UNIVERSIDAD DE EL SALVADOR

FACULTAD DE CIENCIAS NATURALES Y MATEMÁTICA

ESCUELA DE MATEMÁTICA

PROYECTO DE GRADO TITULADO:

"Teoría Analítica y Algebraica de Polinomios"

PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

LICENCIADO EN MATEMÁTICA

Estudiantes: Cidia Lorena Cruz. *Carné:* CC07138

Saúl Edgardo Chinco Aguilar. *Carné:* CA08062

Asesores: Lic. Claudia Patricia Corcio.

Lic. José Daniel Siciliano Álvarez

Ciudad Universitaria, viernes 16 de octubre de 2015

Dedicatoria

A nuestros padres, Francisca, María, Miriam y Jobel.

por su incondicional apoyo, amor y comprensión.

.

Agradecimientos

A Dios, porque nos ha brindado vida, sabiduria y fuerzas para terminar nuestros estudios superiores.

A nuestros padres, por ser nuestro ejemplo de esfuerzo y dedicación y por animarnos a conseguir nuestras metas.

A nuestros asesores, Licda. Claudia Patricia Corcio y Lic. José Daniel Siciliano, por su paciencia y por colaborar en cada aspecto de este trabajo.

A nuestro jurado, MSc. Ingrid Carolina Martínez Barahona y Lic. Yoseman Adony Rivas, por su dedicación, revisiones y correcciones de este trabajo.

A mi esposo, José Luis Teodoro Morales, por su apoyo y amor incondicional.

A nuestros amigos y hermanos(as), Lenny, Jackeline, Ofelia, Margarita, Maricela, Abraham, Mayra, Henry, Mynor, Cecy, Xiomara, Elida, Dianita, Carlos Gamez, Marcela, Yeris, Nancy, Yohana, Yansy y Omar, por apoyarnos y regalarnos una amistad sincera.

Índice general

Introducción

Este trabajo de investigación contiene una exposición de los principales resultados de la teoría de los polinomios, tanto clásicas como modernas. La teoría de Galois se discute principalmente desde el punto de vista de la teoría de polinomios, no de la de la teoría general de campos y sus extensiones. Más precisamente:

En el **capítulo 1** se discute, sobre todo, los teoremas clásicos de la distribución de las raíces de un polinomio y de su derivada. También se muestra cómo determinar el número de raíces reales de un polinomio real, y cómo separarlos.

El **capítulo 2** trata de criterios irreducibilidad de polinomios con coeficientes enteros, entre los cuales se encuentran: El criterio de Eisenstein, El criterio de Perrón y otros.

En el **capítulo 3** introduciremos y estudiaremos algunas clases especiales de polinomios: simétrico (polinomios que son invariables cuando se permutan las indeterminadas), valor entero (polinomios que alcanzan valores enteros en todos los puntos enteros), ciclotómicos (polinomios con todas las raíces n-ésimas primitivas de la unidad como raíces), y algunas clases polinomios interesantes introducidas por Chebyshev.

El **capítulo 4** está dedicado a la teoría de Galois clásica. Es bien sabido que las raíces de una ecuación polinómica de grado como máximo cuatro en una variable pueden expresarse en términos de los radicales de expresiones aritméticas de sus coeficientes. Una aplicación principal de la teoría de Galois es que esto no es posible en general para ecuaciones de grado cinco o más.

En el **capítulo 5** se estudiarán tres teoremas clásicos de Hilbert.

Capítulo 1

Raíces de Polinomios

En este capítulo estudiaremos, el teorema fundamental del álgebra que, aunque este enunciado, en principio, parece ser una declaración débil, implica que todo polinomio de grado n de una variable con grado mayor que cero con coeficientes complejos tiene, contando las multiplicidades, exactamente n raíces complejas, para tal demostración se utilizará el teorema de Rouché.

Aquí se discute el teorema de Cauchy de las raíces de los polinomios, así como sus corolarios y generalizaciones. Y los teoremas de Laguerre que son de importancia en variable compleja y el análisis.

Además, se estudiará el teorema de Gauss que nos permite relacionar las raíces de un polinomio y hace también una relación geométrica de los ceros de un polinomio de tercer grado con coeficientes complejos y los ceros de su derivada.

1.1. Desigualdades para las raíces

1.1.1 El Teorema Fundamental del Álgebra.

***Teorema* 1.1 (Rouché).** Sean f y g polinomios y γ una curva cerrada sin que esta se intersecte en el plano complejo. Si

$$|f(z) - g(z)| < |f(z)| + |g(z)| \qquad (1)$$

para todo $z \in \gamma$, entonces en el interior de γ hay un número igual de raíces de f y g.

Demostración. En el plano complejo, consideremos los campos vectoriales

$$v(z) = f(z) \ y \ w(z) = g(z).$$

A partir de (1) se deduce que en ningún punto de γ los vectores v y w tienen direcciones opuestas entre sí. Recordemos que el índice de la curva γ, con respecto a un campo vectorial v es el número de revoluciones del vector $v(z)$ ya que se ajusta por completo la curva γ. Consideremos el campo vectorial

$$v_t = tv + (1-t)w.$$

Entonces $v_0 = w$ y $v_1 = v$. También es claro que en cada punto $z \in \gamma$ el vector $v_t(z)$ es distinto de cero. Esto significa que el índice $ind(t)$ de γ con respecto al campo vectorial v_t está bien definido. El $ind(t)$ depende continuamente de t, y por lo tanto $ind(t) = const$. En particular, los índices de γ con respecto a los campos vectoriales v y w coinciden.

Se define el índice de un punto singular z_0 como el índice de la curva $|z - z_0| = \varepsilon$, donde ε es suficientemente pequeño.

Pero el índice de γ con respecto a un campo vectorial v es igual a la suma de los índices de puntos singulares, es decir aquellos en los que $v(z) = 0$. Para el campo vectorial $v(z) = f(z)$, el índice del punto singular z_0 es igual a la multiplicidad de la raíz z_0 de f. Por lo tanto la coincidencia de los índices de γ con respecto a los campos de vectores $v(z) = f(z)$ y $w(z) = g(z)$ implica que, dentro de la curva γ el número de raíces de f es igual a las de g. □

Teorema 1.2. Sea $f(z) = z^n + a_1 z^{n-1} + \cdots + a_n$, con $a_i \in \mathbb{C}$. Entonces dentro del círculo $|z| = 1 + max\,|a_i|$ hay exactamente n raíces de f (contando multiplicidad).

Demostración. Sea $a = max\,|a_i|$, dentro del círculo consideramos el polinomio $g(z) = z^n$ que tiene una raíz $z_0 = 0$, de multiplicidad n. Entonces es suficiente verificar que si $|z| = 1 + a$ entonces $|f(z) - g(z)| < |f(z)| + |g(z)|$. Vamos a probar que incluso $|f(z) - g(z)| < |g(z)|$.

En efecto, si $|z| = 1 + a$ entonces:

$$\begin{aligned} |f(z) - g(z)| &= |a_1 z^{n-1} + \cdots + a_n| \leq a_1 |z|^{n-1} + \cdots |z| + a_n \leq a(|z|^{n-1} + \cdots |z| + 1) \\ &= a\left(\frac{|z|^n - 1}{|z| - 1}\right) \end{aligned}$$

como $|z| - 1 = a$, entonces $|f(z) - g(z)| \leq |z|^n - 1 < |z|^n$,

es decir que $|f(z) - g(z)| < |g(z)|$. Aplicando el teorema de Rouché f tiene exactamente n raíces. □

Se estudiará el teorema de Cauchy de las raíces de los polinomios, así como sus corolarios y generalizaciones.

1.1.2 Teorema de Cauchy.

Teorema 1.3 (Cauchy). Sea $f(x) = x^n - b_1x^{n-1} - \cdots - b_n$, donde todos los b_i son no negativos y al menos uno de ellos es distinto de cero. El polinomio f tiene una única raíz (simple) positiva p y el valor absoluto de las otras no exceden a p.

Demostración. Recordemos que, si $f'(x) > 0$, f es creciente; o si $f'(x) < 0$, f es decreciente. Además p es una raíz simple de f si y sólo si $f'(p) \neq 0$.

" $\Longrightarrow$ " Si p es una raíz simple de f entonces $f'(p) \neq 0$.

Sea el polinomio $f(x) = (x-p)g(x)$ luego al derivar el polinomio con respecto a x, tenemos que $f'(x) = g(x) + (x-p)g'(x)$ si evaluamos en p obtenemos que: $f'(p) = g(p)$ analizamos que sí $g(p) = 0$ entonces significa que p es una raíz de g entonces podríamos escribir a g como un polinomio $g(x) = (x-p)h(x)$ pero si fuese así, p no sería raíz simple, por lo que $g(p) \neq 0$ y entonces $f'(p) \neq 0$.

" $\Longleftarrow$ " Si $f'(p) \neq 0$ y del polinomio $f(x) = (x-p)g(x)$ al derivarlo con respecto a x, obtenemos $f'(x) = g(x) + (x-p)g'(x)$ y luego al evaluarlo en p tenemos que

$f'(p) = g(p) \neq 0$ entonces el polinomio g no se puede representar como

$$g(x) = (x-p)h(x),$$

así p es una raíz simple.

Consideremos $F(x) = -\dfrac{f(x)}{x^n} = \dfrac{b_1}{x} + \cdots + \dfrac{b_n}{x^n} - 1$.

Notemos que si $x \neq 0$, la ecuación $f(x) = 0 \Longleftrightarrow F(x) = 0$.

Se estudiará el polinomio F, que en este caso f tendrá propiedades similares.

Para $x > 0$, $\underset{x\to 0^+}{Lim} F(x) = \infty$ y $\underset{x\to\infty}{Lim} F(x) = -1$ entonces F se anula en un punto p. Entonces:

$$F'(x) = -\left(\frac{f'(x)x^n - nx^{n-1}f(x)}{x^{2n}}\right) = -\frac{b_1}{x^2} - \frac{2b_2}{x^3} \cdots - \frac{nb_n}{x^{n+1}} < 0,$$

es decir $F'(x) \neq 0$.

En particular para $x = p$

$$F'(p) = -\left(\frac{f'(p)p^n - np^{n-1}f(p)}{p^{2n}}\right) = -\frac{f'(p)}{p^n} = -\frac{b_1}{p^2} - \frac{2b_2}{p^3} \cdots - \frac{nb_n}{p^{n+1}} < 0.$$

Por lo tanto $F'(p) \neq 0$, es decir p es simple y única.

Queda por demostrar que si x_0 es una raíz de f, entonces $q = |x_0| \leq p$

Supongamos que $p < q$. Notemos que para $x > 0$, $F(x) = -\dfrac{f(x)}{x^n}$ es monótona decreciente, entonces f es monótona creciente.

Entonces, $f(q) > f(p) = 0$, es decir que $f(q) > 0$. Por otra parte, de la igualdad $f(x_0) = 0$ tenemos:

$x_0^n = b_1 x_0^{n-1} + \cdots + b_n$, formamos:

$$\begin{aligned} |x_0|^n &= \left|b_1 x_0^{n-1} + \cdots + b_n\right| \\ &\leq b_1 |x_0|^{n-1} + \cdots + |b_n| \end{aligned}$$

Así tendríamos que $|x_0|^n - b_1 |x_0|^{n-1} - \cdots - |b_n| \leq 0$ entonces $F(|x_0|) = f(q) \leq 0$ y esto es una contradicción ya que $f(q)>0$, por lo tanto $q \leq p$. □

Teorema 1.4. (*Ostrovsky*)**.** Sea $f(x) = x^n - b_1 x^{n-1} - \cdots - b_n$, donde todos los números b_i son no negativos y al menos uno de ellos es diferente de cero. Si el *mcd* de los índices de los coeficientes b_i es igual a 1, entonces f tiene una única raíz positiva p y el valor absoluto de las otras raíces son menores que p.

