_0$ *y* $p^2 \nmid a_0$ *, entonces* $f(x)$ *es irreducible sobre* $\mathbb{Q}[x]$.
Prueba

Sin pérdida de generalidad podemos suponer que $f(x)$ es primitivo, pues el sacar el máximo común divisor de sus coeficientes no modifica la hipotesis, ya que $p \nmid a_n$. Por el lema de Gauss supongamos que $f(x)$ es reducible, entonces:

$$f(x) = (b_r x^r + \ldots + b_1 x + b_0)(c_s x^s + \ldots + c_1 x + c_0)$$

donde los b y c son enteros y donde $r > 0$ y $s > 0$. Comparando los coeficientes de ambos miembros tenemos $a_0 = b_0 c_0$. Como p/a_0, p debe dividir a uno de los dos b_0 ó c_0 . Como $p^2 \nmid a_0$, p no puede dividir a la vez a ambos b_0 y c_0. Supongamos que p/b_0 y $p \nmid c_0$. No todos los coeficientes $b_r, \ldots, b_0$ pueden ser divisibles por p; de otro modo todos los coeficientes de $f(x)$ serían divisible por p, lo que es falso, ya que $p \nmid a_n$. Sea b_k el primer b no divisible por p, $k \leq r < n$. Tenemos entonces que p/b_{k-1} y a los b anteriores. Pero $a_k = b_k c_0 + b_{k-1} c_1 + b_{k-2} c_2 + \ldots + b_0 c_k$ y $p/b_{k-1}, b_{k-2}, \ldots, b_0$, de modo que $p/b_k c_0$. Pero $p \nmid c_0$ y $p \nmid b_k$, lo que entra en conflicto con que $p/b_k c_0$. Esto prueba que nosotros no pudimos haberlo factorizado. Luego $f(x)$ es irreducible.

Ejemplo 4.3. $f(x) = x^4 + x^3 + x^2 + x + 1$ *es irreducible en* $\mathbb{Q}[x]$.

Corolario 4.1. *Existen polinomios irreducibles de cualquier grado en* $\mathbb{Q}[x]$.

Ejemplo 4.4. $2x^n - 4$ *es irreducible en* $\mathbb{Q}[x]$ *para* $n \in \mathbb{N}$

4.4. FACTORIZACIÓN EN $\mathbb{Q}[x]$

Como se vió anteriormente para factorizar un polinomio en $\mathbb{Q}[x]$, dado que las constantes no influyen, alcanza con considerar el polinomio en $\mathbb{Z}[x]$ obtenido

al extraer el *mcd* de los denominadores.
Para factorizar en $\mathbb{Q}[x]$ un polinomio con coeficientes enteros, se puede reducir progresivamente hasta obtener todos los factores irreducibles en $\mathbb{Z}[x]$.

Daremos un algoritmo clásico, debido a Kronecker (1823-1891), y muy sencillo teóricamente 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 inferiores a f de manera que $f = gh$, y se puede suponer sin pérdida de generalidad que $gr(g) \leq \frac{1}{2} gr(f)$.

Ahora si $g \in \mathbb{Z}[x]$ tiene grado $\leq gr(f)/2$; por el teorema de interpolación, queda exactamente determinado por su valor en $\left[|\frac{gr(f)}{2}|\right] + 1$ puntos. También para todo $k \in \mathbb{Z}$ se verifica $f(k) = g(k)h(k)$ o sea $g(k)/f(k)$.

Algoritmo de Factorización de Kronecker

1. Se evalua el polinomio f en $m = \left[|\frac{gr(f)}{2}|\right] + 1$ puntos enteros $k_1, \ldots, k_m$, obteniendo $r_1 = f(k_1), \ldots, r_m = f(k_m)$.

2. Se halla todos los divisores positivos y negativos de cada uno de los valores $r_1, \ldots, r_m$ obtenidos.

3. Para cada elección de m divisores $d_1, \ldots, d_m$ se verifica si el polinomio g que interpola $(k_1, d_1), \ldots, (k_m, d_m)$ es en realidad un factor de f.

4. Si no lo es, se pasa a otra elección de divisores, mientras que si lo es, se repite el procedimiento con g y $\dfrac{f}{g}$.

5. Si para ninguna elección de divisores se obtiene que g/f eso significa que el polinomio f es irreducible.

Ejemplo 4.5. *Sea* $f(x) = x^5 - x^3 + x^2 - 2x - 2$.
Si f *es reducible tiene un factor* $g \in \mathbb{Z}[x]$ *de grado* $\leq \dfrac{gr(f)}{2} = 2,5 \Rightarrow gr(g) \leq 2$, *que será determinado por su valor en tres puntos.*

Observamos que por el Lema de Gauss, las posibles raíces racionales de f son ± 2 pero $f(\pm 2) \neq 0$, luego f no tiene raíces racionales, con lo cual $gr(g) = 2$.

