24

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE CIENCIAS

CAMPOS REALES CERRADOS Y CONTEO DE RAÍCES

ALGUNAS PROPIEDADES BÁSICAS Y EL TEOREMA BUDAN-FOURIER

T E S I S

PARA OBTENER EL GRADO DE:

M A T E M Á T I C O

P R E S E N T A :

TOMÁS LAJOUS LOAEZA

DIRECTOR DE TESIS: DR. ENRIQUE JAVIER ELIZONDO HUERTA

VNIVERSIDAD NACIONAL
AVENMA DE
MEXICO

M. EN C. ELENA DE OTEYZA DE OTEYZA
Jefa de la División de Estudios Profesionales de la
Facultad de Ciencias
Presente

Comunicamos a usted que hemos revisado el trabajo escrito:

Campos reales cerrados y conteo de raíces. Algunas propiedades básicas y el Teorema Budan-Fourier.

realizado por Tomás Lajous Loaeza

con número de cuenta 9851124-6 , quién cubrió los créditos de la carrera de Matemáticas

Dicho trabajo cuenta con nuestro voto aprobatorio.

Atentamente

Director de Tesis Propietario	Dr. Enrique Javier Elizondo Huerta	Javier Elizondo
Propietario	Dra. María de la Paz Alvarez Scherer	4/VII/1
Propietario	M. en C. Francisco de Jesús Struck Chávez	
Suplente	Dr. Héctor Fidencio Sánchez Morgado	F. Sánchez M
Suplente	Mat. José de Jesús Malagón López	11 Malagón

Consejo Departamental de
Matemáticas

M. EN C. ALEJANDRO BRAVO MOJICA

CONSEJO DEPARTAMENTAL
DE
MATEMATICAS

Campos reales cerrados y conteo de raíces

Algunas propiedades básicas y el Teorema Budan-Fourier

Tomás Lajous Loaeza

Tesis para obtener el grado de
MATEMÁTICO

2002

Facultad de Ciencias
Universidad Nacional Autónoma de México

A mis padres

AGRADECIMIENTOS

Junto con la presentación de este trabajo, quiero agradecer a quienes lo hicieron posible. Aprovecho esta página para agradecer:

a José Antonio de la Peña (IMATE-UNAM), Guillermo Fernández del Busto (McKinsey & Co.), y Doug Lind (University of Washington) por su apoyo y generosidad;

a María de la Paz Álvarez Scherer (FdeC-UNAM) por su apoyo incondicional, y a Oscar Palmas (FdeC-UNAM), Francisco Struck (FdeC-UNAM) y Dan Pollack (University of Washington) por haberme, junto con ella, enseñado geometría con mucha paciencia;

a Felipe Bracho (IIMAS-UNAM) por haberme ayudado a aprender cómo acercarme al estudio de las matemáticas, y a León Kushner (FdeC-UNAM) por haberme apoyado al entender de qué se trata y por haberme enseñado el álgebra que ahora uso;

a Javier Elizondo (IMATE-UNAM), mi director de tesis, por llevarme de la mano, aún cuando nos encontrábamos a grandes distancias, y tenerme la paciencia que yo a veces me perdía, a través del tan accidentado desarrollo de esta tesis de licenciatura;

de nuevo al Prof. Elizondo, a Ricky Pollack (CIMS-NYU), y a Miles Reid (Mathematics Institute, University of Warwick) por haberme enseñado a trabajar y a escribir, y particularmente, por haberme enseñado geometría algebraica.

RESUMEN

Esta tesis pretende ser una presentación introductoria al concepto de campo real cerrado y al conteo de raíces reales. La estructura general, al igual que los resultados, proviene del manuscrito *Algorithms in Real Algebraic Geometry* de Saugata Basu, Richard Pollack y Marie-Françoise Roy.

Empezamos definiendo el concepto de campo real cerrado dando algunas de sus propiedades fundamentales. Después de esto podemos hacer la comparación con campos algebraicamente cerrados (un concepto bastante más común) y terminamos dando una herramienta que usaremos más adelante. Este primer capítulo lleva la mayor carga teórica.

En el segundo capítulo demostramos el Teorema Budan-Fourier. El objetivo de esta parte del trabajo es introducir el conteo de raíces en campos reales cerrados. Se centra en la demostración del teorema pero se da también un caso particular de interés. Para cerrar, se dan una aplicación y un ejemplo concreto que pretenden ilustrar el uso de estas herramientas y ayudar al entendimiento del teorema y su demostración.

Este documento fue preparado usando los paquetes `amsmath`, `amssymb` y `amsthm` (parte de $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX, "the TEX macro system of the *American Mathematical Society*") en la distribución teTEX de LATEX 2_ε para `darwin1`, corriendo bajo TEXShop en X.

ÍNDICE GENERAL

1. DEFINICIONES Y PROPIEDADES BÁSICAS

En este capítulo, definimos campos reales y reales cerrados, luego exponemos algunas de sus propiedades básicas. De esta manera preparamos el terreno para luego demostrar el Teorema Budan-Fourier.

1.1 Definición de campo real cerrado

Empezamos con las definiciones básicas.

Un **campo ordenado** $(F, \leq)$ es un campo, F, junto con un orden total, $\leq$, que satisface:

(i) $x \leq y \Rightarrow x + z \leq y + z$,

(ii) $0 \leq x, 0 \leq y \Rightarrow 0 \leq xy$.

El **signo**, signo(a), de un elemento $a \in F$ es

$$\begin{cases} 0 & \text{si } a = 0, \\ 1 & \text{si } a > 0, \\ -1 & \text{si } a < 0. \end{cases}$$

Un **cono** del campo F es un subconjunto P de F tal que:

(i) $x \in P, y \in P \Rightarrow x + y \in P$,

(ii) $x \in P, y \in P \Rightarrow xy \in P$,

(iii) $x \in F \Rightarrow x^2 \in P$.

El cono P es **propio** si además:

(iv) $-1 \notin P$.

Sea $(F, \leq)$ un campo ordenado. El **cono positivo** de $(F, \leq)$ es el subconjunto

$$P = \{x \in F \mid x \geq 0\}.$$

Proposición 1. *Sea $(F, \leq)$ un campo ordenado. El cono positivo P de $(F, \leq)$ es un cono propio que satisface:*

(v) $P \cup -P = F$ *(donde* $-P = \{x \in F \mid -x \in P\}$*).*

Conversamente, si P es un cono propio de un campo F que satisface ***(v)****, entonces F está ordenado por*

$$x \leq y \Leftrightarrow y - x \in P.$$

Demostración. Si P es el cono positivo de F, es claro que $P, -P \subset F$, por lo que $P \cup -P \subset F$. Ahora, sea $x \in F$. Como F es un campo ordenado, podemos usar la ley de tricotomía para ver que sucede uno de los casos $x < 0, x = 0, x > 0$. Si $x = 0$ o $x > 0$ tenemos que $x \in P$. Por otra parte, la definición de $-P$ es equivalente a $-P = \{x \in F \mid x \leq 0\}$, por lo que si $x < 0$, $x \in -P$. Entonces, si $x \in F$, $x \in P$ o $x \in -P$, o de otra forma, $P \cup -P \supset F$. Por lo tanto, $P \cup -P = F$.