Demostración. Por el teorema de Cauchy existe una única raíz p positiva, además las otras raíces de f son negativas o cero.

Sean $b_{k_1}, b_{k_2}, \ldots, b_{k_m}$ los coeficientes positivos, donde $k_1 < k_2 < \cdots < k_m$. Ya que el *mcd* de $k_1, k_2, \ldots, k_m$ es 1, entonces existen enteros $s_1, s_2, \ldots, s_m$ tal que

$$s_1 k_1 + s_2 k_2 + \cdots + s_m k_m = 1.$$

Se considera la función

$$F(x) = \frac{b_{k_1}}{x^{k_1}} + \cdots + \frac{b_{k_m}}{x^{k_m}} - 1$$

la cual tiene una única solución positiva p.

Supongamos que x_0 es otra raíz de f. Consideremos entonces a

$$F(x_0) = \frac{b_{k_1}}{x_0^{k_1}} + \cdots + \frac{b_{k_m}}{x_0^{k_m}} - 1 = 0$$

de la cual se obtiene la desigualdad

$$1 = \frac{b_{k_1}}{x_0^{k_1}} + \cdots + \frac{b_{k_m}}{x_0^{k_m}} \leq \frac{b_{k_1}}{|\, x_0 \,|^{k_1}} + \cdots + \frac{b_{k_m}}{|\, x_0 \,|^{k_m}}$$

Sea $\mid x_0 \mid = q$, entonces,

$$0 \leq F(q) = \frac{b_{k_1}}{q^{k_1}} + \cdots + \frac{b_{k_m}}{q^{k_m}} - 1$$

Por lo que $F(q) = 0$ o $F(q) > 0$. Suponiendo que $F(q) = 0$, entonces

$$\frac{b_{k_i}}{x_0^{k_i}} = \mid \frac{b_{k_i}}{x_0^{k_i}} \mid > 0, \qquad \forall i$$

pero en este caso

$$\frac{b_{k_1}^{s_1}.b_{k_2}^{s_2}\ldots b_{k_m}^{s_m}}{x_0} = \frac{b_{k_1}^{s_1}.b_{k_2}^{s_2}\ldots b_{k_m}^{s_m}}{x_0^{s_1k_1+s_2k_2+\cdots+s_mk_m}} = \left(\frac{b_{k_1}}{x_0^{k_1}}\right)^{s_1} \cdot \left(\frac{b_{k_2}}{x_0^{k_2}}\right)^{s_2} \cdots \left(\frac{b_{k_m}}{x_0^{k_m}}\right)^{s_m} > 0$$

esto implicaría que $x_0 > 0$, lo que genera una contradicción, ya que solo existe una única raíz positiva p por el teorema de Cauchy

Ahora si $F(x) > 0$, entonces

$$0 = F(p) < F(q)$$

así $q < p$, porque estamos analizando una función F monótona decreciente, es decir $\mid x_0 \mid < p$

□

Ejemplo 1.1. Sea el polinomio

$P(x) = x^3 - x^2 - 3x - 4$ así los coeficientes del polinomio P serían los siguientes:

$a_1 = -1$, $a_2 = -3$, $a_3 = -4$ entonces $mcd(1, 2, 3) = 1$ y tiene la raíz positiva es $p = 2.55$ y las otras no exceden a p.

Teorema 1.5 ($Eneström - Kakeya$)**.** Si todos los coeficientes del polinomio

$$g(x) = a_0x^{n-1} + \ldots + a_{n-1}$$

son positivos, entonces, cualquier raíz ε de este polinomio cumple:

$$\min_{1\leq i\leq n-1}\left\{\frac{a_i}{a_{i-1}}\right\} = \delta \leq \mid \varepsilon \mid \leq \gamma = \max_{1\leq i\leq n-1}\left\{\frac{a_i}{a_{i-1}}\right\}$$

Demostración. Considerar el polinomio

$$\begin{aligned}(x-\gamma)\,g(x) &= a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x - \gamma a_0x^{n-1} - \cdots \gamma a_{n-2}x - \gamma a_{n-1} \\ &= a_0x^n + a_1x^{n-1} - \gamma a_0x^{n-1} + .. \cdots + a_{n-1}x - \gamma a_{n-2}x - \gamma a_{n-1} \\ &= a_0x^n - (\gamma a_0 - a_1)\,x^{n-1} - \cdots - (\gamma a_{n-2} - a_{n-1})\,x - \gamma a_{n-1}\end{aligned}$$

Ahora por definición se tiene que:

$$\gamma \geq \frac{a_i}{a_{i-1}}$$

entonces

$$\gamma a_{i-1} - a_i \geq 0$$

Ya que $\gamma a_{n-1} > 0$ se puede aplicar el teorema de Cauchy al polinomio $(x-\gamma)\,g(x)$, así existe una única raíz positiva tal que:

$$\mid \varepsilon \mid \leq \gamma$$

Suponiendo que $\varepsilon = 0$ el teorema se cumple, por lo que podemos suponer $\varepsilon \neq 0$. Como ε es una raíz de $g(x)$, entonces

$$\begin{aligned}a_0\varepsilon^{n-1} + \cdots + a_{n-1} &= 0 \\ a_0 + \cdots + \frac{a_{n-1}}{\varepsilon^{n-1}} &= 0\end{aligned}$$

así $\eta = \frac{1}{\varepsilon}$ es raíz del polinomio

$$f(y) = a_0 + \cdots + a_{n-1}y^{n-1}$$

por lo que

$$\mid \eta \mid = \frac{1}{\mid \varepsilon \mid} \leq \underset{1\leq i\leq n-1}{max}\left\{\frac{a_{i-1}}{ai}\right\} = \frac{1}{\underset{1\leq i\leq n-1}{min}\left\{\frac{a_i}{a_{i-1}}\right\}}$$

entonces

$$\underset{1\leq i\leq n-1}{min}\left\{\frac{a_i}{a_{i-1}}\right\} \leq \varepsilon$$

□

Ejemplo 1.2. Sea el polinomio

$p(x) = x^5 + 15x^4 + 85x^3 + 225x^2 + 274x + 120$

Las raíces del polinomio son -1, -2, -3, -4, -5 y luego encontrar el mínimo valor y el máximo valor de la división de los coeficientes según el teorema,

$$\frac{a_1}{a_0} = \frac{15}{1} = 15, \quad \frac{a_2}{a_1} = \frac{85}{15} = 5.6, \quad \frac{a_3}{a_2} = \frac{225}{85} = 2.7, \quad \frac{a_4}{a_3} = \frac{274}{225} = 3.2, \quad \frac{a_5}{a_4} = \frac{120}{274} = 0.4$$

entonces el valor máximo sería $\gamma = \underset{1\leq i\leq n-1}{max}\left\{\frac{a_i}{a_{i-1}}\right\} = 15$ y el mínimo valor sería $\delta = \underset{1\leq i\leq n-1}{min}\left\{\frac{a_i}{a_{i-1}}\right\} = 0.4$

Así el valor absoluto de cualquiera de las raíces del polinomio p están en $[\delta, \gamma]$.

1.1.3 Teorema de Laguerre.

Sea $z_1, z_2, \ldots, z_n \in \mathbb{C}$ puntos con masa unitaria. El punto $\xi = \frac{1}{n}(z_1 + \cdots + z_n)$ es llamado el centro de masa de $z_1, z_2, \ldots, z_n$.

Este concepto se puede generalizar de la siguiente forma. Realizar una transformación lineal fraccional w, que envíe a z_0 a ∞; es decir:

$$w(z) = \frac{a}{z - z_0} + b$$

Se encontrará el centro de masa de las imágenes y luego aplicar la transformación inversa w^{-1}. Mostraremos que el resultado no depende de a y b.

Recordemos que $w(z)$ es un mapeo biyectivo y conforme ($w'(z) \neq 0$), por eso un punto en las imágenes le corresponde un punto en las preimágenes, es decir al centro de masa de las imágenes de $z_1, z_2, \ldots, z_n$ le corresponde el centro de masa de $z_1, z_2, \ldots, z_n$.

Sea

$$\xi = \frac{1}{n}(w(z_1) + \cdots + w(z_n)),$$

entonces

$$\xi = \frac{1}{n}(\frac{a}{z_1 - z_0} + b + \frac{a}{z_2 - z_0} + b + \cdots + \frac{a}{z_n - z_0} + b)$$

$$\Rightarrow \xi = \frac{a}{n}(\frac{1}{z_1 - z_0} + \frac{1}{z_2 - z_0} + \cdots + \frac{1}{z_n - z_0}) + b$$

Aplicando $w^{-1}(z)$ a ξ, donde $w^{-1}(z) = \frac{a}{z - b} + z_0$, tenemos que:

$$w^{-1}(\xi) = \frac{a}{\xi - b} + z_0 = \frac{a}{\frac{a}{n}(\frac{1}{z_1 - z_0} + \frac{1}{z_2 - z_0} + \cdots + \frac{1}{z_n - z_0}) + b - b} + z_0$$

$$w^{-1}(\xi) = z_0 + n\frac{1}{\frac{1}{z_1 - z_0} + \frac{1}{z_2 - z_0} + \cdots + \frac{1}{z_n - z_0}},$$

que es el resultado que buscamos.

Llamaremos centro de masa de $z_1, z_2, \ldots, z_n$ con respecto a z_0 al punto:

$$\xi_{z_0} = z_0 + n\frac{1}{\frac{1}{z_1 - z_0} + \frac{1}{z_2 - z_0} + \cdots + \frac{1}{z_n - z_0}} \qquad (2)$$

Es claro que el centro de masa de $z_1, z_2, \ldots, z_n$ se encuentra en el interior de la cobertura convexa.

Esto, generaliza fácilmente al caso del centro de masa con respecto a z_0. Sólo hay que sustituir las líneas que conectan los puntos z_i y z_j, por círculos que pasan a través de z_i, z_j y z_0, donde el punto z_0 correspondiente a ∞ se encuentra fuera de la cobertura convexa.

Teorema 1.6. Sea $f(z) = (z - z_1)\cdots(z - z_n)$. Entonces el centro de masa de las raíces de f con respecto a un punto arbitrario z esta dado por

$$\xi_z = z - n\frac{f(z)}{f'(z)}. \qquad (3)$$

Demostración. Aplicando logaritmo, tenemos

$$log(f(z)) = log(z - z_1) + \cdots + log(z - z_n) \qquad (4)$$

entonces de la parte derecha de la igualdad (4) tenemos

$$log'(f(z)) = \frac{1}{z - z_1} + \cdots + \frac{1}{z - z_n},$$

y de la parte izquierda de la igualdad (4) tenemos

$$log'(f(z)) = \frac{f'(z)}{f(z)},$$

por lo tanto:

$$\frac{f'(z)}{f(z)} = \frac{1}{z-z_1} + \cdots + \frac{1}{z-z_n} \Rightarrow \frac{f(z)}{f'(z)} = \frac{1}{\frac{1}{z-z_1} + \cdots + \frac{1}{z-z_n}}$$

Sustituyendo en la fórmula (2): $\xi_z = z - n\frac{f(z)}{f'(z)}$. □

Teorema 1.7. Sea $f(z)$ un polinomio de grado n y x una raíz simple. Entonces el centro de masa de las otras raíces de $f(z)$ con respecto a x es el punto

$$X = x - 2(n-1)\frac{f'(x)}{f''(x)}.$$

Demostración. Como x es una raíz simple de f, entonces $f(z) = (z-x)F(z)$. La idea es aplicar el teorema anterior.