Elijamos los puntos de interpolación $k_1 = 0$, $k_2 = 1$, $k_3 = -1$: 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 $g(-1) \in \{\pm 1\}$.

De aquí podemos ver que se pueden calcular 32 posibles polinomios g y verificar si son en sí divisores de f.

1. Podemos elegir para g los puntos de interpolación $(0,1), (1,1)$ y $(-1,1)$, obtenemos
$$\begin{aligned} g(x) &= 1 \cdot \frac{(x-1)(x+1)}{(0-1)(0+1)} + 1 \cdot \frac{(x-0)(x+1)}{(1-0)(1+1)} + 1 \cdot \frac{(x-0)(x-1)}{(-1-0)(-1-1)} \\ &= -x^2 + 1 + \frac{1}{2}x^2 + \frac{1}{2}x + \frac{1}{2}x^2 - \frac{1}{2}x \\ &= 1 \\ \Rightarrow g(x) &= 1 \end{aligned}$$
que no aporta ningún factor para f.

2. Elejimos los puntos $(0,1), (1,1)$ y $(-1,-1)$, obtenemos el polinomio de interpolación.
$$\begin{aligned} g(x) &= 1 \cdot \frac{(x-1)(x+1)}{(-1)(1)} + 1 \cdot \frac{x(x+1)}{1(1+1)} - 1 \cdot \frac{x(x-1)}{(-1)(-1-1)} \\ &= -x^2 + 1 + \frac{1}{2}x^2 + \frac{1}{2}x - \frac{1}{2}x^2 - \frac{1}{2}x \\ &= -x^2 + x + 1 \end{aligned}$$
y vemos que este polinomio no divide a f (deja por resto $-2x - 1$).

3. Finalmente se puede ir planteando todas las posibles ternas, y podemos elegir los puntos de interpolación $(0,-2),(1,-1)$ y $(-1,-1)$, obteniéndose:

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

Se verifica que $x^2 - 2/f$, con cociente $x^3 + x + 1$.

Ahora $x^2 - 2$ y $x^3 + x + 1$ son ambos irreducibles pues f no tiene raíces en $\mathbb{Q}$. Luego f se factoriza en $\mathbb{Q}[x]$ como

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

Se observa que este algoritmo puede resultar extremadamente lento, pues por más que los valores de $f(k_i)$ sean los más simples posibles, tienen cada uno por lo menos 2 divisores, y al menos se debe de calcular y chequar $2^{[|gr(f)/2|]+1}$ polinomios g.

Posteriormente se mejoró la velocidad de los algoritmos de factorización en $\mathbb{Q}[x]$.

El primero de ellos, debido a H.Zassenhaus (1969), se basa esencialmente en un algoritmo de E.Berlekamp para factorizar rápidamente polinomios en cuerpos finitos. El algoritmo requiere en promedio un número de operaciones del orden de $[gr(f)]^c$, c es una constante calculada, aunque en el peor de los casos puede necesitar un número exponencial en $gr(f)$ operaciones.

5 POLINOMIOS EN $\mathbb{R}[X]$

REVISIÓN DE CONCEPTOS

1. Un polinomio en $\mathbb{R}[x]$ de grado $n \geq 1$ tiene a lo más n raíces contandos con sus multiplicidades.

2. Sea $f \in \mathbb{R}[x]$ de grado ≥ 2. Si f tiene una raíz, entonces f es reducible.

3. $f \in \mathbb{R}[x]$ reducible no implica que f tenga raíces en $\mathbb{R}$. Así el polinomio $(x^2 + 2x + 2)^2$ es reducible y sin raíces reales.

4. $f \in \mathbb{R}[x]$ de grado 2 ó 3 es reducible si y solo sí tiene una raíz en $\mathbb{R}$.

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

5.1. POLINOMIOS IRREDUCIBLES EN $\mathbb{R}[x]$

Proposición 5.1. *Todo polinomio en $\mathbb{R}[x]$ de grado impar tiene al menos una raíz real.*

Prueba

Sea $f(x) = a_n x^n + \ldots + a_1 x + a_0$ con n impar.

Si $a_n > 0$, entonces

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

Si $a_n < 0$ se tiene

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

En ambos casos los signos son opuestos,y 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 $f(\alpha) = 0$. ■

Se puede ser más explicito y precisar mejor cuántas raíces reales puede tener f.