Supongamos que P es un cono propio de F que satisface **(v)**. Sean $x, y \in F$ tales que $x \leq y$. Tenemos tres casos a considerar:

$x, y \in P$: $x \leq y \Rightarrow x + (-x) \leq y + (-x) \Rightarrow 0 \leq y - x \Rightarrow y - x \in P$,

$x \in -P, y \in P$: $x \in -P \Rightarrow -x \in P \Rightarrow y - x \in P$,

$x, y \in -P$: $\Rightarrow -x, -y \in P$ y regresamos al primer caso.

Tenemos de los casos anteriores que $x \leq y \Rightarrow y - x \in P$. Por otra parte, sean $x, y \in F$ tales que $y - x \in P$. Luego que $0 \leq y - x \Rightarrow 0 + x \leq y - x + x \Rightarrow x \leq y$. Vemos entonces que $x \leq y$. Por lo tanto, $x \leq y \Leftrightarrow y - x \in P$. □

Usamos $F^{(2)}$ para denotar los cuadrados de los elementos de F y $\sum F^{(2)}$ el conjunto de **sumas de cuadrados de elementos de** F. Claramente, $\sum F^{(2)}$ es un cono contenido en todo cono de F.

Un campo F es un **campo real** si $-1 \notin \sum F^{(2)}$. Notemos que un campo real debe de tener característica 0.

Damos ahora la presentación del lema de Zorn, que usaremos para demostrar el Lema 1. Como nota al margen, mencionamos un resultado

no-trivial[1]: *el lema de Zorn es independiente de los axiomas (Zermelo-Fraenkel) de teoría de conjuntos.* También, notamos que el axioma de elección y el principio del buen orden son presentaciones equivalentes de este lema.

Lema de Zorn. *Sea S un conjunto no-vacío ordenado inductivamente. Existe un elemento maximal en S.*[2]

Lema 1. *Si P es un cono propio de F entonces*

(i) Si $-a \notin P$ entonces $P[a] = \{x + ay \mid x, y \in P\}$ es un cono propio de F.

(ii) P está contenido en el cono positivo de un orden sobre F.

Demostración.

(i) Supongamos que $-1 = x + ay$ con $x, y \in P$. Tenemos dos casos, o $y = 0$ o $y \neq 0$. Si $y = 0$ tenemos que $-1 \in P$, que es una contradicción. Si $y \neq 0$, entonces $-a = (1/y)^2 y(1 + x) \in P$, que también es una contradicción. Por lo tanto $x + ay \neq -1, \forall x, y \in P$, y $P[a]$ es un cono propio de F.

(ii) Consideremos una cadena de conos propios de F ordenados por contención. Su unión es de nuevo un cono propio de F. Consideremos la cadena de uniones de cadenas de conos propios. Este conjunto, S, está ordenado inductivamente y es no-vacío pues contiene al menos a P. Entonces el lema de Zorn nos dice que existe Q, un cono propio maximal, que contiene a P. Nos es suficiente mostrar que $Q \cup -Q = F$ para ver que Q es el cono positivo de un orden de F. Supongamos que $-a \notin Q$. Entonces, **(i)** nos dice que $Q[a]$ es un cono propio. Ahora, como Q es maximal, $Q[a] = Q$ y entonces $a \in Q$, o $-a \in -Q$. Es decir, $Q \cup -Q = F$ y por lo tanto $P \subset Q$, donde Q es el cono positivo de algún orden en F.

□

Damos ahora una proposición que caracteriza un campo real.

[1] Ver Dummit, David y Foote, Richard, *Abstract Algebra, Second Edition*, John Wiley & Sons, 1999. p.875.

[2] Presentado como en Lang, Serge, *Algebra, Third Edition*, Addison-Wesley, 1993. p.880.

Proposición 2. *Sea F un campo. Entonces las siguientes propiedades son equivalentes:*

(i) *F es real.*

(ii) *F tiene un cono propio.*

(iii) *F se puede ordenar.*

(iv) *Para todo $x_1, x_2, \ldots, x_n$ en F*

$$\sum_{i=1}^{n} x_i^2 = 0 \Rightarrow x_1 = x_2 = \cdots = x_n = 0.$$

Demostración.

(i)⇔(iii) Como F es real, $-1 \notin \sum F^{(2)}$ y $\sum F^{(2)}$ es un cono propio. Ahora, por el Lema 1, $\sum F^{(2)}$ está contenido en el cono positivo de un orden de F. Por lo tanto F se puede ordenar y **(i)⇒(iii)**.

Por otra parte, supongamos que F tiene un orden $\leq$. Entonces, por la Proposición 1, el cono positivo P de $(F, \leq)$ es propio. Ahora, como $\sum F^{(2)} \subset P$ y $-1 \notin P$, tenemos que $-1 \notin \sum F^{(2)}$. Por lo tanto, F es real y **(iii)⇒(i)**.

(iii)⇒(ii) Es directo de la Proposición 1.

(ii)⇒(iv) Usando la condición **(ii)** del Lema 1, como F tiene un cono propio, sea P, P está contenido en el cono positivo de un orden de F. Sean $x_1, x_2, \ldots, x_n \in F$, en este orden de F, $x_1^2, x_2^2, \ldots, x_n^2 \geq 0$. Luego que $\sum_{i=1}^{n} x_i^2$ es una suma de elementos no negativos que es igual a 0. De aquí que todos los sumandos, $x_1^2, x_2^2, \ldots, x_n^2$, son cero y por lo tanto $x_1 = x_2 = \cdots = x_n = 0$.

(iv)⇔(i) Supongamos que **(i)** es falso, entonces existen $x_1, \ldots, x_n$ en F para los cuales $-1 = \sum_{i=1}^{n} x_i^2$. Esto implica entonces que **(iv)** es falso y por lo tanto que **(iv)⇒(i)**.

Ahora, supongamos que **(iv)** es falso, entonces existen $x_1, \ldots, x_n$ en F, no todos cero, con $\sum_{i=1}^{n} x_i^2 = 0$. Sin pérdida de generalidad, asumimos que $x_1 \neq 0$. Entonces $-x_1 = \sum_{i=2}^{n} x_i^2$, y $-1 = \sum_{i=2}^{n} (x_i/x_1)^2$. Esto implica entonces que **(i)** es falso y por lo tanto que **(i)⇒(iv)**.

Por lo tanto **(i)**, **(ii)**, **(iii)**, y **(iv)** son equivalentes. □

Un **campo real cerrado** R es un campo ordenado, cuyo cono positivo es el conjunto de cuadrados $R^{(2)}$, y tal que todo polinomio en $R[X]$ de grado impar tiene una raíz en R.

(Notamos que la condición de que el cono positivo de un campo real cerrado R sea $R^{(2)}$ quiere decir que R tiene un orden único como campo ordenado.)

1.2 Relación entre campos algebraicamente cerrados y campos reales cerrados

Empezamos esta sección con resultados intermedios para luego caracterizar un campo real cerrado en términos de su relación con campos algebraicamente cerrados y extensiones algebraicas.

Un polinomio $Q(Y_1, \ldots, Y_p) \in F[Y_1, \ldots, Y_p]$ es **simétrico** si para toda permutación σ de $\{1, 2, \ldots, p\}$, $Q(Y_{\sigma(1)}, \ldots, Y_{\sigma(2)}) = Q(Y_1, \ldots, Y_p)$.