Entonces

$$f'(z) = F(z) + (z-x)F'(z)$$

y

$$f''(z) = F'(z) + F'(z) + (z-x)F''(z) = 2F'(z) + (z-x)F''(z).$$

Por lo tanto,

$$f'(x) = F(z) \text{ y } f''(x) = 2F'(x)$$

Aplicando la fórmula (3) para el polinomio F de grado $n-1$.

Tenemos el resultado, $X = x - 2(n-1)\frac{f'(x)}{f''(x)}$. □

Teorema 1.8 (*Laguerre*). Sea $f(z)$ un polinomio de grado n y

$$X(z) = z - 2(n-1)\frac{f'(z)}{f''(z)}.$$

Sea el círculo (ó linea) C que pasa a través de una raíz simple z_1 de $f(z)$ y las otras raíces de f pertenecen a uno de los dominios en el que C divide al plano. Entonces $X(z_1)$ también pertenece al mismo dominio.

Demostración. En el centro de masa, el círculo C corresponde a la línea, de manera que todas las raíces de f, excepto z_1, se encuentra a un lado de ella. El centro de

masa de estas raíces se encuentra en el mismo lado de ésta línea. Como aplicamos la transformación fraccional, estas lineas se transforman en círculos. □

Corolario 1.1. Sea z_1 una de las raíces simples de f con el valor absoluto máximo. Entonces

$$|X(z_1)| \leq |z_1|$$

es decir,

$$\left| z_1 - 2(n-1)\frac{f'(z_1)}{f''(z_1)} \right| \leq |z_1|$$

Demostración. Como $|z_1|$ es máximo de f, sea el disco $D = \{z \in \mathbb{C} / \, |z| \leq |z_1|\}$. Todas las raíces de f están en D, por lo tanto, aplicando el teorema anterior $X(z_1)$ pertenece al disco, es decir $|X(z_1)| \leq |z_1|$.

□

1.1.4 Polinomio Apolar.

Sea $f(z)$ un polinomio de grado n y ζ un número fijo o ∞. La función

$$A_\zeta f(z) = \begin{cases} (\zeta - z) f'(z) + n f(z) & \zeta \neq \infty \\ f'(z) & \zeta = \infty \end{cases}$$

es llamada la derivada de $f(z)$ con respecto al punto ζ. Notemos que si

$$f(z) = \sum_{k=0}^{n} \binom{n}{k} a_k z^k \qquad (5)$$

entonces $f'(z)$ la podemos calcular de la siguiente manera:
El $k-ésimo$ término de $f'(z)$ será

$$\begin{aligned} \frac{d}{dz}\left(\binom{n}{k+1} a_{k+1} z^{k+1} \right) &= \binom{n}{k+1} a_{k+1} (k+1) z^k \\ &= \frac{n!}{(n-k-1)!\,(k+1)!} a_{k+1} (k+1) z^k \\ &= n \frac{(n-1)!}{(n-k-1)!k!} a_{k+1} z^k \\ &= n \binom{n-1}{k} a_{k+1} z^k \end{aligned}$$

Así

$$f'(z) = \sum_{k=0}^{n-1} n \left(\begin{array}{c} n-1 \\ k \end{array} \right) a_{k+1} z^k$$

Ahora si $\zeta \neq \infty$

$$\begin{aligned} A_\zeta f(z) &= (\zeta - z) f'(z) + n f(z) \\ &= (\zeta - z) n \sum_{k=0}^{n-1} \left(\begin{array}{c} n-1 \\ k \end{array} \right) a_{k+1} z^k + n \sum_{k=0}^{n} \left(\begin{array}{c} n \\ k \end{array} \right) a_k z^k \end{aligned}$$

Así

$$\begin{aligned} \frac{1}{n} A_\zeta f(z) &= (\zeta - z) \sum_{k=0}^{n-1} \left(\begin{array}{c} n-1 \\ k \end{array} \right) a_{k+1} z^k + \sum_{k=0}^{n} \left(\begin{array}{c} n \\ k \end{array} \right) a_k z^k \\ &= \sum_{k=0}^{n-1} \left(\begin{array}{c} n-1 \\ k \end{array} \right) a_{k+1} \zeta z^k - \sum_{k=0}^{n-1} \left(\begin{array}{c} n-1 \\ k \end{array} \right) a_{k+1} z^{k+1} + \sum_{k=0}^{n} \left(\begin{array}{c} n \\ k \end{array} \right) a_k z^k \\ &= \sum_{k=0}^{n-1} \left(\begin{array}{c} n-1 \\ k \end{array} \right) a_{k+1} \zeta z^k - \sum_{k=1}^{n} \left(\begin{array}{c} n-1 \\ k-1 \end{array} \right) a_k z^k + \sum_{k=0}^{n} \left(\begin{array}{c} n \\ k \end{array} \right) a_k z^k \end{aligned}$$

$$\begin{aligned} &= \sum_{k=1}^{n-1} \left(\begin{array}{c} n-1 \\ k \end{array} \right) a_{k+1} \zeta z^k - \sum_{k=1}^{n-1} \left(\begin{array}{c} n-1 \\ k-1 \end{array} \right) a_k z^k + \sum_{k=1}^{n-1} \left(\begin{array}{c} n \\ k \end{array} \right) a_k z^k \\ &\quad + \left(\begin{array}{c} n-1 \\ 0 \end{array} \right) a_1 \zeta + \left(\begin{array}{c} n \\ 0 \end{array} \right) a_0 \\ &= \sum_{k=1}^{n-1} \left[\left(\begin{array}{c} n-1 \\ k \end{array} \right) a_{k+1} \zeta + \left(\left(\begin{array}{c} n \\ k \end{array} \right) - \left(\begin{array}{c} n-1 \\ k-1 \end{array} \right) \right) a_k \right] z^k \\ &\quad + \left(\begin{array}{c} n-1 \\ 0 \end{array} \right) a_1 \zeta + \left(\begin{array}{c} n \\ 0 \end{array} \right) a_0 \end{aligned}$$

Ocupando la identidad

$$\left(\begin{array}{c} n \\ k \end{array} \right) - \left(\begin{array}{c} n-1 \\ k-1 \end{array} \right) = \left(\begin{array}{c} n-1 \\ k \end{array} \right)$$

se obtiene que

$$\frac{1}{n} A_\zeta f(z) = \sum_{k=1}^{n-1} \left(\begin{array}{c} n-1 \\ k \end{array} \right) (a_k + a_{k+1} \zeta) z^k \qquad (6)$$

Sean $z_1, \ldots, z_n$ las raíces del polinomio (5) y $\zeta_1, \ldots, \zeta_n$ las raíces del polinomio

$$g(z)=\sum_{k=0}^{n}\left(\begin{array}{c} n \\ k \end{array}\right) b_k z^k$$

La fórmula (6) implica que

$$\frac{1}{n}A_{\zeta_n}f(z)=\sum_{k=1}^{n-1}\left(\begin{array}{c} n-1 \\ k \end{array}\right)\left(a_k+a_{k+1}\zeta_n\right)z^k$$

Derivando el polinomio $\frac{1}{n}A_{\zeta_n}f(z)$ con respecto a ζ_{n-1} obtenemos que:

$$\begin{aligned}\frac{1}{n-1}\frac{1}{n}A_{\zeta_{n-1}}A_{\zeta_n}f(z) &= \sum_{k=1}^{n-2}\left(\begin{array}{c} n-2 \\ k \end{array}\right)\left(a_k+a_{k+1}\zeta_n+\left(a_{k+1}+a_{k+2}\zeta_n\right)\zeta_{n-1}\right)z^k \\ &= \sum_{k=1}^{n-2}\left(\begin{array}{c} n-2 \\ k \end{array}\right)\left(a_k+a_{k+1}\left(\zeta_n+\zeta_{n-1}\right)+a_{k+2}\zeta_n\zeta_{n-1}\right)z^k\end{aligned}$$

Derivando el polinomio $\frac{1}{n-1}\frac{1}{n}A_{\zeta_{n-1}}A_{\zeta_n}f(z)$ con respecto a ζ_{n-2} obtenemos que:

$$\begin{aligned}\frac{1}{n-2}\frac{1}{n-1}\frac{1}{n}A_{\zeta_{n-2}}A_{\zeta_{n-1}}A_{\zeta_n}f(z) &= \sum_{k=0}^{n-3}\left(\begin{array}{c} n-3 \\ k \end{array}\right)\left(a_k+a_{k+1}\left(\zeta_n+\zeta_{n-1}\right)+a_{k+2}\zeta_n\zeta_{n-1}\right. \\ &\quad \left.+\left(a_{k+1}+a_{k+2}\left(\zeta_n+\zeta_{n-1}\right)+a_{k+3}\zeta_n\zeta_{n-1}\right)\zeta_{n-2}\right)z^k \\ &= \sum_{k=0}^{n-3}\left(\begin{array}{c} n-3 \\ k \end{array}\right)\left(a_k+a_{k+1}\left(\zeta_n+\zeta_{n-1}+\zeta_{n-2}\right)\right. \\ &\quad +a_{k+2}\left(\zeta_n\zeta_{n-1}+\zeta_n\zeta_{n-2}+\zeta_{n-1}\zeta_{n-2}\right) \\ &\quad \left.+a_{k+3}\zeta_n\zeta_{n-1}\zeta_{n-2}\right)z^k\end{aligned}$$

En general si se sigue derivando hasta llegar al polinomio constante tendremos que:

$$\frac{1}{n!}A_{\zeta_1}A_{\zeta_2}\ldots A_{\zeta_n}f(z)=a_0+a_1\sigma_1+\cdots+a_n\sigma_n$$

Donde

$$\begin{aligned}\sigma_1 &= \zeta_1+\zeta_2+\cdots+\zeta_n = -\left(\begin{array}{c} n \\ 1 \end{array}\right)\frac{b_{n-1}}{b_n} \\ \sigma_2 &= \zeta_1\zeta_2+\cdots+\zeta_{n-1}\zeta_n = \left(\begin{array}{c} n \\ 2 \end{array}\right)\frac{b_{n-2}}{b_n} \\ &\vdots \\ \sigma_n &= \zeta_1\zeta_2\cdots\zeta_n = (-1)^n\left(\begin{array}{c} n \\ n \end{array}\right)\frac{b_0}{b_n}\end{aligned}$$

Además la igualdad

$$\frac{1}{n!}A_{\zeta_1}A_{\zeta_2}\ldots A_{\zeta_n}f\left(z\right)=0$$

es equivalente a

$$a_0+a_1\left(-1\right)\left(\begin{array}{c} n \\ 1 \end{array}\right)\frac{b_{n-1}}{b_n}+a_2\left(\begin{array}{c} n \\ 2 \end{array}\right)\frac{b_{n-2}}{b_n}+\cdots+a_n\left(-1\right)^n\left(\begin{array}{c} n \\ n \end{array}\right)\frac{b_0}{b_n}=0$$

es decir,

$$a_0b_n+a_1b_{n-1}\left(-1\right)\left(\begin{array}{c} n \\ 1 \end{array}\right)+a_2b_{n-2}\left(\begin{array}{c} n \\ 2 \end{array}\right)+\cdots+a_nb_0\left(-1\right)^n\left(\begin{array}{c} n \\ n \end{array}\right)=0$$

Definición 1.1. Dos polinomios de la forma

$$\frac{1}{n}A_\zeta f\left(z\right)=\sum_{k=1}^{n-1}\left(\begin{array}{c} n-1 \\ k \end{array}\right)\left(a_k+a_{k+1}\zeta\right)z^k$$

y

$$g\left(z\right)=\sum_{k=0}^{n}\left(\begin{array}{c} n \\ k \end{array}\right)b_kz^k$$

tales que satisfacen la siguiente ecuación

$$a_0b_n+a_1b_{n-1}\left(-1\right)\left(\begin{array}{c} n \\ 1 \end{array}\right)+a_2b_{n-2}\left(\begin{array}{c} n \\ 2 \end{array}\right)+\cdots+a_nb_0\left(-1\right)^n\left(\begin{array}{c} n \\ n \end{array}\right)=0$$

son llamados polinomios Apolar.