Teorema 5.1. *Sea $f \in \mathbb{R}[x]$ y sea $z \in \mathbb{C}\backslash\mathbb{R}$ un número imaginario.*
Entonces

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

Prueba

1. Sea $f(x) = a_n x^n + \ldots + a_1 x + a_0$.

   entonces

   $f(z) = 0 \Leftrightarrow a_n z^n + \ldots + a_1 z + a_0 = 0.$

   $\Leftrightarrow \overline{a_n z^n + \ldots + a_1 z + a_0} = \overline{0}.$

   $\Leftrightarrow \overline{a}_n \overline{z}^n + \ldots + \overline{a}_1 \overline{z} + \overline{a}_0 = 0.$

   $\Leftrightarrow a_n \overline{z}^n + \ldots + a_1 \overline{z} + a_0 = 0.$

   $(\overline{a_i} = a_i\,,\ \forall \quad i = 0, 1, \ldots, n,$ pues $\ a_i \in \mathbb{R}) \Leftrightarrow f(\overline{z}) = 0$

2. Si z es raíz de multiplicidad k de $f \Leftrightarrow f(z) = f'(z) = f''(z) = \ldots = f^{(k-1)}_{(z)} = 0$ y $f^{(k)}(z) \neq 0$ pero $f', \ldots, f^{(k-1)}, f^{(k)}$ también son polinomios en $\mathbb{R}[x]$ y por (1): $f(\overline{z}) = \ldots = f^{(k-1)}(\overline{z}) = 0$ y $f^{(k)}(\overline{z}) \neq 0 \Leftrightarrow \overline{z}$ es raíz de multiplicidad k de f.

■

Este teorema nos dice que las raíces complejas no reales de un polinomio real f viene en parejas de complejos conjugados, o sea un polinomio f en $\mathbb{R}[x]$ de grado n, que tiene exactamente n raíces complejas contados con sus multiplicidades, tiene un número par de ellas que son complejas no reales y el resto son reales. Así un polinomio real de grado impar tiene un número impar de raíces reales.

Observación 5.1. *Sean z y $\overline{z}$ números complejos conjugados no reales, entonces el polinomio $(x-z)(x-\overline{z})$ es un polinomio en $\mathbb{R}[x]$, pues*
$(x-z)(x-\overline{z}) = x^2 - (z+\overline{z})x + z\overline{z} = x^2 - 2\mathbb{R}e(z)x + |z|^2 \in \mathbb{R}[x]$.

Proposición 5.2. *(Polinomio irreducible en $\mathbb{R}[x]$) Los polinomios irreducibles en $\mathbb{R}[x]$ son exactamente los de grado 1 y aquellos de grado 2 con discriminante negativo.*

Prueba

Es claro que los polinomios de grado 1 y los de grado 2 con discriminante negativo son irreducibles.

Recíprocamente, si f tiene grado impar > 1 entonces tiene al menos una raíz real luego es reducible.

Si f es de grado 2, es reducible si y solo sí tiene discriminante mayor o igual a cero.

Si f tiene grado par ≥ 4, o bien tiene alguna raíz real en tal caso es reducible, o bien todos sus raíces son complejos no reales y vienen en pares conjugados, si z es una de esa raíces, el polinomio real $(x-z)(x-\overline{z})$ divide a $f \in \mathbb{R}[x]$ y f resulta reducible. ■

Corolario 5.1. *(Factorización en $\mathbb{R}[x]$) La factorización en irreducibles de un polinomio $f \in \mathbb{R}[x]$ puede adoptar la forma general:*

$$f(x) = c(x-\alpha_1)^{k_1} \dots (x-\alpha_r)^{k_r}(x^2+u_1x+v_1)^{j_1} \dots (x^2+u_sx+v_s)^{j_s}$$

con r o s eventualmente nulos

$k_i, j_l \geq 1\ (1 \leq i \leq r, 1 \leq l \leq s)$ *y* $u_l^2 - 4v_l < 0$.

5.2. CANTIDAD DE RAÍCES REALES DE UN POLINOMIO EN $\mathbb{R}[x]$

Se sabe que $f \in \mathbb{R}[x]$ de grado $n \geq 1$ tiene exactamente n raíces complejas (contados con sus multiplicidades). También si $gr(f) \geq 5$, no existe una fórmula general para expresar las raíces. ¿Cuántos de estas raíces serán reales?.

No existe para raíces reales un criterio como el Lema de Gauss para raíces racionales, pero si existe un algoritmo que permite contar con exactitud la cantidad de raíces reales del polinomio f en un intervalo (Teorema de Sturm, 1836). Previamente veamos un criterio más sencillo, debido a Descartes (1596-1650), que permite acotar la cantidad de raíces reales de f.
Introduzcamos las siguientes notaciones:
Notación: Sea $f(x) = a_n x^n + \ldots + a_1 x + a_0 \in \mathbb{R}[x]$

1. $Z_+(f)$ = cantidad de raíces reales estrictamente positivas de f (contados con su multiplicidad).

2. $Z_-(f)$ =cantidad de raíces reales estrictamente negativos de f (contados con su multiplicidad).