Para $k = 1, 2, \ldots, p$, la **k-ésima función simétrica elemental** es

$$E_k = \sum_{1 \le i_1 < \cdots < i_k \le p} Y_{i_1} \cdot Y_{i_2} \cdots Y_{i_k}.$$

Definimos el **orden lexicográfico** sobre los monomios de tal manera que

$$Y^\alpha = Y_1^{\alpha_1} \cdot Y_2^{\alpha_2} \cdots Y_p^{\alpha_p} > Y^\beta = Y_1^{\beta_1} \cdot Y_2^{\beta_2} \cdots Y_p^{\beta_p}$$

si

$$\begin{gathered}(\alpha_1 > \beta_1) \\ \vee(\alpha_1 = \beta_1, \alpha_2 > \beta_2) \\ \vdots \\ \vee(\alpha_1 = \beta_1, \ldots, \alpha_{k-1} = \beta_{k-1}, \alpha_k > \beta k) \\ \vdots \\ \vee(\alpha_1 = \beta_1, \ldots, \alpha_{p-1} = \beta_{p-1}, \alpha_p > \beta_p),\end{gathered}$$

Proposición 3. *Sea F un campo y $Q(Y_1, \ldots, Y_p) \in F[Y_1, \ldots Y_p]$ un polinomio simétrico. Existe un polinomio $R(T_1, \ldots, T_p) \in F[T_1, \ldots, T_p]$ tal que $Q(Y_1, \ldots, Y_p) = R(E_1, \ldots, E_p)$.*

Demostración. Como $Q(Y_1, \ldots, Y_p)$ es simétrico, su monomio principal en el orden lexicográfico $c_\alpha Y^\alpha = c_\alpha Y_1^{\alpha_1} \cdots Y_p^{\alpha_p}$ satisface $\alpha_1 \ge \cdots \ge \alpha_p$. Consideramos ahora $c_\alpha E_1^{\alpha_1 - \alpha_2} \cdots E_{p-1}^{\alpha_{p-1} - \alpha_p} \cdot E_p^{\alpha_p}$, su monomio principal con respecto al orden lexicográfico es también $c_\alpha Y^\alpha = c_\alpha Y_1^{\alpha_1} \cdots Y_p^{\alpha_p}$. Ahora, sea

$$Q_1 = Q(Y_1, \ldots, Y_p) - c_\alpha E_1^{\alpha_1 - \alpha_2} \cdots E_{p-1}^{\alpha_{p-1} - \alpha_p} \cdot E_p^{\alpha_p}.$$

Si $Q_1 = 0$, tenemos que $R(E_1, \ldots, E_p) = c_\alpha E_1^{\alpha_1 - \alpha_2} \cdots E_{p-1}^{\alpha_{p-1} - \alpha_p} \cdot E_p^{\alpha_p}$ y por lo tanto que $Q(Y_1, \ldots, Y_p) = R(E_1, \ldots, E_p)$. De lo contrario, el monomio

principal con respecto al orden lexicográfico de Q_1 es estrictamente menor que $Y_1^{\alpha_1} \cdots Y_p^{\alpha_p}$. Entonces iteramos la construcción anterior con Q_1. Notamos ahora que no existe una sucesión decreciente infinita de monomios en el orden lexicográfico. Por lo tanto la construcción iterativa debe de parar. Llegamos entonces a una n finita tal que $Q_n = 0$. Retrocedemos en el proceso sustituyendo los $Q_i, 1 \leq i \leq n-1$ por polinomios en $E_1, \ldots, E_p$. Tenemos entonces una expresión de $Q(Y_1, \ldots, Y_p)$ en términos de $E_1, \ldots, E_p$. Esto termina la demostración. □

Lema 2. *Sean $y_1, \ldots, y_p$ elementos de un campo F y $P = (X - y_1), \ldots, (X - y_p) = X^p + C_1 X^{p-1} + \cdots + C_p$, entonces $C_k = (-1)^k E_k$. Donde E_k es la k-ésima función simétrica elemental evaluada en $Y_i = y_i, 1 \leq i \leq p$.*

Demostración. Primero hacemos la expansión de $(X - y_1), \ldots, (X - y_p)$. Un cómputo relativamente tedioso nos muestra que

$$\begin{aligned}(X - y_1), \ldots, (X - y_p) &= X^p + (-1)^1 (y_1 + \cdots + y_p) X^{p-1} \\ &\quad + (-1)^2 (y_1 y_2 \cdot y_1 y_3 \cdots y_1 y_p \cdots y_{p-1} yp) + \cdots \\ &\quad + (-1)^p y_1 \cdots y_p \\ &= X^p - E_1 X^{p-1} + \cdots + (-1)^p E_p.\end{aligned}$$

Por lo tanto, $P = X^p + C_1 X^{p-1} + \cdots + C_p$, con $C_k = (-1)^k E_k$. □

Corolario 1. *Sea $P \in F[X]$, y $y_1, \ldots, y_d$ las raíces de P (contadas con multiplicidad) en un campo algebraicamente cerrado C que contenga a F. Si un polinomio $Q(Y_1, \ldots, Y_d) \in F[Y_1, \ldots, Y_d]$ es simétrico, $Q(y_1, \ldots, y_d) \in F$.*

Demostración. Sea $P \in F[X]$ con raíces $y_1, \ldots y_p \in C$. Como C es algebraicamente cerrado, P se factoriza como $P = (X - y_1), \ldots, (X - y_p)$. Por el Lema 2, $P = X^p - E_1 X^{p-1} + \cdots + (-1)^p E_p$, donde E_k es la k-ésima función simétrica elemental evaluada en $Y_i = y_i, 1 \leq i \leq p$. Como $P \in F[X]$, tenemos que E_k, evaluada en $Y_i = y_i, 1 \leq i \leq p$, está en F.

Ahora, sea $Q(Y_1, \ldots, Y_d) \in F[Y_1, \ldots, Y_d]$ simétrico. Entonces por la Proposición 3, $Q(Y_1, \ldots, Y_p) = R(E_1, \ldots, E_p)$. Luego que $Q(y_1, \ldots, y_p)$ se puede expresar en términos de $E_k, 1 \leq k \leq p$, donde E_k es la k-ésima función simétrica elemental evaluada en $Y_i = y_i, 1 \leq i \leq p$. Como cada E_k evaluada en $Y_i = y_i, 1 \leq i \leq p$ está en F, tenemos que $Q(y_1, \ldots, y_p) \in F$. □

La siguiente proposición caracteriza un campo real cerrado en términos de extensiones algebraicas y campos algebraicamente cerrados.

Proposición 4. *Si F es un campo, las siguientes propiedades son equivalentes:*

(i) *F es real cerrado.*

(ii) *$F[i] = F[X]/(X^2 + 1)$ es un campo algebraicamente cerrado.*

(iii) *F es un campo real que no tiene una extensión algebraica real no-trivial. Es decir, no existe ningún campo real F_1 que sea algebraico sobre F y distinto de F.*

Demostración.