Lema 1.1. Si todas las raíces $z_1,\ldots,z_n$ de $f\left(z\right)$ se encuentran dentro de un dominio circular K y ζ se encuentra fuera de K, entonces todas las raíces de $A_\zeta f\left(z\right)$ se encuentran dentro de K.

Demostración. En primer lugar observemos que, si w_i es una raíz del polinomio $A_\zeta f\left(z\right)$, entonces ζ es el centro de masa de las raíces de $f\left(z\right)$ con respecto a w_i. En efecto, si $\zeta\neq\infty$, entonces podemos expresar la igualdad $A_\zeta f\left(z\right)=0$ en la siguiente forma.

$$\left(\zeta-w_i\right)f^{'}\left(w_i\right)+nf\left(w_i\right)=0$$

es decir,

$$\zeta=w_i-n\frac{f\left(w_i\right)}{f^{'}\left(w_i\right)}$$

Suponiendo que $w_i \notin K$, el mapeo $w(z)$ usado para definir el centro de masa generalizado, mapea w_i al infinito y al circulo K a una recta, en la cual en uno de los semiplanos se encuentran las imágenes de las raíces de f, el centro de masa regular de estos puntos se encuentra en el mismo semiplano y su imagen inversa bajo w^{-1} se encuentra dentro de K, lo que genera una contradicción. Por lo tanto $w_i \in K$.
En el otro caso $\zeta = \infty$ se tiene que $f'(w_i) = 0$ así $w_i \in K$. □

Teorema 1.9 (*J.H.Grace*, 1902)**.** Sean f y g polinomios apolar. Si todas las raíces de f pertenecen a un dominio circular K, entonces al menos una de las raíces de g pertenece a K.

Demostración. Supóngase que todas las raíces $\zeta_1, \ldots, \zeta_n$ de g se encuentran fuera de K. Consideremos el polinomio $A_{\zeta_2} \ldots A_{\zeta_n} f(z)$. El grado de este polinomio es igual a 1, es decir es de la forma $c(z-k)$. El lema anterior implica que $k \in K$, esto ya que todas las raíces del polinomio $A_{\zeta_n} f(z)$ se encuentran dentro de K y como se ha supuesto que ζ_{n-1} está fuera de K aplicando de nuevo el lema tendremos que todas las raíces del polinomio $A_{\zeta_{n-1}} A_{\zeta_n} f(z)$ se encuentran dentro de K y así sucesivamente. Ya que f y g son polinomios apolar, sabemos que $A_{\zeta_1} c(z-k) = 0$. Así aplicando la definición de derivada con respecto a ζ_1 tenemos que:

$$A_{\zeta_1}(z-k) = (\zeta_1 - z) + (z-k) = 0$$

entonces,

$$k = \zeta_1 \notin K$$

Obteniendo una contradicción. Por lo tanto al menos una de las raíces de g se encuentra en K. □

Ejemplo 1.3.

1. El polinomio $f(z) = 1 - z + cz^n$, donde $c \in \mathbb{C}$ y n es par, posee una raíz en el disco $\mid z - 1 \mid \leq 1$.

Demostración. Se tiene

$$f(z) = 1 - z + cz^n = 1 + \begin{pmatrix} n \\ 1 \end{pmatrix} \left(-\frac{1}{n}\right) z + cz^n.$$

Sea

$$g(z) = z^n + \begin{pmatrix} n \\ 1 \end{pmatrix} b_{n-1} z^{n-1} + \cdots + b_0.$$

Así los polinomios f y g son apolares si

$$1 - \begin{pmatrix} n \\ 1 \end{pmatrix} \left(-\frac{1}{n}\right) b_{n-1} + (-1)^n c b_0 = 0$$

es decir, si

$$1 + b_{n-1} + cb_0 = 0$$

Ahora sea

$$\zeta_k = 1 - e^{\frac{2\pi i k}{n}} \qquad para \quad k = 1, \ldots, n$$

Y encontremos $g(z)$ tal que

$$g(z) = \prod_{k=1}^{n} (z - \zeta_k) = z^n + \begin{pmatrix} n \\ 1 \end{pmatrix} b_{n-1} z^{n-1} + \cdots + b_0$$

Entonces

$$\begin{pmatrix} n \\ 1 \end{pmatrix} b_{n-1} = -\sum_{k=1}^{n} \zeta_k = -\sum_{k=1}^{n} \left(1 - e^{\frac{2\pi i k}{n}}\right) = -n + \sum_{k=1}^{n} \left(e^{\frac{2\pi i}{n}}\right)^k = (-n-1) + \frac{1 - \left(e^{\frac{2\pi i}{n}}\right)^{n+1}}{1 - e^{\frac{2\pi i}{n}}}$$

$$= -n$$

así

$$b_{n-1} = -1$$

Además

$$b_0 = \pm \prod_{k=1}^{n} \zeta_k = 0$$

ya que

$$\zeta_n = 0$$

Así se puede concluir que los polinomios $f(z)$ y $g(z)$ son apolares. Ya que todas las raíces de g se encuentran en el disco $\mid z - 1 \mid \leq 1$, al menos una de las raíces de f se

encuentra en este disco. □

2. El polinomio $1 - z + c_1 z^{n_1} + \cdots + c_k z^{n_k}$, donde $1 < n_1 < n_2 < \cdots < n_k$, tiene al menos una raíz en el disco

$$| z | \leq \frac{1}{\left(1 - \frac{1}{n_1}\right) \cdots \left(1 - \frac{1}{n_k}\right)}.$$

Demostración. Se iniciará con el polinomio $f(z) = 1 - z + c_1 z^{n_1}$. Supongamos lo contrario, es decir, que todas las raíces se encuentran en el dominio circular $| z | > \frac{n_1}{n_1 - 1}$. Entonces por lema las raíces del polinomio

$$A_0 f(z) = n_1 - (n_1 - 1) z$$

también se encuentran en el dominio $| z | > \frac{n_1}{n_1 - 1}$.
Pero la raíz de $A_0 f(z)$ es igual a $\frac{n_1}{n_1 - 1}$ obteniéndose así una contradicción. Para el polinomio $1 - z + c_1 z^{n_1} + \cdots + c_k z^{n_k}$, usaremos inducción sobre k. Consideremos el polinomio

$$A_0 f(z) = n_k - (n_k - 1) z + c_1 (n_k - n_1) z^{n_1} + \cdots + c_{k-1} (n_k - n_{k-1}) z^{n_{k-1}}.$$

En este polinomio, cambiemos z por $\frac{n_k}{n_k - 1} w$. Por hipótesis inductiva, las raíces del polinomio obtenido se encuentran dentro del disco

$$| w | \leq \frac{n_1}{n_1 - 1} . \frac{n_2}{n_2 - 1} \cdot \cdots \cdot \frac{n_{k-1}}{n_{k-1} - 1},$$

Y por lo tanto todas las raíces de $A_0 f(z)$ se encuentran en el disco

$$| z | \leq \frac{n_1}{n_1 - 1} . \frac{n_2}{n_2 - 1} \cdot \cdots \cdot \frac{n_k}{n_k - 1}.$$

Además por hipótesis inductiva todas las raíces de $f(z)$ se encuentran fuera del disco, generándose así una contradicción. □

Definición 1.2. Sea $f(z) = \sum_{i=0}^{n} \binom{n}{i} a_i z^i$ y $g(z) = \sum_{i=0}^{n} \binom{n}{i} b_i z^i$. El polinomio

$$h(z) = \sum_{i=1}^{n} \binom{n}{i} a_i b_i z^i$$

es llamado la composición de f y g.

Teorema 1.10 (*Szegö*)**.** Sean f y g polinomios de grado n, y supongamos que todas las raíces de f se encuentran en un dominio circular K. Entonces hay una raíz de h, la composición de f y g que es de la forma $-\zeta_i k$, donde ζ_i es una raíz de g y $k \in K$.

Demostración. Sean

$$f(z) = \sum_{i=0}^{n} \binom{n}{i} a_i z^i$$

$$g(z) = \sum_{i=0}^{n} \binom{n}{i} b_i z^i$$

Supongamos que γ es una raíz de h, es decir

$$\sum_{i=1}^{n} \binom{n}{i} a_i b_i \gamma^i = 0 \qquad (*)$$

Se define el polinomio

$$G(z) = z^n g\left(-\gamma z^{-1}\right) = z^n \sum_{i=1}^{n} \binom{n}{i} b_i \left(-\gamma z^{-1}\right)^i = \sum_{i=1}^{n} \binom{n}{i} b_i \gamma^i z^{n-i} (-1)^i$$

así

$$\begin{aligned} G(z) &= -\binom{n}{1} b_1 \gamma z^{n-1} + \binom{n}{2} b_2 \gamma^2 z^{n-2} - \ldots + (-1)^n \binom{n}{n} b_n \gamma^n \\ f(z) &= \binom{n}{1} a_1 z + \binom{n}{2} a_2 z^2 + \ldots + \binom{n}{n} a_n z^n \end{aligned}$$

Ahora para que f y G sean apolares debe de cumplirse que:

$$-\binom{n}{1} a_1 (-b_1 \gamma) + \binom{n}{2} a_2 \left(b_2 \gamma^2\right) + \ldots + (-1)^n a_n \left(b_n \gamma^n\right) (-1)^n = 0$$

pero esta igualdad es cierta por $(*)$

Aplicando el teorema de Grace, una de las raíces de $G(z)$ se encuentra en K. Así $k \in K$ es la raíz de $G(z)$, entonces $g\left(-\gamma k^{-1}\right) = 0$.

Por lo que $-\gamma k^{-1} = \zeta_i$, donde ζ_i es una raíz de g. □

1.1.5 El problema de Routh-Hurwitz.

Definición 1.3 (Polinomio estable). Son polinomios que cumplen con la propiedad que todas sus raíces pertenecen a la izquierda del semi-plano, es decir las partes reales de las raíces son negativas.

El problema de Routh-Hurwitz consiste en:

Averiguar (directamente) al ver los coeficientes del polinomio si es estable o no

En primer lugar, es suficiente considerar el caso de los polinomios con coeficientes reales. En efecto, si

$$p(z) = \sum_{i=0}^{n} a_n z^n$$

es un polinomio con coeficientes complejos, podemos considerar el polinomio:

$$p^*(z) = p(z)\overline{p(\overline{z})} = (\sum_{i=0}^{n} a_n z^n)(\sum_{i=0}^{n} \overline{a_n} z^n)$$

Claramente, las partes reales de las raíces de $\overline{p(\overline{z})}$ son las mismas que las de $p(z)$. Por otra parte, los coeficientes de $p^*(z)$ son simétricos con respecto a a_n y $\overline{a_n}$. Esto significa que los coeficientes de $p^*(z)$ son invariantes por conjugación, es decir que son reales.