3. $V(f) = V(a_n, \ldots, a_0)$ = número de cambios de signo en la sucesión ordenada $a_n, \ldots, a_0$ saltando los ceros.

Ejemplo 5.1. *Sí* $f(x) = 3x^5 + 2x^4 - x^3 + x - 6$, *Entonces*

$$V(f) = V(3, 2, -1, 0, 1, -6) = 3$$

pues primero pasa de 2 *a* -1*, luego pasa de* -1 *a* 1 *y finalmente de* 1 *a* -6*, en total* 3 *cambios de signo.*

- *Sí* $g(x) = 2x^5 + x^3 + x + 2 \Rightarrow V(g) = 0$,
- *Sí* $h(x) = x^3 - x^2 + 2x - 5 \Rightarrow V(h) = 3$

Proposición 5.3. *(Regla de los signos de Descartes)*
Sea $f(x) = a_n x^n + \ldots + a_0 \in \mathbb{R}[x]$*, entonces:*

1. $Z_+(f) \leq V(f)$
2. $V(f) - Z_+(f)$ es siempre un número par.
3. $Z_-(f) \leq V(f(-x)) = V((-1)^n a_n\,,\,(-1)^{n-1}a_{n-1}, \ldots, a_0)$ 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 5.2. *Descartes enuncia esta regla, basándose posiblemente en hechos empíricos y demostraciones parciales para polinomios de grado* 1 *y* 2*, y polinomios con coeficientes positivos donde es claro esta proposición. Posteriormente el resultado fue probado con total generalidad por Gauss.*

El inciso 4, que no es tan conocido empezó a ser comentado y usado hacia 1980, resulta útil cuando uno de antemano sabe que un polinomio real tiene todas sus raíces reales, por ejemplo cuando se trata del polinomio característico de una matríz simétrica. En ese caso, la regla de los signos de Descartes permite calcular la signatura de la matríz sin factorizar el polinomio característico.

Prueba

Demostraremos aquí completamente el inciso 1, que se basa en el Teorema de Rolle. Sea $f : \mathbb{R} \to \mathbb{R}$ continua y derivable, y $\alpha < \beta$ tales que $f(\alpha) = f(\beta)$, entonces existe

$\gamma,\ \alpha < \gamma < \beta$ 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 consecutivos de f hay un número impar de raíes 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 $f(-x)$, así 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 $gr(f)$: siempre vale $V(f) + V(f(-x)) \leq n$).

Luego, si f tiene n raíces reales, que podemos suponer no nulos, la única posibilidad es que se cumplan las igualdades en los dos primeros incisos.

Demostremos ahora el inciso 1:

La demostración se hace por inducción en $gr(f) = n$

- Sí $n = 1$,
  $f(x) = ax + b$ y $Z_+(f) = 1 \Leftrightarrow ab < 0 \ \Leftrightarrow V(f) = 1$.

- Sí $n > 1$, sin pérdida de generalidad, podemos suponer que:
  $f(x) = a_n x^n + \ldots + a_j x^j + a_0$ con $a_n \neq 0\,,\ a_j \neq 0 (n \geq n-1 \geq \ldots \geq j)$ y $a_0 > 0$.

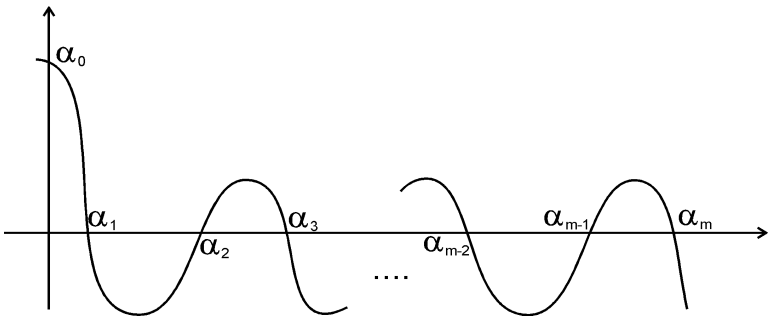
Quitando la raíz 0 tantas veces como aparece y eventualmente cambiando f por $-f$ (ya que estos cambios no modifican ni $Z_+(f)$ ni $V(f)$).

Luego $f'(x) = na_n x^{n-1} + \ldots + ja_j x^{j-1}$, se tiene 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:

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

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



Se tiene $Z_+(f) = k_1 + k_2 + \ldots + k_m$, 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, $Z_+(f') \geq (k_1 - 1) + \ldots + (k_m - 1) + m - 1 = k_1 + \ldots + k_m - 1 = Z_+(f) - 1$

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.

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

   Haciendo el mismo análisis, se obtiene $Z_+(f') \geq Z_+(f) - 1$, pero en este caso $V(f') = V(f)$.