(i)⇒(ii) Sea $P \in F[X]$ de grado $p = 2^m n$ con n impar. Mostramos por inducción sobre m que P tiene una raíz en $F[i]$. Si $m = 0$ entonces p es impar y P tiene una raíz en F y por tanto en $F[i]$. Supongamos el resultado para $m - 1$. Sean $y_1, \dots y_p$ las raíces de P contadas con multiplicidad en un campo algebraicamente cerrado que contenga a F. Para todo $h \in \mathbb{Z}$, sea

$$Q_h(Y_1, \dots, Y_p, X) = \prod_{\lambda<\mu}(X - Y_\lambda - Y_\mu - hY_\lambda Y_\mu).$$

Los coeficientes del polinomio $Q_h(Y_1, \dots, Y_p, X)$ son simétricos en $Y_1, \dots, Y_p$, y entonces, por el Corolario 1, $Q_h(y_1, \dots, y_p, X) \in F[X]$. El grado de $Q_h(y_1, \dots, y_p, X)$ es $p(p-1)/2 = 2^{m-1}n'$ con n' impar. Por la hipótesis de inducción, $Q_h(y_1, \dots, y_p, X)$ tiene una raíz en $F[i]$, luego que para cada $h \in \mathbb{Z}$ existen λ y μ con $y_\lambda + y_\mu + hy_\lambda y_\mu \in F[i]$. Ahora, como hay una infinidad de enteros y sólo un número finito de pares λ y μ, existen λ y μ con $y_\lambda + y_\mu \in F[i]$ y $y_\lambda y_\mu \in F[i]$. Estos elementos y_λ y y_μ son las soluciones de una ecuación cuadrática con coeficientes en $F[i]$, que tienes sus dos soluciones en $F[i]$. El polinomio P tiene entonces una raíz en $F[i]$.

Para $P = a_p X^p + \cdots + a_0 \in F[i][X]$, escribimos $\overline{P} = \overline{a_p} X^p + \cdots + \overline{a_0}$. Como $P\overline{P} \in F[X]$, $P\overline{P}$ tiene una raíz x en $F[i]$. Luego que $P(x) = 0$ o $\overline{P}(x) = 0$. En el primer caso ya terminamos y en el segundo $P(\overline{x}) = 0$.

(ii)⇒(iii) Primero demostramos que F es real. Como $F[i]$ es un campo, $X^2 + 1$ es irreducible sobre F. Entonces -1 no es un cuadrado en F. Ahora, sólo nos falta mostrar que, en F, una suma de cuadrados es

un cuadrado. Sean $a, b \in F$ y $c, d \in F$ tales que $a + ib = (c + id)^2$. Luego, consideremos las normas de $a + ib$ y de $(c + id)^2$. Tenemos entonces que

$$||a + ib|| = (a + ib)(\overline{a + ib}) = (a + ib)(a - ib) = a^2 + b^2$$

y

$$\begin{aligned} ||c + id|| &= (c + id)^2\overline{(c + id)^2} = (c^2 - d^2 + 2icd)(c^2 - d^2 - 2icd) \\ &= c^4 + 2c^2d^2 + d^4 = (c^2 + d^2)^2. \end{aligned}$$

Luego, como $||a + ib|| = ||c + id||$, tenemos que $a^2 + b^2 = (c^2 + d^2)^2$, y que una suma de cuadrados en F es un cuadrado. Entonces no hay suma de cuadrados en F igual a -1, y por lo tanto F es real.

Para concluir, sólo nos hace falta notar que $F[i]$ es la única extensión algebraica no trivial de F.

(iii)⇒(i) Supongamos que $a \in F$. Si a no es un cuadrado en F, entonces $F[\sqrt{a}] = F[X]/(X^2 - a)$ es una extensión algebraica no trivial de F, y luego que $F[\sqrt{a}]$ no es real. Por tanto,

$$-1 = \sum_{i=1}^{n}(x_i + \sqrt{a}y_i)^2, \text{ de donde } -1 = \sum_{i=1}^{n} x_i^2 + a\sum_{i=1}^{n} y_i^2 \in F.$$

Ahora, como F es real, $-1 \neq \sum_{i=1}^{n} x_i^2$ y de aquí que $y = \sum_{i=1}^{n} y_i^2 \neq 0$. Tenemos entonces que

$$\begin{aligned} -a &= \left(\sum_{i=1}^{n} y_i^2\right)^{-1}\left(1 + \sum_{i=1}^{n} x_i^2\right) \\ &= \left(\sum_{i=1}^{n}\left(\frac{y_i}{y^2}\right)^2\right)\left(1 + \sum_{i=1}^{n} x_i^2\right) \in \sum F^2. \end{aligned}$$

Lo anterior muestra que $F^{(2)} \cup -F^{(2)} = F$ y entonces que sólo hay un orden posible de F con $F^{(2)}$ como cono positivo. También muestra que si a no es un cuadrado, es negativo en este orden y por tanto que todo elemento positivo es un cuadrado.

Ahora sólo nos falta mostrar que si $P \in F[X]$ es de grado impar, entonces P tiene una raíz en F. Supongamos que no es el caso, sea P un polinomio de grado impar $p > 1$ tal que todo polinomio de grado impar $< p$ tiene una raíz en F. Como un polinomio de grado impar tiene al menos un factor irreducible impar, asumimos sin pérdida de generalidad que P es irreducible. El cociente $F[X]/(P)$ es una extensión algebraica no trivial de F y entonces

$$-1 = \sum_{i=1}^{n} H_i^2 + PQ, \text{ donde } \deg(H_i) < p.$$

Como el sumando de mayor grado en la expansión de $\sum_{i=1}^{n} H_i^2$ tiene una suma de cuadrados como coeficiente y F es real, $\sum_{i=1}^{n} H_i^2$ es un polinomio de grado par $< 2p-2$. Luego, el polinomio Q tiene grado impar $\leq p-2$, y una raíz x en F. Pero entonces $-1 = \sum_{i=1}^{n} H_i(x)^2$, que contradice el hecho de que F es real. Por lo tanto, para todo p impar, P de grado p tiene una raíz en F.

Por lo tanto, **(i)**, **(ii)** y **(iii)** son equivalentes. □

1.3 Una herramienta

En esta sección presentamos un serie de resultados que nos llevan a una herramienta importante en cuestiones de conteo de raíces. Son resultados que se derivan de las propiedades básicas y caracterizaciones dadas en las secciones anteriores.

Proposición 5. *Sea R un campo real cerrado, $P \in R[X]$. Los factores irreducibles de P son lineales, o de la forma $(X-c)^2+d^2=(X-c-id)(X-c+id)$.*

Demostración. La Proposición 4, (ii) nos asegura que $C = R[i]$ es algebraicamente cerrado. Entonces P se factoriza en factores lineales sobre C. Ahora, como en C el conjugado $c-id$ de una raíz $c+id$ de P también es raíz de P, tenemos que $(X-c-id), (X-c+id)$ son factores en C. De aquí que $(X-c)^2+d^2=(X-c-id)(X-c+id)$ es factor en R. De esta manera, todo factor de P en R que no sea lineal es de la forma dada. □

Proposición 6 (Teorema del valor intermedio). *Sea R un campo real cerrado, $P \in R[X], a, b \in R$ con $a < b$. Si $P(a)P(b) < 0$, entonces existe x en (a,b) tal que $P(x) = 0$.*

Demostración. Los factores irreducibles de P son, usando la Proposición 5 lineales o de la forma $(X-c)^2+d^2$. Si $\text{signo}(P(a)) \neq \text{signo}(P(b))$, entonces $\text{signo}(Q(a)) \neq \text{signo}(Q(b))$, para algún factor lineal Q de P. Entonces la raíz de Q está en (a,b) y por lo tanto existe $x \in (a,b)$ tal que $P(x) = 0$. □

Corolario 2. *Sea R un campo real cerrado, $P \in R[X]$ tal que P no vale cero en (a,b), entonces P tiene signo constante en el intervalo (a,b).*

Demostración. Supongamos que P no tiene signo constante en (a,b). Entonces la Proposición 6 nos dice que P tiene una raíz en (a,b), una contradicción. □

El corolario anterior muestra que tiene sentido hablar del signo de un polinomio a la derecha (respectivamente, izquierda) de cualquier $a \in R$. A saber, el signo de P a la derecha (resp., izquierda) de a es el signo de P en cualquier intervalo (a,b) (resp., (b,a)) en el que P no vale cero. También podemos hablar del signo de $P(+\infty)$ (resp., $P(-\infty)$) como el signo de $P(M)$ para M suficientemente grande (resp., chica).