Teorema 1.11 Sea $p(z) = z^n + a_1 z^{n-1} + \cdots + a_n$ un polinomio con coeficientes reales. Sea $q(z) = z^m + b_1 z^{m-1} + \cdots + b_n$, donde $m = \dfrac{n(n-1)}{2}$, el polinomio cuyas raíces son todas las sumas de pares de las raíces de p. El polinomio p es estable sí y sólo si todos los coeficientes del polinomio p y q son positivos.

Demostración. " $\Rightarrow$ " Supongamos que $p(z)$ es estable, es decir, la parte real de las raíces son negativas. Si α es una raíz real de p, donde le corresponde el factor $z - \alpha$, con coeficientes positivos ($\alpha < 0$). Al par de raíces conjugadas, le corresponde el factor

$$(z - a - ib)(z - a + ib) = z^2 - 2az + a^2 + b^2$$

los coeficientes son positivos ya que $a < 0$. Con este procedimiento, todos los coeficientes de P son positivos.

Las raíces complejas de q están dentro del par de raíces conjugadas, porque los coeficientes de q son reales. Además, la parte real de todas las raíces de q es negativa.

" $\Leftarrow$ " Supongamos que todos los coeficientes del polinomio p y q son positivos. En este caso, la parte real de las raíces de p y q son negativas. Ya que, si tenemos el par

de raíces conjugadas $\alpha \pm \beta$, el factor

$$(z-\alpha-i\beta)(z-\alpha+i\beta) = z^2 - 2\alpha z + \alpha^2 + \beta^2$$

nos daría que p tendría coeficientes negativos. □

1.2. Las raíces de un polinomio y las de su derivada.

1.2.1 Teorema de Gauss-Lucas.

Teorema 1.12$(Gauss - Lucas)$. Las raíces de P' pertenecen a la cobertura convexa de las raíces del polinomio P.

Demostración. Sea

$$P(z) = (z-z_1)(z-z_2)\ldots(z-z_n)$$

así

$$\frac{P'(z)}{P(z)} = \frac{1}{z-z_1} + \ldots + \frac{1}{z-z_n}$$

Si z_i es raíz de $P'(z)$, para algún i, entonces z_i pertenece a la cobertura convexa de las raíces de P. Supongamos que w es raíz de $P'(w)$ y $P(w) \neq 0$. Si w no pertenece a la cobertura convexa de los puntos z_1, z_2, …, z_n, entonces, existe una recta L que pasa por w y que no intersecta a la cobertura convexa de los puntos z_1, $z_2, \ldots,$ z_n. Así los vectores $w-z_1, \ldots, w-z_n$ se encuentran en uno de los semiplanos determinados por esta recta. Además los vectores $\frac{1}{w-z_1}, \ldots, \frac{1}{w-z_n}$ se encuentran en un solo semiplano, ya que $\frac{1}{z} = \frac{\overline{z}}{|z|^2}$.

Por lo que

$$\frac{P'(w)}{P(w)} = \frac{1}{w-z_1} + \ldots + \frac{1}{w-z_n} \neq 0$$

La cual es una contradicción, así w pertenece a la covertura convexa de las raíces de P. □

Teorema 1.13. Sea $P(z) = (z-x_1)(z-x_2)\ldots(z-x_n)$, donde $x_1 < x_2 < \ldots < x_n$. Si alguna raíz x_i es remplazada por $x_i' \in (x_i, x_{i+1})$, entonces todas las raíces de P' incrementan su valor.

Demostración. Sean $z_1 < z_2 < \ldots < z_{n-1}$ las raíces de P', y $x_1, \ldots, x_n$ las raíces de P. Supongamos que $z_1' < z_2' < \ldots < z_{n-1}'$ son las raíces de Q'

y $x_1^{'} = x_1, \ldots, x_{i-1}^{'} = x_{i-1}$, $x_i^{'}$, $x_{i+1}^{'} = x_{i+1}, \ldots, x_n^{'} = x_n$ son las raíces de Q. Para las raíces de z_k y $z_k^{'}$ tenemos las siguientes relaciones

$$\sum_{i=1}^{n} \frac{1}{z_k - x_i} = 0 \qquad (*)$$

$$\sum_{i=1}^{n} \frac{1}{z_k^{'} - x_i^{'}} = 0 \qquad (**)$$

Supongamos que la conclusión del teorema es falsa, es decir, $z_k^{'} < z_k$ para algún k. Entonces $z_k^{'} - x_i^{'} < z_k - x_i$. Observemos que las diferencias $z_k^{'} - x_i^{'}$ y $z_k - x_i$ son del mismo signo. En efecto

$z_j < x_i$, $z_j^{'} < x_i^{'}$ para $j \leq i-1$ y $z_j > x_i$, $z_j^{'} > x_i^{'}$ para $j \geq i$.

Por lo tanto, $\dfrac{1}{z_k - x_i} < \dfrac{1}{z_k^{'} - x_i^{'}}$ para toda $i = 1, \ldots, n$. Pero en este caso las relaciones $(*)$ y $(**)$ no pueden cumplirse, generando así una contradicción. □

1.2.2 Localización de las raíces de la derivada.

Definición 1.6: Sea f un polinomio con coeficientes reales. Para todo par de raíces conjugadas z y $\overline{z}$ de f, el disco con diámetro $z\overline{z}$ es llamado disco de Jensen para f.

Si $z\overline{z}$ es diámetro, queremos decir que z y $\overline{z}$ son los extremos del disco.

Teorema 1.14 $(Jensen)$. Toda raíz no real de f', se encuentra dentro o en la frontera de uno de los discos de Jensen para f.

Demostración. Sea $z_1, \cdots, z_n$ las raíces de f, entonces:

$$\frac{f'(z)}{f(z)} = \sum_{j=1}^{n} \frac{1}{z - z_j} \qquad (1)$$

Se demostrará que si z está fuera del disco de Jensen con diámetro $z_p z_q$ entonces:

$$sig\ Im(\frac{1}{z - z_p} + \frac{1}{z - z_q}) = -sig\ Imz \quad (2)$$

En efecto; sea $z_p = a + bi$ y $z_q = a - bi$

$$\frac{1}{z - a - bi} + \frac{1}{z - a + bi} = \frac{2(z-a)}{(z-a)^2 + b^2} = \frac{2(z-a)((\overline{z} - a)^2 + b^2)}{|(z-a)^2 + b^2|^2}$$

Entonces

$$Im((z-a)(\overline{z}-a)^2+(z-a)b^2) = Im((\overline{z}-a)\,|z-a|^2+(z-a)b^2) = (b^2-|z-a|^2)Imz$$

Ahora demostraremos que si $z \notin \mathbb{R}$ y $z_j = a \in \mathbb{R}$, entonces

$$Sig\ Im(\frac{1}{z-z_j}) = -Sig\ Imz \quad (3)$$

En efecto,

$$\frac{1}{z-a} - \frac{1}{\overline{z}-a} = \frac{\overline{z}-z}{|z-a|^2} = \frac{-2Imz}{|z-a|^2}$$

Las fórmulas (1), (2) y (3) implica que si un punto $z \notin \mathbb{R}$ se encuentra fuera de todos los discos de Jensen, entonces

$$Sin\ Im\frac{f'(z)}{f(z)} = -Sig\ Imz \neq 0$$

Por lo tanto $f'(z) \neq 0$, es decir z no es una raíz de f'. □

1.2.3 La conjetura de Sendov-Ilieff.

En 1962, el matemático Búlgaro B. Sendov hizo la siguiente conjetura que con frecuencia es atribuida a otro matemático Búlgaro L. Ilieff:

"Sea $p(z)$ un polinomio (grad$p \geq 2$) donde todas las raíces se encuentran en el disco $|z| \leq 1$. Si z_0 es una raíz de $p(z)$, entonces el disco $|z - z_0| \leq 1$ contiene al menos una raíz de $p'(z)$"

La conjetura de Sendov-Ilieff esta probada para polinomios de grado menores o iguales a cinco y para algunos polinomios particulares.

Nos limitaremos a probar la conjetura de Sendov-Ilieff para polinomios de la forma

$$p(z) = (z - z_0)^{n_0}(z - z_1)^{n_1}(z - z_2)^{n_2}$$

Cuando $n = n_0 + n_1 + n_2 \geq 4$. En este caso tenemos que probar que si $|z_i| \leq 1$ para $i = 0, 1, 2$. Entonces el polinomio $p'(z)$ tiene una raíz en el disco $|z - z_0| \leq 1$.

Es necesario expresar $p'(z)$ factorizado. Entonces

$$\begin{aligned} p'(z) &= n_0(z-z_0)^{n_0-1}(z-z_1)^{n_1}(z-z_2)^{n_2} + n_1(z-z_1)^{n_1-1}(z-z_0)^{n_0}(z-z_2)^{n_2} \\ &\quad +n_2(z-z_2)^{n_2-1}(z-z_1)^{n_1}(z-z_0)^{n_0} \\ &= (z-z_0)^{n_0-1}(z-z_1)^{n_1-1}(z-z_2)^{n_2-1} + (n_0(z-z_1)(z-z_2) + n_1(z-z_0)(z-z_2) \\ &\quad +n_2(z-z_0)(z-z_1)) \end{aligned}$$

Notemos que $q(z) = n_0(z-z_1)(z-z_2) + n_1(z-z_0)(z-z_2) + n_2(z-z_0)(z-z_1)$ es un polinomio de grado 2, que lo podemos factorizar con sus raíces de la siguiente forma

$$q(z) = n\left(\frac{n_0}{n}(z-z_1)(z-z_2) + \frac{n_1}{n}(z-z_0)(z-z_2) + \frac{n_2}{n}(z-z_0)(z-z_1)\right)$$

entonces $q(z) = n(z-w_1)(z-w_2)$.

Con esto

$$p'(z) = n(z-z_0)^{n_0-1}(z-z_1)^{n_1-1}(z-z_2)^{n_2-1}(z-w_1)(z-w_2) \quad (4)$$

Si $n_0 > 1$, entonces z_0 es una raíz de $p'(z)$. Supongamos que $n_0 = 1$, entonces $p(z) = (z-z_0)(z-z_1)^{n_1}(z-z_2)^{n_2}$. Con esto,

$$p'(z_0) = (z_0-z_1)^{n_1}(z_0-z_2)^{n_2} \quad (5)$$

De (4) y (5) tenemos que

$$(z_0-z_1)(z_0-z_2) = n(z-w_1)(z-w_2).$$

Teniendo en cuenta que $|z_0-z_1| \leq |z_0| + |z_1| = 2$ y $|z_0-z_2| \leq 2$, obtenemos

$$|z-w_1|\,|z-w_2| = \frac{1}{n}\,|z_0-z_1|\,|z_0-z_2| \leq \frac{4}{n} \leq 1.$$

Por lo tanto $|z-w_1| \leq 1$ o $|z-w_1| \leq 1$

Lema 1.2. Sea $p(z)$ un polinomio de grado n, donde $n \geq 2$. Si z_0 es una raíz de $p(z)$

$$|p''(z_0)| \geq (n-1)\,|p'(z_0)|\,,$$

entonces al menos una raíz de $p'(z)$ está en el disco $|z-z_0| \leq 1$.