   Usando la hipótesis inductiva, se prodría concluir que $Z_+(f) \leq V(f) + 1$ que no es lo que se busca.

   Si pudieramos 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:

$$\lim_{x\to 0^+} f(x) = \lim_{x\to 0^+} a_0 + a_j x^j \left(1 + \frac{a_{j+1}}{a_j}x + \ldots + \frac{a_n}{a_j}x^{n-j}\right) = a_0,$$

Pero, 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:

1. 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.

2. 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 $Z_+(f) = 1$.

3. 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.

4. Sea $f(x) = x^5 - 3x^4 + 1$. Como $V(f) = 2$, por lo tanto f tiene 0 o 2 raíces reales positivas. Pero podemos ver que $f(0) = 1$ y $f(1) = -1$ entonces f tiene una raíz real en el intervalo $< 0, 1 >$, luego f tiene 2 raíces reales positivas, y f tiene exáctamente 1 raíz real negativa (pues $f(-x) = -x^5 - 3x^4 + 1$), y 2 raíces complejas no reales conjugados.

Veamos ahora el Teorema de Sturm que permite determinar exactamente el número de raíces reales de un polinomio real f en el intervalo $\langle a, b\rangle$. Para lo cual necesitamos asociar al polinomio f un polinomio $\overline{f}$ con las mismas raíces complejas que f, pero todas de multiplicidad 1.

Proposición 5.4. *Sea* $f \in \mathbb{R}[x], gr(f) \geq 1$. *Entonces el polinomio* $\overline{f} = \frac{f}{mcd(f,f')} \in \mathbb{C}[x]$ *tiene las mismas raíces complejas de* f, *pero todas de multiplicidad* 1 *(*$\overline{f}$ *se llama el polinomio libre de cuadrados asociado a* f*).*

Prueba

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

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

Luego $mcd(f, f') = (x-\alpha_1)^{k_i-1}\dots(x-\alpha_m)^{k_m-1} \in \mathbb{C}[x]$ y

$\overline{f} = \dfrac{f}{mcd(f,f')} = c(x-\alpha_1)\dots(x-\alpha_m) \in \mathbb{C}[X]$ verifica lo enunciado. ■

Observación 5.3. *Se puede calcular* $mcd(f, f')$ *sin conocer la factorización de* f *en* $\mathbb{C}[x]$, *aplicando por ejemplo el algoritmo de Euclides, y por lo tanto para cada* $f \in \mathbb{R}[x]$ *determinar el polinomio* $\overline{f}$ *libre de cuadrados asociado a* f.

Definición 5.1 (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:*

1. $f_0 = f$,
2. $f_1 = f'$,
3. Para todo $i \geq 1$, se efectua el algoritmo de división
   $f_{i-1} = q_i f_i + r_i$ con $gr(r_i) < gr(f_i)$ y se define $f_{i+1} = -r_i$
4. Se termina cuando se llega a $f_s =$ constante (debemos observar 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 hipótesis que f no tenga raíces múltiples en $\mathbb{C}$ garantiza que se llega siempre f_s igual a una constante no nula).

Se denota también:

- $Z_{<a,b>}|f|$ = cantidad de raíces reales de f en el intervalo $\langle a, b\rangle$.
- $Z(f) = Z_{<-\infty,\infty>}(f)$ = cantidad total de raíces reales de f.
- $\forall\ c \in \mathbb{R}$, $V(c) = V(f_0(c), f_1(c), \ldots, f_s(c))$ = número de variaciones de signos en la sucesión ordenada $(f_0(c), f_1(c), \ldots, f_s(c))$.

Teorema 5.2 (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 $Z_{<a,b>}(f) = V(a) - V(b)$.*
Previo a la demostración, realicemos algunos ejemplos:

Ejemplo 5.2. *Sea $f(x) = x^3 - 4x^2 + 4x - 7$.*

$$V(f) = V(1, -4, 4, -7) = 3.$$

$$V(f) - Z_+(f) = par$$

Luego por la regla de los signos de Descartes f tiene 1 ó 3 raíces reales positivos.

$$f(-x) = -x^3 - 4x^2 - 4x - 7 \quad \Rightarrow V(f(-x)) = 0.$$

Entonces f no tiene ninguna raíz real negativa.
Se tiene $f'(x) = 3x^2 - 8x + 4 = (3x - 2)(x - 2)$
(Observemos que f' tiene exáctamente 2 raíces reales positivas, pero esto no nos permite decidir si f tiene 1 ó 3 raíces reales).
Hallemos la sucesión de Sturm de f, aún sin saber si f no tiene raíces múltiples.