Sea K un campo de característica 0. La **multiplicidad** de una raíz $r \in K$ de $P \in K[X]$ es el número entero μ tal que

$$P(r) = P'(r) = \cdots = P^{(\mu-1)}(r) = 0,\ P^{(\mu)} \neq 0.$$

De manera equivalente, $P = (X - r)^{\mu}Q(X)$ con $Q(r) \neq 0$. Si r no es raíz de P, la multiplicidad de r en P se define como 0.

Como una herramienta para demostrar los lemas que nos llevarán a la demostración del Teorema Budan-Fourier, damos la siguiente

Proposición 7. *Si r es una raíz de P en una campo real cerrado R de multiplicidad μ, entonces el signo de P a la derecha de r es el signo de $P^{(\mu)}(r)$ y el signo de P a la izquierda de r es el signo de $(-1)^{\mu}P^{(\mu)}(r)$.*

Demostración. Escribimos $P = (X - r)^{\mu}Q(X)$, donde $Q(r) \neq 0$. Ahora consideramos $P^{(\mu)}$. El primer sumando es claramente $Q(X)$, y los demás tienen un factor $(X - r)$, por lo que $P^{(\mu)}(r) = Q(r)$ y $\text{signo}(P^{(\mu)}(r)) = \text{signo}(Q(r))$.

Sea $\varepsilon > 0$, entonces, como $Q(r) \neq 0$, tenemos que

$$\text{signo}(Q(r - \varepsilon)) = \text{signo}(Q(r)) = \text{signo}(Q(r + \varepsilon)),$$

usando un argumento de continuidad. De aquí tenemos que

$$\text{signo}(P(r + \varepsilon)) = \text{signo}(\varepsilon^{\mu}Q(r + \varepsilon)) = \text{signo}(Q(r)) = \text{signo}(P^{(\mu)}(r))$$

y

$$\begin{aligned}\text{signo}(P(r - \varepsilon)) &= \text{signo}((-\varepsilon)^{\mu}Q(r + \varepsilon)) = \text{signo}((-1)^{\mu}Q(r)) \\ &= \text{signo}((-1)^{\mu}P^{(\mu)}(r))\end{aligned}$$

El resultado sigue por continuidad. □

2. CONTEO DE RAíCES

Hay un criterio muy simple para saber si un polinomio $P \in C[X]$ tiene alguna raíz en C, a saber, la tiene si y sólo si $\deg P \neq 0$. Es mucho más difícil decidir si un polinomio $P \in R[X]$ tiene una raíz en R. El primer resultado en esta dirección fue demostrado por Descartes, y luego generalizado por Budan con una demostración de Fourier. El resultado nos permite dar una cota superior al número de raíces de un polinomio en un intervalo (y de esta manera en R) y en algunos casos particulares de decidir directamente si el polinomio tiene al menos una raíz.

2.1 El Teorema Budan-Fourier

Empezando con algunas definiciones, podemos después demostrar dos lemas que harán posible la demostración del teorema. Seguimos esto con la demostración y presentación del Teorema Budan-Fourier.

El **número de cambios de signo**, $\mathrm{V}(a)$, en una sucesión, $a = a_1, \ldots, a_k$ de elementos de $R \setminus \{0\}$ se define por inducción sobre k como:

$$\mathrm{V}(a_1) = 0$$

$$\mathrm{V}(a_1, \ldots, a_k) = \begin{cases} \mathrm{V}(a_1, \ldots, a_{k-1}) + 1 & \text{si } \operatorname{signo}(a_{k-1}a_k) = -1 \\ \mathrm{V}(a_1, \ldots, a_{k-1}) & \text{si } \operatorname{signo}(a_{k-1}a_k) = 1 \end{cases}$$

Esta definición se extiende a cualquier sucesión finita a de elementos en R al considerar la sucesión finita b que se obtiene al eliminar los ceros en a y definiendo $\mathrm{V}(a) = \mathrm{V}(b)$, estipulando que V de la sucesión vacía es 0.

Sea P un polinomio de grado p en una variable en $R[X]$. Dado $a \in R \cup \{-\infty, \infty\}$, escribimos $\mathrm{V}(\mathrm{Der}(P); a)$ en lugar de $\mathrm{V}(P(a), P'(a), \ldots, P^p(a))$. Dados a y b en $R \cup \{-\infty, \infty\}$, escribimos $\mathrm{V}(\mathrm{Der}(P); a, b)$ en lugar de $\mathrm{V}(\mathrm{Der}(P); a) - \mathrm{V}(\mathrm{Der}(P); b)$. Usamos la notación $n(P; (a, b])$ para expresar el número de raíces de P en $(a, b]$ contadas con multiplicidad.

Lema 3. *Sea P un polinomio de grado p en una variable en $R[X]$; sea c una raíz de P con multiplicidad μ.*

Si ningún $P^{(k)}, 0 \leq k \leq \mu$ tiene raíz en $[d, c)$, entonces

$$V(P(d), P'(d), \ldots, P^{(\mu)}(d)) - V(P(c), P'(c), \ldots, P^{(\mu)}(c)) = \mu.$$

Si ningún $P^{(k)}$ tiene raíz en $(c, d']$, entonces

$$V(P(c), P'(c), \ldots, P^{(\mu)}(c)) - V(P(d'), P'(d'), \ldots, P^{(\mu)}(d')) = 0.$$

Demostración. Dado que c es una raíz de multiplicidad μ, tenemos que

$$V(P(c), P'(c), \ldots, P^{(\mu-1)}(c), P^{(\mu)}(c)) = V(0, 0, \ldots, 0, 0) = V(\emptyset) = 0.$$

Ahora, consideramos los signos de

$$P(d), P'(d), \ldots, P^{(\mu-1)}(d), P^{(\mu)}(d),$$

que, usando la Proposición 7, son iguales a los signos de

$$(-1)^{\mu} P^{(\mu)}(c), (-1)^{\mu-1} P^{(\mu)}(c), \ldots, -P^{(\mu)}(c), P^{(\mu)}(c),$$

y es claro que

$$V((-1)^{\mu} P^{(\mu)}(c), (-1)^{\mu-1} P^{(\mu)}(c), \ldots, -P^{(\mu)}(c), P^{(\mu)}(c)) = \mu.$$

Por lo tanto,

$$V(P(d), P'(d), \ldots, P^{(\mu)}(d)) - V(P(c), P'(c), \ldots, P^{(\mu)}(c)) = \mu.$$

Análogamente, los signos de

$$V(P(d'), P'(d'), \ldots, P^{(\mu-1)}(d'), P^{(\mu)}(d'))$$

son, usando la Proposición 7, iguales a los signos de

$$P^{(\mu)}(c), P^{(\mu)}(c), \ldots, P^{(\mu)}(c), P^{(\mu)}(c),$$

y es claro que

$$V(P^{(\mu)}(c), P^{(\mu)}(c), \ldots, P^{(\mu)}(c), P^{(\mu)}(c)) = 0.$$

Por lo tanto,

$$V(P(c), P'(c), \ldots, P^{(\mu)}(c)) - V(P(d'), P'(d'), \ldots, P^{(\mu)}(d')) = 0. \quad \square$$

Una vez demostrado este primer lema, pasamos a uno cuyo resultado es menos fuerte, y cuyo uso de la Proposición 7 es más sutil, pero que que tiene una consecuencia más marcada tanto en la demostración como en la presentación del teorema.