Demostración. Sea $w_1, \cdots, w_{n-1}$ las raíces de p' y supongamos que el coeficiente de

la potencia mayor de p es uno. En este caso $p'(z) = n\prod_{j=1}^{n-1}(z - w_j)$. De esto, se tiene

$$\frac{p''(z)}{p'(z)} = \sum_{j=1}^{n-1} \frac{1}{z - w_j}$$

Por hipótesis z_0 es una raíz simple de $p(z)$, es decir $p'(z_0) \neq 0$. Ahora supongamos que $|z_0 - w_j| > 1$ para $j = 1, \cdots, n-1$. Entonces la desigualdad $|p''(z_0)| \geq (n-1)\,|p'(z_0)|$ implica que

$$n - 1 \leq \left|\frac{p''(z_0)}{p'(z_0)}\right| \leq \sum_{j=1}^{n-1} \frac{1}{|z_0 - w_j|} < n - 1$$

y esto es una contradicción. □

Capítulo 2

Polinomios irreducibles

Sean f y g polinomios en una variable con coeficientes en un campo K. Decimos que f es divisible por g si $f = gh$, donde h es un polinomio con coeficientes en K.

El polinomio d es llamado común divisor de f y g si ambos son divisibles por d. El divisor común de f y g es llamado máximo común divisor si es divisible por cualquier divisor común de f y g.

Se puede encontrar el máximo común divisor $d = (f, g)$ de f y g con ayuda del algoritmo de Euclides. Supongamos que $grad\,(f) \geq grad\,(g)$. Sea r_1 el residuo después de la división de f por g, sea r_2 el residuo después de la división de g por r_1, y en general sea r_{k+1} el residuo después de la división de r_{k-1} por r_k. Ya que los grados de los polinomios son estrictamente decrecientes, se tendrá para algún n que $r_{n+1} = 0$, es decir, r_{n-1} es divisible por r_n. Podemos ver que f y g son divisibles por r_n ya que r_n divide a todos los polinomios r_{n-1}, $r_{n-2}, \ldots$. Además, si f y g son divisibles por un polinomio h, entonces r_n también es divisible por h ya que h divide a r_1, $r_2, \ldots$. Por lo tanto $r_n = (f, g)$.

Se estudiarán las principales propiedades de los polinomios irreducibles, Criterios de irreducibilidad y la irreducibilidad de los polinomios de la forma $x^n \pm x^m \pm x^p \pm 1$.

2.1. Principales propiedades de polinomios irreducibles.

2.1.1 Factorización de polinomios en factores irreducibles.

Teorema 2.1. Si d es el máximo común divisor de los polinomios f y g, entonces existen polinomios a y b tal que $d = af + bg$.

Demostración. Sea el conjunto $S = \{fx + gy : \ x, y \in K[x]\}$ y sea $l = af + bg$ el menor polinomio de este conjunto. Si $l \nmid f$, existen q y r tales que $f = ql + r$, $0 < r < l$.

$$r = f - ql = f - q(af + bg) = f(1 - qa) + g(-qb).$$

Entonces r pertenece al conjunto S y es menor que l; y eso contradice la elección del polinomio l. Luego $l \setminus f$. Por la misma razón $l \mid g$. Es decir $l \mid (f, g) = d$.

Por otra parte $d \mid f$ y $d \mid g$. En particular $d \mid af + bg$. Por lo tanto hemos probado que $l = af + bg = d$. □

Lema 2.1. Si el polinomio qr es divisible por un polinomio irreducible p, entonces q o r es divisible por p.

Demostración. Supongamos que q no es divisible por p. Entonces $(p, q) = 1$, es decir existen polinomios a y b tal que $ap + bq = 1$. Multiplicando ambos lados de esta identidad por r tenemos que $apr + bqr = r$. Pero pr y qr son divisibles por p, así r es divisible por p. □

Teorema 2.2 Sea K un campo. Entonces el polinomio $f \in K[x]$ puede ser factorizado en factores irreducibles y esta factorización es única.

Demostración. La existencia de la factorización es fácil de probar por inducción sobre $n = grad(f)$. Primero notemos que si f es irreducible su factorización es f. Para $n = 1$, el polinomio f es irreducible. Supongamos que la factorización existe para cualquier polinomio de grado menor que n y sea $grad(f) = n$. Si asumimos que f es reducible, es decir, $f = gh$, donde $grad(g) < n$ y $grad(h) < n$. Pero las factorizaciones de f y g existen por hipótesis inductiva.

Ahora se probará que la factorización es única. Sean $ag_1 \dots g_s = bh_1 \dots h_t$, donde $a, b \in K$ y $g_1 \dots g_s$, $h_1 \dots h_t$ son polinomios mónicos, irreducibles sobre K. Claramente, en este caso $a = b$. El polinomio $g_1 \dots g_s$ es divisible por el polinomio irreducible h_1, por lo que $h_1 = g_1$, al seguir con este proceso tendremos que $h_i = g_i$. □

La irreducibilidad sobre el anillo de los enteros $\mathbb{Z}$ está definido de la siguiente manera, $f \in \mathbb{Z}[x]$ es irreducible sobre $\mathbb{Z}$ si no puede ser representado como producto de polinomios de grados positivos con coeficientes enteros. Notemos que cuando los coeficientes de un polinomio pertenecen a un anillo, no siempre se pueden dividir

los coeficientes por otro; en este caso solo podemos dividir los coeficientes por el máximo común divisor de todos los coeficientes. Esta complicación motiva la siguiente definición.

Definición 2.1. Sea $f(x) = \sum a_i x^i$, donde $a_i \in \mathbb{Z}$. El máximo común divisor de los coeficientes $a_0, \ldots, a_n$ es llamado el conteo de f y denotado por $cont(f)$. Claramente $f(x) = cont(f)\, g(x)$, donde g es un polinomio sobre $\mathbb{Z}$ con conteo 1. Los polinomios cuyo conteo es igual a uno son llamados *primitivos*.

Lema 2.2. (*Gauss*)

$$cont(fg) = cont(f)\, cont(g)$$

Demostración. Se demostrará que si f y g son dos polinomios primitivos entonces fg es primitivo.

Sean f y g primitivos, investiguemos si existe algún primo p que pueda dividir a $cont(fg)$. Sea $f = a_n x^n + ... + a_0$ y $g = b_m x^m + ... + b_0$. Al ser f y g primitivos $p \nmid cont(f)$ y $p \nmid cont(g)$. Por lo tanto existen a_i y b_j no divisibles por el primo p. Sean $i_0 := min\{i / p \nmid a_i\}$ y $j_0 := \{j / p \nmid b_j\}$ y estudiemos el coeficiente $c_{i_0+j_0}$ del producto fg .

$$c_{i_0+j_0} = a_{i_0+j_0}b_0 + \cdots + a_{i_0+1}b_{j_0-1} + a_{i_0}b_{j_0} + a_{i_0-1}b_{j_0+1} + \cdots + a_0 b_{i_0+j_0}$$

Por definición de i_0 y j_0 se observa que $p/a_0, ..., p/a_{i_0-1}$ y $p/b_0, ..., p/b_{j_0-1}$, salvo eventualmente a $a_{i_0}b_{j_0}$. Además $p \nmid a_{i_0}$ y $p \nmid b_{j_0}$, ya que p es primo

$p \nmid a_{i_0}b_{j_0} \Rightarrow p \nmid c_{i_0+j_0} \Rightarrow p \nmid cont(fg) \Rightarrow cont(fg) = 1$, por lo tanto fg es primitivo.

Ahora se procede a demostrar el lema de Gauss.

Sea $f = cont(f)\overline{f}$ y $g = cont(g)\,\overline{g}$ con $\overline{f}$ y $\overline{g} \in \mathbb{Z}[x]$ primitivos. Se tiene que

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

□

Corolario 2.1. Un polinomio con coeficientes enteros es irreducible sobre $\mathbb{Z}$ sí y sólo sí es irreducible sobre $\mathbb{Q}$.

Demostración. Sea $f \in \mathbb{Z}[x]$ y $f = gh$, donde $g, h \in \mathbb{Q}[x]$. Asumamos que

$cont\,(f) = 1$. Para g, seleccionemos un entero positivo m tal que $mg \in \mathbb{Z}[x]$. Sea $n = cont\,(mg)$. Entonces el racional $r = \dfrac{m}{n}$ es tal que $rg \in \mathbb{Z}[x]$ y $cont\,(rg) = 1$. Similarmente, seleccionemos un número racional positivo s para h. Vamos a demostrar que en este caso $rs = 1$, es decir la factorización $f = (rg)(sh)$ es una factorización sobre $\mathbb{Z}$. En efecto, gracias al lema de Gauss, $cont\,(rg)\,cont\,(sh) = cont\,(rsgh)$, es decir $cont\,(rsf) = 1$. Ya que $cont\,(f) = 1$ deducimos que $rs = 1$ lo cual nos genera una contradicción. □

2.1.2 Criterio de Eisenstein.

Uno de los mejores criterios de irreducibilidad de polinomios es el criterio de Eisenstein.

Teorema 2.3 (*Criterio de Einsenstein*)**.** Sea $f(x) = a_0 + a_1x + \cdots + a_nx^n$ un polinomio con coeficientes enteros tal que a_n no es divisible por un primo p, mientras los coeficientes $a_0, \ldots, a_{n-1}$ son divisibles por p pero a_0 no es divisible por p^2. Entonces f es irreducible sobre $\mathbb{Z}$.

Demostración. Supongamos que

$$f = gh = \left(\sum b_k x^k\right)\left(\sum c_l x^l\right)$$

donde g y h son polinomios de grados positivos y con coeficientes enteros. El número $b_0c_0 = a_0$ es divisible por p, por lo que uno de los números b_0 o c_0 es divisible por p. Suponiendo que b_0 es divisible por p, entonces c_0 no puede ser divisible por p ya que $a_0 = b_0c_0$ no es divisible por p^2. Si todos los números b_i son divisibles por p, entonces lo es a_n. Así b_i no es divisible por p para algún i, donde $0 < i < gradg < n$; asumamos que i es el mínimo índice de los números b_i que no son divisibles por p.
Por hipótesis el número a_i es divisible por p. Además

$$a_i = b_ic_0 + b_{i-1}c_1 + \cdots + b_0c_i$$

donde todos los sumandos $b_{i-1}c_1, \ldots, b_0c_i$ son divisibles por p mientras b_ic_0 no lo es esto genera una contradicción. □

Ejemplo 2.1.

1. Sea p un primo y q no divisible por p. Entonces $x^m - pq$ es irreducible sobre $\mathbb{Z}$.

2. El polinomio $4x^5 + 7x^4 - 14x^3 + 49x^2 - 28$ no puede ser escrito como el producto de dos polinomios con coeficientes racionales de grados al menos 1.

2.2. Criterios de irreducibilidad.

2.2.1 Polinomios con un coeficiente dominante.

Teorema 2.4 (*Criterio de Perron*) Sea $f(x) = x^n + a_1x^{n-1} + \cdots + a_n$ un polinomio con coeficientes enteros tal que $a_n \neq 0$.

a) Si $\mid a_1 \mid > 1 + \mid a_2 \mid + \cdots + \mid a_n \mid$, entonces f es irreducible sobre $\mathbb{Z}$.

b) Si $\mid a_1 \mid \geq 1 + \mid a_2 \mid + \cdots + \mid a_n \mid$ y $f(\pm 1) \neq 0$, entonces f es irreducible sobre $\mathbb{Z}$.