$$
\begin{aligned}
f_0(x) &= x^3 - 4x^2 + 4x - 7 \\
f_1(x) &= f'(x) = 3x^2 - 8x + 4 \\
f_2(x) &= \tfrac{8}{9}x + \tfrac{47}{9} \text{ pues } f_0(x) = \left(\tfrac{1}{3}x - \tfrac{4}{9}\right) f_1(x) - \tfrac{8}{9}x - \tfrac{47}{9} \\
f_3(x) &= \tfrac{-9891}{64} \text{ pues } f_1(x) = (\tfrac{27}{8}x - \tfrac{1845}{64}) f_2(x) + \tfrac{9891}{64}
\end{aligned}
$$

Como llegamos a que f_3 es una constante no nula, se deduce de inmediato que f no tiene raíces múltiples en $\mathbb{C}$ (debemos tener en cuenta que la sucesión de Sturm es, salvo eventualmente un signo, la del algoritmo de Euclides para calcular el $mcd(f, f')$).

Aplicamos ahora el Teorema de Sturm

1. *Sea por ejemplo $a = 0$ y $b = 1$, entonces:*

   $V(a) = V(0) = V(f_0(0), f_1(0), f_2(0), f_3(0)) = V(-7, 4, \frac{47}{9}, \frac{-9891}{64}) = 2$
   $V(b) = V(1) = V(-6, -1, \frac{55}{9}, \frac{-9891}{64}) = 2.$

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

2. *Sea ahora $a = 3$ y $b = 4$. Luego se tiene:*

   $V(a) = V(3) = V(-4, 7, \frac{71}{9}, \frac{-9891}{64}) = 2 \quad y$

   $V(b) = V(4) = V(9, 20, \frac{79}{9}, \frac{-9891}{64}) = 1$

   Por lo tanto, $Z_{<3,4>}(f) = V(3) - V(4) = 1$, luego f tiene 1 raíz real en el intervalo $< 3, 4 >$

3. *También queremos averiguar la cantidad de raíces reales de f. Como sabemos $M = 1 + 4 + 4 + 7 = 16$ es una cota superior para los módulos de las raíces de f (Proposición 5), podríamos calcular $V(-16) - V(16)$, ó también $V(-N) - V(N)$, para todo $N \geq 16$.*

Si elegimos entonces N suficientemente grande, es decir superior a todas la raíces de los f_i para todo $i, 0 \leq i \leq 2$:

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

pues el coeficiente principal de f_i es positivo.

De la misma manera:

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

Así, observamos que:

$$\begin{array}{rcccccl} V(-N) & = & V(-\infty) & = & V(-\infty, +\infty, -\infty, -\frac{9891}{64}) & = & 2 \\ V(N) & = & V(+\infty) & = & V(+\infty, +\infty, +\infty, -\frac{9891}{64}) & = & 1 \end{array}$$

De donde concluimos que:

$Z(f) = Z_{<-N,N>}(f) = Z_{<-\infty,+\infty>} = V(-\infty) - V(+\infty) = 1$

$\therefore$ *el número total de raíces reales de f es* 1.

□

Como corolario del ejercicio precedente se obtiene.

Corolario 5.2 (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, entonces $Z(f) = V(-\infty) - V(+\infty)$ donde:*

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

Ejemplo 5.3. *Sea el polinomio cuadrático $f(x) = x^2 + bx + c \in \mathbb{R}[x]$. Vamos a justificar por medio del Teorema de Sturm, el hecho que f tiene 2 raíces reales si y solo sí $b^2 - 4c \geq 0$.*

f tiene raíces simples $\Leftrightarrow mcd(f, f') = 1$ donde $f'(x) = 2x + b$ o sea, $mcd(f, f') = 1 \Leftrightarrow f\left(-\frac{b}{2}\right) \neq 0 \Leftrightarrow \frac{b^2}{4} - \frac{b^2}{2} + c \neq 0 \Leftrightarrow b^2 - 4c \neq 0$

Es decir, si $b^2 - 4c \neq 0$, f tiene raíces simples y podemos aplicar directamente el Teorema de Sturm. Mientras que si $b^2 - 4c = 0$, $mcd(f, f') = x + \frac{b}{2}$ y tenemos que trabajar con el cociente $\overline{f}(x) = x + \frac{b}{2}$

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

   $f_0(x) = x^2 + bx + c, \quad f_1(x) = 2x + b, \quad f_2(x) = \frac{b^2-4c}{4}$

   Luego

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

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

   Es decir,

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

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

$$\overline{f_0}(x) = x + \frac{b}{2} \ , \ \overline{f_1}(x) = 1$$

   aqui,

$$V(-\infty) = V(-\infty, 1) = 1 \quad y$$

$$V(+\infty) = V(+\infty, 1) = 0,$$

   entonces:

$$Z(\overline{f}) = 1,$$

   es decir f tiene una raíz doble.