Lema 4. *Sea P un polinomio de grado p en una variable en $R[X]$; sea c una raíz de $P^{(i)}$ con multiplicidad μ y $P^{(i-1)}(c) \neq 0$.*

Si ningún $P^{(k)}, i-1 \leq k \leq i+\mu$ tiene raíz en $[d, c)$, entonces

$$V(P^{(i-1)}(d), P^{(i)}(d), \ldots, P^{(i+\mu)}(d)) - V(P^{(i-1)}(c), P^{(i)}(c), \ldots, P^{(i+\mu)}(c))$$

es par y no negativo.

Si ningún $P^{(k)}$ tiene raíz en $[c, d')$, entonces

$$V(P^{(i-1)}(c), P^{(i)}(c), \ldots, P^{(i+\mu)}(c)) - V(P^{(i-1)}(d'), P^{(i)}(d'), \ldots, P^{(i+\mu)}(d')) = 0.$$

Demostración. Consideremos los signos de

$$P^{(i-1)}(d), P^{(i)}(d), \ldots, P^{(i+\mu)}(d).$$

Dado que ni d ni c son raíces de $P^{(i-1)}$, y que no hay raíces de este entre d y c, tenemos que $\text{signo}(P^{(i-1)}(d)) = \text{signo}(P^{(i-1)}(c))$. Con esto en mente, y usando de nuevo la Proposición 7 vemos que los signos considerados son iguales a los signos de

$$P^{(i-1)}(c), (-1)^{(\mu)} P^{(i+\mu)}(c), \ldots, -P^{(i+\mu)}(c), P^{(i+\mu)}(c).$$

Análogamente, tenemos que los signos de

$$P^{(i-1)}(d'), P^{(i)}(d'), \ldots, P^{(i+\mu)}(d')$$

son, usando la Proposición 7, iguales a los de

$$P^{(i-1)}(c), P^{(i+\mu)}(c), \ldots, P^{(i+\mu)}(c), P^{(i+\mu)}(c).$$

Llegamos a la conclusión del lema examinando los cuatro posibles casos a continuación:

Si $P^{(i-1)}(c) \cdot P^{(i+\mu)}(c) > 0$ y μ es impar,

$$\begin{aligned} V(P^{(i-1)}(d), P^{(i)}(d), \ldots, P^{(i+\mu)}(d)) &= \mu + 1 \\ V(P^{(i-1)}(c), P^{(i)}(c), \ldots, P^{(i+\mu)}(c)) &= 0 \\ V(P^{(i-1)}(d'), P^{(i)}(d'), \ldots, P^{(i+\mu)}(d')) &= 0 \end{aligned}$$

Si $P^{(i-1)}(c) \cdot P^{(i+\mu)}(c) < 0$ y μ es impar,

$$\begin{aligned} V(P^{(i-1)}(d), P^{(i)}(d), \ldots, P^{(i+\mu)}(d)) &= \mu \\ V(P^{(i-1)}(c), P^{(i)}(c), \ldots, P^{(i+\mu)}(c)) &= 1 \\ V(P^{(i-1)}(d'), P^{(i)}(d'), \ldots, P^{(i+\mu)}(d')) &= 1 \end{aligned}$$

Si $P^{(i-1)}(c) \cdot P^{(i+\mu)}(c) > 0$ y μ es par,

$$\begin{aligned} V(P^{(i-1)}(d), P^{(i)}(d), \ldots, P^{(i+\mu)}(d)) &= \mu \\ V(P^{(i-1)}(c), P^{(i)}(c), \ldots, P^{(i+\mu)}(c)) &= 0 \\ V(P^{(i-1)}(d'), P^{(i)}(d'), \ldots, P^{(i+\mu)}(d')) &= 0 \end{aligned}$$

Si $P^{(i-1)}(c) \cdot P^{(i+\mu)}(c) < 0$ y μ es par,

$$\begin{aligned} V(P^{(i-1)}(d), P^{(i)}(d), \ldots, P^{(i+\mu)}(d)) &= \mu + 1 \\ V(P^{(i-1)}(c), P^{(i)}(c), \ldots, P^{(i+\mu)}(c)) &= 1 \\ V(P^{(i-1)}(d'), P^{(i)}(d'), \ldots, P^{(i+\mu)}(d')) &= 1 \end{aligned}$$

En todos los casos considerados es claro que

$$V(P^{(i-1)}(d), P^{(i)}(d), \ldots, P^{(i+\mu)}(d)) - V(P^{(i-1)}(c), P^{(i)}(c), \ldots, P^{(i+\mu)}(c))$$

es par y no negativo, y que

$$V(P^{(i-1)}(c), P^{(i)}(c), \ldots, P^{(i+\mu)}(c)) - V(P^{(i-1)}(d'), P^{(i)}(d'), \ldots, P^{(i+\mu)}(d')) = 0.$$

□

Una vez demostrados los dos lemas, vemos qué podemos hacer con los resultados de estos y algunas consecuencias de las definiciones que hemos dado.

Lo primero a notar es que podemos segmentar tanto el conteo de raíces como el número de cambios de signo de P, un polinomio de grado p en una variable en $R[X]$ en un intervalo. La segmentación se hace con una partición de dicho intervalo. Es decir, podemos ver que, claramente, para todo $c \in (a, b)$

$$n(P; (a, b]) = n(P; (a, c]) + n(P; (c, b]) \quad \text{y}$$

$$V(\mathrm{Der}(P); a, b) = V(\mathrm{Der}(P); a, c) + V(\mathrm{Der}(P); c, b)$$

Ahora, sean $c_1 < c_2 < \cdots < c_{r-1} < c_r$ las raíces reales de los polinomios $P^{(j)}, j = 0, 1, \ldots, p-1$ en el intervalo (a, b). Luego, sean $a = c_0, b = c_{r+1}$ y $d_i \in (c_i, c_{i+1})$ de tal manera que $a = c_0 < d_0 < c_1 < d_1 < \cdots < c_r < d_r < c_{r+1} = b$.

Consideremos el intervalo $(d_i, c_{i+1}]$ para alguna $0 \leq i \leq r$. Tenemos entonces que examinar dos casos, uno en el que c_{i+1} es raíz de P y otro en el que es raíz de alguna de sus derivadas (pero no de las anteriores ni de P).