Demostración. a) En primer lugar se probará que todas las raíces de f, excepto una, se encuentran dentro del disco $\mid z \mid \leq 1$. Claramente el polinomio

$$g(x) = x^n + a_1x^{n-1}$$

satisface esta propiedad, es decir todas las raíces de g, excepto una, se encuentran dentro del disco $\mid z \mid \leq 1$. Por el teorema de Rouché es suficiente probar que para $\mid z \mid = 1$ se satisface que

$$\mid f(z) - g(z) \mid < \mid f(z) \mid + \mid g(z) \mid$$

Pero para $\mid z \mid = 1$ se tiene, por una parte,

$$\mid f(z) - g(z) \mid = \mid a_2z^{n-2} + \ldots + a_n \mid \leq \mid a_2 \mid + \ldots + \mid a_n \mid < \mid a_1 \mid -1 \qquad (1)$$

Y por otro lado

$$\mid f(z) \mid + \mid g(z) \mid \geq \mid g(z) \mid = \mid z^n + a_1z^{n-1} \mid = \mid z + a_1 \mid \geq \mid a_1 \mid -1 \qquad (2)$$

Supongamos ahora lo contrario, que f puede ser representado como el producto de polinomios f_1 y f_2 de grados positivos con coeficientes enteros. El producto de las raíces de cada uno de los polinomios f_1 y f_2 es un entero diferente de cero, y además cada uno de esos polinomios tiene una raíz cuyo valor absoluto no es menor que uno. Pero f tiene solo una de tales raíces, obteniendo así una contradicción.

b) Si $\mid a_1 \mid = 1 + \mid a_2 \mid + \ldots + \mid a_n \mid$, la desigualdad (1) no es estricta. Pero si

$f(\pm 1) \neq 0$, la desigualdad (2) es estricta. En efecto, para $\mid z \mid = 1$ la igualdad

$$\mid f(z) \mid + \mid g(z) \mid = \mid a_1 \mid -1$$

implica que

$$\mid f(z) \mid + \mid g(z) \mid = \mid g(z) \mid$$

lo que implica que

$$\mid f(z) \mid = 0$$

Pero $f(\pm 1) \neq 0$ lo cual genera una contradicción. □

Ejemplo 2.2 . ¿ Para que valores de "c" son irreducibles los polinomios de la forma

$x^2 + nx + c$?.

Demostración. Por el criterio de Perron, (a), estos polinomios son irreducibles cuando $0 < |c| < (n-1)$ y $c \in \mathbb{Z}$. □

Ejemplo 2.3. Los polinomios de la forma $x^{2n-1} + 2x + 1$ son irreducibles en $\mathbb{Z}$.

Teorema 2.5 Sean $a_1 \geq a_2 \geq \cdots \geq a_n$ enteros positivos y $n \geq 2$. Entonces el polinomio

$$P(x) = x^n - a_1 x^{n-1} - a_2 x^{n-2} - \cdots - a_n$$

es irreducible sobre $\mathbb{Z}$.

Demostración. Consideremos el polinomio

$$\begin{aligned} f(x) &= (x-1) P(x) \\ &= x^{n+1} - a_1 x^n - a_2 x^{n-1} - \cdots - a_{n-1} x^2 - a_n x \\ &\quad -x^n + a_1 x^{n-1} + \cdots + a_{n-2} x^2 + a_{n-1} x + a_n \end{aligned}$$

Así

$$f(x) = x^{n+1} - (a_1 + 1) x^n + (a_1 - a_2) x^{n-1} + \cdots + (a_{n-1} - a_n) x + a_n$$

o de forma equivalente

$$f(x) = x^{n+1} - b_1 x^n + b_2 x^{n-1} + \cdots + b_n x + b_{n+1}$$

Los números $b_1, b_2, \ldots, b_{n+1}$ son enteros positivos o cero y $b_1 = 1 + b_2 + \cdots + b_{n+1}$. Además $f(x)$ satisface una de las condiciones del teorema anterior, pero no satisface la segunda condición ya que $f(1) = 0$. Nosotros podemos aplicar el siguiente argumento.

Sea

$$h(z) = b_1 z^n - b_2 z^{n-1} - \cdots - b_{n+1}$$

En primer lugar se mostrará que, para todo ε suficientemente grande $\varepsilon > 0$, tenemos

$$\mid h(z) \mid > \mid z^{n+1} \mid = \mid f(z) + h(z) \mid$$

donde $\mid z \mid = 1 + \varepsilon$. En efecto, si $\mid z \mid = 1 + \varepsilon$, entonces

$$\begin{aligned} \mid h(z) \mid &= \mid b_1 z^n - b_2 z^{n-1} - \cdots - b_{n+1} \mid \\ &\geq b_1 \mid z \mid^n - b_2 \mid z \mid^{n-1} - \cdots - b_{n+1} \\ &= b_1 (1+\varepsilon)^n - b_2 (1+\varepsilon)^{n-1} - \cdots - b_{n+1} \end{aligned}$$

Así

$$\mid h(z) \mid - \mid z^{n+1} \mid \geq b_1 (1+\varepsilon)^n - b_2 (1+\varepsilon)^{n-1} - \cdots - b_{n+1} - (1+\varepsilon)^{n+1}$$

Recordemos que

$$(1+\varepsilon)^n = \sum_{i=0}^{n} \binom{n}{i} \varepsilon^{n-i},$$

cuando $i = n - 1$ el término es

$$\binom{n}{n-1} \varepsilon = n\varepsilon$$

$$(1+\varepsilon)^{n-1} = \sum_{i=0}^{n-1} \binom{n-1}{i} \varepsilon^{n-1-i},$$

cuando $i = n - 2$ el término es

$$\binom{n-1}{n-2} \varepsilon = (n-1)\varepsilon$$

y así sucesivamente.

Por lo que

$$\begin{aligned}
\mid h(z) \mid - \mid z^{n+1} \mid &\geq nb_1\varepsilon - (n-1)\, b_2\varepsilon - \cdots - 2b_{n-1}\varepsilon - b_n\varepsilon - b_{n+1} - (n+1)\,\varepsilon + \cdots \\
&= \varepsilon\,(nb_1 - (n-1)\, b_2 - \cdots - 2b_{n-1} - b_n - (n+1)) + \cdots \\
&= \varepsilon\,(nb_1 - nb_2 - \cdots - nb_{n-1} - nb_n - n + b_2 + 2b_3 + \cdots \\
&\quad + (n-2)\, b_{n-1} + (n-1)\, b_n - 1) + \cdots \\
&= \varepsilon\,(n\,(b_1 - b_2 - \cdots - nb - b_n - 1) \\
&\quad + (b_2 + 2b_3 + \cdots + (n-1)\, b_n - 1)) + \cdots \\
&= \varepsilon\,(b_2 + 2b_3 + \cdots + (n-1)\, b_n + nb_{n+1} - 1) + \ldots
\end{aligned}$$

Así el coeficiente de ε es positivo, y además, para $\varepsilon > 0$ suficientemente grande, tenemos que $\mid h(z) \mid - \mid z^{n+1} \mid > 0$. En este caso

$$\begin{aligned}
\mid f(z) + h(z) \mid &= \mid z^{n+1} \mid \\
&< \mid h(z) \mid \\
&\leq \mid f(z) \mid + \mid h(z) \mid
\end{aligned}$$

Además por el teorema de Rouché, el polinomio $f(z)$ tiene tantas raíces dentro del disco $\mid z \mid \leq 1+\varepsilon$ como $h(z)$. Pero todas las raíces de $h(z)$ se encuentran estrictamente dentro del disco $\mid z \mid \leq 1$. En efecto, si $\mid z \mid \geq 1$, entonces

$$\begin{aligned}
\mid h(z) \mid &\geq b_1 \mid z \mid^n - b_2 \mid z \mid^{n-1} - \cdots - b_{n+1} \\
&\geq \mid z \mid^n (b_1 - b_2 - \cdots - b_{n+1}) \\
&= \mid z \mid^n \\
&> 0
\end{aligned}$$

Cuando $\varepsilon \to 0$, vemos que dentro y sobre la frontera del disco unitario hay exactamente n raíces del polinomio $f(x) = (1-x)\, P(x)$. Ya que exactamente $n-1$ raíces de $P(x)$ se encuentran dentro de el disco unitario y una de ellas se encuentra fuera de ella, podemos concluir que P es irreducible. □

Teorema 2.6 Sea $f(x) = x^n + a_1 x^{n-1} + \cdots + a_{n-1}\, x \pm p$, un polinomio con coeficientes enteros, p un primo.

a) Si $p > 1 + \mid a_1 \mid + \cdots + \mid a_{n-1} \mid$, entonces f es irreducible.

b) Si $p \geq 1 + \mid a_1 \mid + \cdots + \mid a_{n-1} \mid$ y las raíces de f no son raíces de la unidad, entonces f es irreducible.

Demostración. Supongamos que $f(x) = g(x)\, h(x)$, donde g y h son polinomios de

grados positivos con coeficientes enteros. El producto de los términos constantes de g y h es igual a $\pm p$. Ya que p es primo, uno de esos términos constantes es igual a ± 1. Además el producto de los valores absolutos de las raíces de uno de los polinomios g o h es igual a 1. Este polinomio posee una raíz α tal que $\mid \alpha \mid \leq 1$. Así α también es raíz de f, $f(\alpha) = 0$.

Ahora

$$\begin{aligned} p &= \mid \alpha^n + a_1\alpha^{n-1} + \cdots + a_{n-1}\alpha \mid \\ &\leq 1 + \mid a_1 \mid + \cdots + \mid a_{n-1} \mid \end{aligned}$$

que es una contradicción para el caso (a).

En el caso (b), α no es raíz de la unidad. Así $\mid \alpha \mid < 1$ y además

$$p < 1 + \mid a_1 \mid + \cdots + \mid a_{n-1} \mid$$

que es una contradicción. □

2.2.2 Irreducibilidad de polinomios que alcanzan valores pequeños.

Para el siguiente lema se necesita la siguiente consecuencia directa del teorema fundamental del álgebra.

Lema 2.3. Si f y g son polinomios de grado a lo sumo n y para $d_0 < d_1 < \cdots < d_n$ se cumple que $f(d_i) = g(d_i)$ para $i \in \{0, 1, \ldots, n\}$, entonces $f = g$.

Demostración. Sean

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n$$

$$g(x) = b_0 + b_1 x + \cdots + b_n x^n$$

además $f(d_i) = g(d_i)$ para $i \in \{0, 1, \ldots, n\}$, es decir

$$a_0 + a_1 d_i + \cdots + a_n d_i^n = b_0 + b_1 d_i + \cdots + b_n d_i^n$$

o

$$(a_0 - b_0) + (a_1 - b_1) d_i + \cdots + (a_n - b_n) d_i^n = 0$$

Por lo que el polinomio

$$h(x) = c_0 + c_1 x + \cdots + c_n x^n$$

$$c_i = a_i - b_i$$

tiene $n+1$ raíces distintas y eso solo puede pasar si $h(x)$ es el polinomio cero por lo tanto

$a_i = b_i$ para $i \in \{0, 1, \ldots, n\}$, así $f = g$. □

Lema 2.4 (*Pólya*)**.** Sea g un polinomio de grado k con coeficientes enteros y sean $d_0 < d_1 < \cdots < d_n$ enteros no raíces de g. Entonces $\mid g(d_i) \mid \geq k!2^{-k}$ para algún i.