□

Prueba Del Teorema de Sturm

Dado que f y f' son primos entre sí, y que la sucesión de Sturm coincide salvo eventualmente signos con la sucesión de restos dado por el Algoritmo de Euclides,

no solamente se obtiene que $f_s \in \mathbb{R}\backslash\{0\}$,sino que para todo $i, (1 \leq i \leq s-1)$ los polinomios f_i y f_{i+1} son primos entre sí, 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 (si hubiese un cambio de signo, habría una raíz). Por lo tanto $f_i(c)$ es de signo constante, para $c \in I$. Denotemos por $\beta_1, \beta_2, \ldots, \beta_t$ todas las raíces del polinomio f_i ordenados de menor a mayor y por $c_1, \ldots, c_{t-1}$ puntos intermedios elegidos arbitrarios:

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

Calculemos

$$V(a) - V(b) = [V(a) - V(c_1] + [V(c_1) - V(c_2)] + \ldots + [V(c_{t-1}) - V(b)]$$

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

1. 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 dan las siguientes posibilidades:

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

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

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

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

En cualquiera de los dos casos:

$$V(f_0(c_{k-1}), f_1(c_{k-1})) - V(f_0(c_k), f_1(c_k)) = 1 - 0 = 1$$

2. 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 mcd $(f_{i-1}, f_i) = 1 =$ mcd (f_i, f_{i+1})), y por lo tanto f_{i-1} y f_{i+1} tienen signo constante en $[c_{i-1}, c_k]$.

   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 signos opuestos, 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}	$-$		$-$

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

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

3. 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:

$$\begin{aligned} V(c_{k-1}) - V(c_k) \quad &= V(f_0(c_{k-1}), f_1(c_{k-1}), \ldots, f_s(c_{k-1})) - \\ &\qquad V(f_0(c_k), f_1(c_k), \ldots, f_s(c_k)) \end{aligned}$$

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 encuentra 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 calcular en forma exacta la cantidad de raíces reales de un polinomio f libre de cuadrados. Aún más, permite

por dicotomía, aproximar tanto como se quiere (hallando intervalos pequeños donde se encuentra exactamente una raíz de f). Pero la operatividad de este algoritmo es muy elevado, y podemos observar que en las sucesivas divisiones para construir la sucesión de Sturm, aparecen números cada vez más grandes, aún así el polinomio sea simple en $\mathbb{Z}[x]$.

Ejemplo 5.4. *(Polinomios de tercer grado)*

Aquí utilizaremos la discusión de este párrafo para determinar cuántos raíces reales tiene el polinomio $x^3 + px + q$ en función de los parámetros $p, q \in \mathbb{R}$.

$$f(x) = x^3 + px + q \ , \ p, q \in \mathbb{R}$$

El polinomio f tiene 1 o 3 raíces reales. Vamos a distinguir los casos posibles según los signos que pueden tener p y q, aplicando la regla de los signos de Descartes y el Teorema de Sturm.

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

$V(-,0,-,q)$

Aplicando la regla de los signos de Descartes:

Si $q > 0, V(f) = 0$ *y* $V(f(-x)) = 1$, f *tiene exactamente* 1 *raíz real negativa; si* $q < 0$, $V(f) = 1$ *y* $V(f(-x)) = 0$, *entonces* f *tiene exactamente* 1 *raíz real positiva. Luego en ambos casos si* $p > 0$ f *tiene exactamente* 1 *raíz real.*

4. *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 debemos averiguar 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 positica y hay que determinar si tiene* 0 *ó* 2 *raíces reales negativas.*

     Concluyamos la discusión aplicando el Teorema de Sturm al polinomio f. *Calculando la sucesión de Sturm, se tiene:*

     $f_0(x) = x^3 + px + q$, $\quad f_1(x) = 3x^2 + p$, $\quad f_2(x) = -\frac{2p}{3}x - q$,

     $f_3(x) = \frac{-4p^3 - 27q^2}{4p^2}$

     f *es libre de cuadrados si y solo si* $4p^3 + 27q^2 \neq 0$, *y en esta caso podemos aplicar directamente el Teorema de Sturm.*

   - *Caso* $4p^3 + 27q^2 \neq 0$*:*

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

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

     Luego

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

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

Usando la sucesión de Sturm, también podemos enumerar los ceros de polinomios complejos en regiones no acotadas del plano complejo. El siguiente teorema establece:

Teorema 5.3 (Teorema de Routh)**.** *Sean* $p(z)=\gamma(z)+i\delta(z)$*, donde* $\gamma(z)=Re(p(z))$ *y* $\delta(z)=Im(p(z))$ *son polinomios reales, con* $\delta(z)\neq 0$ *y que no tenga ceros reales. El polinomio* $p(z)$ *posee* n_1 *ceros (contando con sus multiplicidades) en el semiplano superior del plano complejo y* n_2 *ceros (contando con sus multiplicidades) en el semiplano inferior del plano complejo.*
Sea $V(z)$ *la variación de signos obtenidos en el punto* z *para la sucesión de Sturm iniciada con* $\gamma(z)$ *y* $\delta(z)$*, evaluándose* $z\in\mathbb{R}$*. Entonces para* $n=gr(p)$ *se tiene:*

$$n_1=\frac{1}{2}(n+V(\infty)-V(-\infty))$$

$$n_2=\frac{1}{2}(n-V(\infty)+V(-\infty))$$

Prueba [ver ([8])].