Supongamos que c_{i+1} es raíz de P con multiplicidad μ, entonces podemos usar el Lema 3 para concluir rápidamente que

$$V(P(d_i), P'(d_i), \ldots, P^{(\mu)}(d_i)) - V(P(c_{i+1}), P'(c_{i+1}), \ldots, P^{(\mu)}(c_{i+1})) = \mu.$$

Además, como no hay raíces de $P^{(j)}, j = \mu + 1, \ldots, p-1$ en $[d_i, c_{i+1}]$, tenemos que

$$V(P^{(\mu+1)}(d_i), \ldots, P^{(p-1)}(d_i)) - V(P^{(\mu+1)}(c_{i+1}), \ldots, P^{(p-1)}(c_{i+1})) = 0.$$

Juntando estos dos resultados vemos que

$$V(\mathrm{Der}(P); d_i, c_{i+1}) = \mu,$$

y como la única raíz de P en (d_i, c_{i+1}) es c_{i+1}, con multiplicidad μ, es claro que en este caso,

$$V(\mathrm{Der}(P); d_i, c_{i+1}) - n(P; (d_i, c_{i+1}]) = \mu - \mu = 0.$$

Supongamos ahora que c_{i+1} es raíz de $P^{(k)}$ con multiplicidad μ, y que $P^{(j)} \not\equiv 0$ para $j = 0, 1, \ldots, k-1, k+\mu+1, \ldots, p-1$. Podemos entonces usar el Lema 4 para obtener que

$$V(P^{(k-1)}(d_i), \ldots, P^{(k+\mu)}(d_i)) - V(P^{(k-1)}(c_{i+1}), \ldots, P^{(k+\mu)}(c_{i+1}))$$

es par y no negativo. Por otra parte, como no hay raíces de $P^{(j)}, j = 0, 1, \ldots, k-1, k+\mu+1, \ldots, p-1$ en $[d_i, c_{i+1}]$ vemos que

$$V(P(d_i), \ldots, P^{(k-2)}(d_i)) - V(P(c_{i+1}), \ldots, P^{(k-2)}(c_{i+1})) = 0$$
$$V(P^{(k+\mu+1)}(d_i), \ldots, P^{(p-1)}(d_i)) - V(P^{(k+\mu+1)}(c_{i+1}), \ldots, P^{(p-1)}(c_{i+1})) = 0$$

Además, como, en particular, no hay raíces de P en $[d_i, c_{i+1}]$, sabemos que $n(P; (d_i, c_{i+1}]) = 0$. Juntamos estos resultados y obtenemos que para este caso,

$$V(\mathrm{Der}(P); d_i, c_{i+1}) - n(P; (d_i, c_{i+1}])$$

es par y no negativo.

Con los dos casos anteriores mostramos que para todo $0 \leq i \leq r$,

$$V(\mathrm{Der}(P); d_i, c_{i+1}) - n(P; (d_i, c_{i+1}])$$

es par y no negativo.

Tomamos ahora el intervalo $(c_i, d_i]$ para alguna $0 \leq i \leq r$, podemos seguir un razonamiento muy similar al que usamos para el intervalo $(d_i, c_{i+1}]$. De nuevo tenemos dos casos, aquel en le cual c_i es raíz de P y otro en el que es raíz de alguna de sus derivadas (pero no de las anteriores ni de P).

Supongamos que c_i es raíz de P con multiplicidad μ, entonces podemos usar el Lema 3 para concluir rápidamente que

$$V(P(c_i), P'(c_i), \ldots, P^{(\mu)}(c_i)) - V(P(d_i), P'(d_i), \ldots, P^{(\mu)}(d_i)) = 0.$$

Además, como no hay raíces de $P^{(j)}, j = \mu+1, \ldots, p-1$ en $[c_i, d_i]$, tenemos que

$$V(P^{(\mu+1)}(c_i), \ldots, P^{(p-1)}(c_i)) - V(P^{(\mu+1)}(d_i), \ldots, P^{(p-1)}(d_i)) = 0.$$

Juntando estos dos resultados vemos que

$$V(\mathrm{Der}(P); c_i, d_i) = 0,$$

y como no hay raíz de P en $(c_i, d_i]$, es claro que en este caso,

$$V(\mathrm{Der}(P); c_i, d_i) - n(P; (c_i, d_i]) = 0 - 0 = 0.$$

Supongamos ahora que c_i es raíz de $P^{(k)}$ con multiplicidad μ, y que $P^{(j)} \neq 0$ para $j = 0, 1, \ldots, k-1, k+\mu+1, \ldots, p-1$. Podemos entonces usar el Lema 4 para obtener que

$$V(P^{(k-1)}(c_i), \ldots, P^{(k+\mu)}(c_i)) - V(P^{(k-1)}(d_i), \ldots, P^{(k+\mu)}(d_i)) = 0.$$

Por otra parte, como no hay raíces de $P^{(j)}, j = 0, 1, \ldots, k-1, k+\mu+1, \ldots, p-1$ en $[c_i, d_i]$ vemos que

$$\mathrm{V}(P(c_i), \ldots, P^{(k-2)}(c_i)) - \mathrm{V}(P(d_i), \ldots, P^{(k-2)}(d_i)) = 0$$
$$\mathrm{V}(P^{(k+\mu+1)}(c_i), \ldots, P^{(p-1)}(c_i)) - \mathrm{V}(P^{(k+\mu+1)}(d_i), \ldots, P^{(p-1)}(d_i)) = 0$$

Además, como, en particular, no hay raíces de P en $[c_i, d_i]$, sabemos que $n(P; (c_i, d_i]) = 0$. Juntamos estos resultados y obtenemos que para este caso,

$$\mathrm{V}(\mathrm{Der}(P); c_i, d_i) - n(P; (c_i, d_i]) = 0.$$

Con los dos casos anteriores mostramos que para todo $0 \leq i \leq r$,

$$\mathrm{V}(\mathrm{Der}(P); c_i, d_i) - n(P; (c_i, d_i]) = 0.$$

Ahora, vemos el intervalo entero $(a, b]$. Usando la idea de segmentación por particiones mencionada al principio de esta discusión, junto con los resultados para subintervalos recién expuestos, vemos que

$$\begin{aligned}
\mathrm{V}(\mathrm{Der}(P); a, b) - n(P; (a, b]) &= \sum_{i=0}^{r} (\mathrm{V}(\mathrm{Der}(P); c_i, d_i) + \mathrm{V}(\mathrm{Der}(P); d_i, c_{i+1})) \\
&\quad - \sum_{i=0}^{r} (n(P; (c_i, d_i]) + n(P; (d_i, c_{i+1}])) \\
&= \sum_{i=0}^{r} (\mathrm{V}(\mathrm{Der}(P); c_i, d_i) - n(P; (c_i, d_i]) \\
&\quad + \mathrm{V}(\mathrm{Der}(P); d_i, c_{i+1}) - n(P; (d_i, c_{i+1}])) \\
&= \sum_{i=0}^{r} (\mathrm{V}(\mathrm{Der}(P); d_i, c_{i+1}) - n(P; (d_i, c_{i+1}]))
\end{aligned}$$

que es claramente par y no negativo. Escrito de otra forma, tenemos el

Teorema (Budan-Fourier). *Sea P un polinomio de grado p en una variable en $R[X]$. Dados a y b en $R \cup \{-\infty, \infty\}$*

1. $n(P; (a, b]) \leq \mathrm{V}(\mathrm{Der}(P); a, b)$,
2. $\mathrm{V}(\mathrm{Der}(P); a, b) - n(P; (a, b])$ *es par.*

2.2 La ley de signos de Descartes

Como caso particular del Teorema Budan-Fourier, podemos demostrar fácilmente el resultado encontrado por Descartes hace más de 350 años. Es fundamentalmente más débil que el teorema anterior, pero es de interés y de utilidad en casos sencillos, sobre todo por la facilidad de su aplicación.