Ejemplo 5.5. $P(z)=z^5+2z^3+(3+i)z^2+(-63+i)$*, entonces*
$\gamma(z)=Re(p(z))=z^5+2z^3+3z^2-63$ *y* $\delta(z)=Im(p(z))=z^2+1\neq 0$
Luego la sucesión de Sturm tiene la forma:

$$\begin{aligned} f_0(z) &= \gamma(z)\\ f_1(z) &= \delta(z)\\ f_2(z) &= z+66\\ f_3(z) &= -4357\neq 0 \end{aligned}$$

Ahora $V(\infty) = 1$ *y* $V(-\infty) = 2$*, aplicando el toerema (5.3) obtenemos*

$$\begin{aligned} n_1 &= \tfrac{1}{2}(n + V(\infty) - V(-\infty) = \tfrac{1}{2}(5 + 1 - 2) = 2 \\ n_2 &= \tfrac{1}{2}(n - V(\infty) + V(-\infty) = \tfrac{1}{2}(5 - 1 + 2) = 3. \end{aligned}$$

Así tenemos $n_1 = 2$ *ceros en el semiplano superior y* $n_2 = 3$ *ceros en el semiplano inferior.*

También podemos determinar los ceros $p(z)$ en el semiplano derecho del plano complejo, basta hacer la transformación $z \leftarrow iz$. En el ejemplo anterior se obtiene 3 ceros en el semiplano derecho y 2 en el semiplano izquierdo del plano complejo.

En general podemos determinar los ceros de $p(z)$ en cada cuadrante del plano complejo.

6 CONCLUSIONES

Vemos que el estudio de los polinomios es esencial e importante, desde la óptica matemática y práctica.

Nos permite resolver ecuaciones, estudiar funciones y también hallar sus raíces, nos llevan a dar soluciones a problemas generales que se plantean, como resolver una ecuación diferencial lineal, hallar los valores propios de una matriz, etc.

Para estudiar las raíces de un polinomio, se ha tenido que realizar estudios previos, desarrollar una serie de teorías, a travez de los tiempos este conocimiento ha prosperado y se han sentado bases sólidas.

los polinomios constituyen objetos matemáticos importantes, pues, permite resolver ciertas ecuaciones diferenciales de segundo orden suponiendo soluciones polinomicas de infinitos términos, también aparecen como pollinomios de Bessel y de Lagendre.

Podemos también ver los polinomios como funciones conitnuas con derivadas continuas de todos los ordenes.

El estudio analítico de los polinomios constituye una teoría rigurosa y formal cuyas aplicaciones en la ingeniería, fisíca, economía entres otras disciplinas son múltiples.

Bibliografía

[1] B. N. Datta, Numerical Linear Algebra and Applications, Books Publishing Company. 1995.

[2] R. A. DeCarlo, Linear Systems: A State Variable Approach with Numerical Implementation, Printice Hall, 1989.

[3] B. P. Deminovich y I. A. Maron, Cálculo Numérico Fundamental, Paraninfo- Madrid, 1985.

[4] Fraleigh, John B. A First Course in Abstract Algebra, Addison Wesley 2002.

[5] P. Henrici, Applied Computational Complex Analysis, Vol. 1. John Wiley & Sons 1977.

[6] Herstein, I. N. Álgebra Moderna Ginn 1964.

[7] P. D. Lax, Linear Algebra and Its Applications, The Wiley Bicentennial-Knowledge 2007

[8] Marden, Morris. Geometry of polinomyals. American Mathematical Society Providence, Rhode Island. Mathematical Surveys and Monographs, number 3, 1989.

[9] C. D. Meyer, Matrix Analysis and Applied Linear Algebra, SIAM 2001.

[10] E. D. Nering, Álgebra Lineal y Teoría de Matrices, Editorial Limusa, México 1984.

[11] B. Noble y J. W. Daniel, Álgebra Lineal Aplicada, Prentice-Hall Hispanoamericana. S.A. 1989

[12] G. Strang, Linear Algebra and Its Applications, Books/Cole 2005.

[13] L. Trefethen, Numerical Linear Algebra. SIAM 1997.