Necesitamos primero introducir algo de notación. Sea $P = a_p X^p + a_{p-1} X^{p-1} + \cdots + a_1 X + a_0$ un polinomio en una variable en $R[X]$. Escribimos $V(P)$ para representar el número de cambios de signo de $a_p, a_{p-1}, \ldots, a_0$ y $\text{pos}(P)$ para el número de raíces reales de P contadas con multiplicidad.

Consideramos el intervalo $(0, +\infty)$ y aplicamos Budan-Fourier. Es claro que

$$P(0) = a_0, P'(0) = a_1, \ldots, P^{(p-1)}(0) = a_{p-1}, P^{(p)}(0) = a_p,$$

por lo que

$$V(\text{Der}(P); 0) = V(P).$$

Por otra parte, cuando evaluamos la k-ésima derivada de P, $P^{(k)}, 0 \leq k \leq p$ en $+\infty$, el sumando $p^k a_p X^{p-k}$ es claramente dominante y su signo es $\text{signo}(a_p)$. De aquí que

$$V(\text{Der}(P); +\infty) = 0$$

y por lo tanto

$$V(\text{Der}(P); 0, +\infty) = V(P).$$

Ahora, únicamente hace falta notar que $\text{pos}(P) = n(P; (0, +\infty))$ por definición, para poder presentar la

Ley de signos de Descartes. *Sea $P = a_p X^p + a_{p-1} X^{p-1} + \cdots + a_1 X + a_0$ un polinomio en una variable en $R[X]$, entonces*

1. $\text{pos}(P) \leq V(P)$,
2. $V(P) - \text{pos}(P)$ *es par.*

2.3 Una aplicación y un ejemplo

Para finalizar damos una aplicación muy sencilla del Teorema Budan-Fourier y damos un ejemplo. Ambos pretenden ilustrar la demostración y dar instancias del uso del teorema. Empezamos con la aplicación, que nos da un método fácil para determinar si un polinomio tiene 0, 1 o más raíces en un intervalo dado, aún cuando sólo para algunos casos.

Proposición 8. *Sea P un polinomio de grado p en una variable en $R[X]$.*

1. *Si $V(\mathrm{Der}(P); a, b) = 0$ entonces P no tiene raíz en $(a, b]$.*
2. *Si $V(\mathrm{Der}(P); a, b) = 1$ entonces P tiene exactamente una raíz en $(a, b]$.*

Esta proposición sigue directamente del teorema, pero damos una pequeña demostración ilustrativa.

Demostración.

1. El teorema nos dice que $V(\mathrm{Der}(P); a, b) \geq n(P; (a, b])$, y como $V(\mathrm{Der}(P); a, b) = 0$, $n(P; (a, b]) = 0$. Ie. P no tiene raíz en $(a, b]$.
2. Por otra parte, usando el teorema, $V(\mathrm{Der}(P); a, b) - n(P; (a, b])$ es par y no negativo, pero $V(\mathrm{Der}(P); a, b) = 1$. Por lo tanto, $V(\mathrm{Der}(P); a, b) - n(P; (a, b]) = 0$ y $n(P; (a, b]) = 1$. Ie. P tiene exactamente una raíz en $(a, b]$. □

Con esto en mente, damos un ejemplo para tratar de entender porque la diferencia entre cambios de signo de $\mathrm{Der}(P)$ y el número de raíces es par. Hacemos uso de la aplicación anterior para ver que el teorema puede no decirnos mucho sobre las raíces de un polinomio en un intervalo dado.

Ejemplo. *El polinomio $P = X^2 - X + 1$ no tiene raíz real, pero $V(\mathrm{Der}(P); 0, 1) = 2$. Es imposible encontrar $a \in (0, 1]$ tal que $V(\mathrm{Der}(P); 0, a) = 1$ y $V(\mathrm{Der}(P); a, 1) = 1$ dado que de otra manera habrían dos raíces reales. Esto quiere decir que no importa de que manera refinemos el intervalo $(0, 1]$, quedaremos con un intervalo (aquel que contenga $1/2$) que nos de 2 cambios de signo.*

Podemos fácilmente factorizar P como

$$P = \left(X - \frac{1 + i\sqrt{3}}{2}\right)\left(X - \frac{1 - i\sqrt{3}}{2}\right),$$

por lo que vemos que no tiene raíces reales. En particular, P no tiene raíces reales en el intervalo $(0, 1]$.

Por otra parte, $V(\mathrm{Der}(P); 0, 1) = 2$. Para ver esto, usamos que

$$\begin{array}{lll} P = X^2 - X + 1 & P(0) = 1 & P(1) = 1 \\ P' = 2X - 1 & P'(0) = -1 & P(1) = 1 \\ P'' = 2 & P''(0) = 2 & P''(1) = 2 \end{array}$$

para generar la tabla

	0	1
signo(P)	+	+
signo(P')	−	+
signo(P'')	+	+

y concluir que

$$V(\mathrm{Der}(P); 0, 1) = V(\mathrm{Der}(P); 0) - V(\mathrm{Der}(P); 1) = 2 - 0 = 2.$$

Ahora, supongamos que existe $a \in (0, 1]$ tal que $V(\mathrm{Der}(P); 0, a) = 1$ y $V(\mathrm{Der}(P); a, 1) = 1$. La Proposición 8 nos dice entonces que existen $r \in (0, a]$ y $r' \in (a, 1]$ tales que $P(r) = P(r') = 0$. Pero esto es una contradicción dado que P no tiene raíces reales. Tenemos entonces que para cualquier partición de $(0, 1]$ que hagamos, tendremos un intervalo $(c, c']$ tal que $V(\mathrm{Der}(P); c, c') = 2$.

Sea $(c, c'] \subset (0, 1]$ tal que $V(\mathrm{Der}(P); c, c') = 2$. Aseveramos que $1/2 \in (c, c']$. Tenemos entonces dos casos, $1/2 < c$ o $c' < 1/2$. Notamos primero que $1/2$ es raíz de P', que es lineal, por lo que $P' \leq 0 \in (0, 1/2]$ y $P' > 0 \in (1/2, 1]$. Tenemos entonces las tablas:

$1/2 < c$	c	c'
signo(P)	+	+
signo(P')	+	+
signo(P'')	+	+

y

$c' < 1/2$	c	c'
signo(P)	+	+
signo(P')	−	−
signo(P'')	+	+

por lo que en estos casos

$$V(\mathrm{Der}(P); c, c') = 0 - 0 = 0 \quad \text{y} \quad V(\mathrm{Der}(P); c, c') = 2 - 2 = 0.$$

Por lo tanto, $1/2 \in (c, c']$.

Notamos finalmente que $1/2$ es un mínimo local positivo de P (es raíz de P'), lo que nos da las variaciones de signo.