Demostración. Sea $g = a_0 + a_1 x + ... + a_k x^k$ y consideremos el polinomio

$$G(x) = (x-d_0)(x-d_1)\cdots(x-d_k)\sum_{i=0}^{k}\frac{g(d_i)}{x-d_i}\prod_{j\neq i}\frac{1}{d_i-d_j}$$

Ahora veamos que:

$$G(d_i) = g(d_i) \qquad\qquad i = 0, \ldots, k$$

$$\begin{aligned} G(x) &= (x-d_0)(x-d_1)\cdots(x-d_k)\frac{g(d_0)}{x-d_0}\prod_{j\neq 0}\frac{1}{d_0-d_j} \\ &\quad +(x-d_0)(x-d_1)\cdots(x-d_k)\frac{g(d_1)}{x-d_1}\prod_{j\neq 1}\frac{1}{d_1-d_j}+\cdots \\ &\quad \cdots+(x-d_0)(x-d_1)\cdots(x-d_k)\frac{g(d_k)}{x-d_k}\prod_{j\neq k}\frac{1}{d_k-d_j} \end{aligned}$$

Así

$$G(d_0) = g(d_0)$$

$$G(d_1) = g(d_1)$$

$$\vdots$$

$$G(d_k) = g(d_k)$$

Por lo que se puede concluir que

$$G(x) = g(x)$$

Como $G(x) = g(x)$ el coeficiente de x^k, a_k es entero diferente de cero, ya que de lo contrario el grado del polinomio g no sería k, tenemos que:

$$\mid \sum_{i=0}^{k} g(d_i)\prod_{i\neq j}\frac{1}{d_i-d_j} \mid \geq 1$$

Así

$$\begin{aligned} 1 &\leq |\sum_{i=0}^{k} g(d_i) \prod_{i\neq j} \frac{1}{d_i - d_j}| \\ &\leq \sum_{i=0}^{k} |\, g(d_i) \prod_{i\neq j} \frac{1}{d_i - d_j}| \\ &= \sum_{i=0}^{k} |\, g(d_i)\,| \prod_{i\neq j} \frac{1}{|\, d_i - d_j\,|} \end{aligned}$$

Sea

$$\begin{aligned} 1 &\leq |\, g(d_l)\,| \sum_{i=0}^{k} \prod_{j\neq i} \frac{1}{|\, d_i - d_j\,|} \\ \frac{1}{\sum_{i=0}^{k} \prod_{j\neq i} \frac{1}{|d_i - d_j|}} &\leq |\, g(d_l)\,| \qquad (1) \end{aligned}$$

Por otra parte

$$\sum_{i=0}^{k} \prod_{j\neq i} \frac{1}{|\, d_i - d_j\,|} \leq \sum_{i=0}^{k} \prod_{j\neq k} \frac{1}{|\, i - j\,|}$$

Además el $i-$*ésimo* término de esta sumatoria es:

$$\begin{aligned} \prod_{j\neq k} \frac{1}{|\, i-j\,|} &= \frac{1}{|\, i-0\,|} * \frac{1}{|\, i-1\,|} * \cdots * \frac{1}{|\, i-(i-1)\,|} * \frac{1}{|\, i-(i+1)\,|} * \cdots * \frac{1}{|\, i-k\,|} \\ &= \frac{1}{i!\,(k-i)!} \end{aligned}$$

Así

$$\begin{aligned} \sum_{i=0}^{k} \prod_{j\neq k} \frac{1}{|\, i-j\,|} &= \sum_{i=0}^{k} \frac{1}{i!\,(k-i)!} \\ &= \frac{1}{k!} \sum_{i=0}^{k} \frac{k!}{i!\,(k-i)!} \\ &= \frac{1}{k!} \sum_{i=0}^{k} \begin{pmatrix} k \\ i \end{pmatrix} \\ &= \frac{1}{k!} 2^k \end{aligned}$$

por lo tanto

$$k!2^{-k} \leq \frac{1}{\sum_{i=0}^{k} \prod_{j \neq i} \frac{1}{|d_i - d_j|}} \qquad (2)$$

De (1) y (2) se puede concluir que la desigualdad deseada. □

Teorema 2.7 (*Pólya*). Sea f un polinomio de grado n con coeficientes enteros y definamos $m = \left[\frac{n+1}{2}\right]$. Supongamos que para n enteros diferentes $a_1, a_2, \ldots, a_n$, tenemos que $\mid f(a_i) \mid < 2^{-m}m!$ y los números $a_1, a_2, \ldots, a_n$ no son raíces de f, entonces f es irreducible.

Demostración. Supongamos que $f = gh$, donde g y h son polinomios con coeficientes enteros. Asumamos que $grad(h) \leq grad(g) = k$. Entonces $m \leq k < n$. Claramente $g(a_i) \neq 0$ y $g(a_i)$ divide a $f(a_i)$. Por lo tanto

$$\mid g(a_i) \mid \leq \mid f(a_i) \mid < 2^{-m}m!$$

Por otro lado por el lema de *Pólya*, tenemos que $\mid g(a_i) \mid \geq 2^{-k}k!$ para uno de los a_i. Como $m \leq k$, obtenemos que $2^{-k}k! \geq 2^{-m}m!$. En efecto, para $m = k + r$,

$$\frac{m!}{k!} = (k+1)(k+2)\cdots(k+r) = 2^r = \frac{2^m}{2^k}$$

□

Ejemplo 2.4 El polinomio $f(x) = (x-1)(x-2)\cdots(x-n) + 1$ es irreducible.

2.3. Algunas propiedades sobre trinomios y cuatrinomios

2.3.1 Polinomios de la forma $x^n \pm x^m \pm x^p \pm 1$.

Para este capítulo sea $f(x) = x^n + \varepsilon_1 x^m + \varepsilon_2 x^p + \varepsilon_3$, $n > m > p \geq 1$ y $\varepsilon_i = \pm 1$

Definición 2.2. Sea $\varphi(x)$ de grado p se dice ser recursivo si $\varphi(x) = \pm x^p \varphi\left(\frac{1}{x}\right)$.

Lema 2.5. Sea $f(x) = \varphi(x)\psi(x)$, donde $\varphi(x)$ y $\psi(x)$ son polinomios mónicos de grado positivo con coeficientes enteros. Entonces al menos uno de los polinomios $\varphi(x)$ y $\psi(x)$ es recursivo.

Demostración. Sea $r = grad(\varphi)$ y $s = n - r = grad(\psi)$. Consideremos los polinomios:

$$\begin{aligned} f_1(x) &= x^r\varphi\left(\frac{1}{x}\right)\psi(x) = \sum_{i=0}^{n} c_i x^{n-i} \\ f_2(x) &= x^s\psi\left(\frac{1}{x}\right)\varphi(x) = x^n\left(\left(\frac{1}{x}\right)^r\varphi(x)\psi\left(\frac{1}{x}\right)\right) = x^n f_1\left(\frac{1}{x}\right) = \sum_{i=0}^{n} c_{n-i}x^{n-i}. \end{aligned}$$

Notemos que

$$\begin{aligned} f_1(x)f_2(x) &= \left(x^r\varphi\left(\frac{1}{x}\right)\psi(x))(x^n\left(\frac{1}{x}\right)^r\varphi(x)\psi\left(\frac{1}{x}\right)\right) \\ &= x^n\varphi\left(\frac{1}{x}\right)\psi\left(\frac{1}{x}\right)\varphi(x)\psi(x) \\ &= x^n f\left(\frac{1}{x}\right)f(x) \end{aligned}$$

$$\left(\sum_{i=0}^{n} c_i x^{n-i}\right)\left(\sum_{i=0}^{n} c_{n-i}x^{n-i}\right) = \left(1+\varepsilon_1 x^{n-m}+\varepsilon_2 x^{n-p}+\varepsilon_3 x^n)(x^n+\varepsilon_1 x^m+\varepsilon_2 x^p+\varepsilon_3\right)$$

La comparación de coeficientes de x^{2n} muestra que $c_0c_n = \varepsilon_3$ y por esto $c_0 = \pm 1$ y $c_n = \pm 1$.

Comparando los coeficientes de x^n muestra que

$$\begin{aligned} \sum_{i=0}^{n} c_i^2 &= 1 + \sum_{i=1}^{3}\varepsilon_i^2 = 4 \\ \sum_{i=1}^{n-1} c_i^2 &= 2. \end{aligned}$$

Así, $c_0 = \pm 1$, $c_n = \pm 1$, $c_\alpha = \pm 1$ y $c_\beta = \pm 1$ para algún $1 \le \alpha < \beta \le n-1$, todos los otros coeficientes c_i son cero. Por lo tanto, $f_1(z)f_2(z)$ puede ser expresado de las siguientes dos formas:

$$c_0c_nx^{2n}+c_\alpha c_n x^{2n-\alpha}+c_\beta c_n x^{2n-\beta}+c_0c_\alpha x^{n+\alpha}+c_0c_\beta x^{n+\beta}+c_\alpha c_\beta x^{2n+\beta-\alpha}+4x^n+\cdots \quad (1)$$

$$\varepsilon_3x^{2n}+\varepsilon_2x^{2n-p}+\varepsilon_1x^{2n-m}+\varepsilon_1\varepsilon_3x^{n+m}+\varepsilon_2\varepsilon_3x^{n+p}+\varepsilon_1\varepsilon_2x^{n+m-p}+4x^n+\cdots \quad (2)\,.$$

Con el fin de comparar (1) y (2) se ordenaron los monomios con respecto al tamaño de los grados teniendo en cuenta sólo los tres más altos monomios.

Para (1), obtenemos las cuatro posibilidades:

$$\beta \le \frac{n}{2} \;:\; 2n > 2n-\alpha > 2n-\beta,$$

$$\beta > \frac{n}{2},\ \alpha \leq 2n-\beta :\ 2n > 2n-\alpha \geq n+\beta,$$

$$\beta > \frac{n}{2},\ \frac{n}{2} \geq \alpha > n-\beta\ :\ 2n > n+\beta > 2n-\alpha$$

$$\beta > \frac{n}{2},\ \alpha > \frac{n}{2}\ :\ 2n > n+\beta > n+\alpha$$

Para (2), obtenemos las dos posibilidades:

$$n \geq 2m\ :\ 2n > 2n-p > 2n-m,$$

$$2m > n \geq n+p\ :\ 2n > 2n-p > n+m.$$

Comparando los tres monomios de grados mas altos en (1) y (2) obtenemos para el par $(\alpha,\ \beta)$ las siguientes cuatro posibilidades:

$(\alpha,\ \beta) = (p,\ m),\ (p,\ n-m),\ (m,\ n-p)\ o\ (n-m,\ n-p)$.

Si $(\alpha,\ \beta) = (p,\ m)$ la comparación de (1) con (2) muestra que:

$c_0c_n = \varepsilon_3,\ c_pc_n = \varepsilon_2,\ c_mc_n = \varepsilon_1$.

Por lo tanto

$$f_1(x) = c_n\left(\varepsilon_3 x^n + \varepsilon_2 x^{n-p} + \varepsilon_1 x^{n-m} + 1\right) = c_n x^n f\left(\frac{1}{x}\right).$$

Por lo tanto

$$\varphi(x) = c_0 x^r \varphi\left(\frac{1}{x}\right).$$

Si $(\alpha,\ \beta) =\ (p,\ n-m)$ entonces encontramos en (1) monomios de grados

$$2n,\ 2n-p,\ n+m,\ n+p,\ 2n-m,\ 2n-m-p,\ n$$

y en (2) monomios de grados $2n,\ 2n-p,\ 2n-m,\ n+m,\ n+p,\ n+m-p,\ n$.

Por lo tanto el número $2n-m$ es igual a uno de los tres números $n+m, n+p, n+m-p$. Las igualdades $2n-m-p = n+m$ y $2n-m-p = n+p$ contradicen el supuesto de que $n \leq m+p$ y por lo tanto $2n-m-p = n+m-p$, es decir, $n = 2m$. Por lo tanto $(\alpha,\ \beta) =\ (p,\ m)$.

Si $(\alpha,\ \beta) = (m,\ n-p)$, de manera similar ver que $n = 2m$, es decir,

$(\alpha,\ \beta) = (n-m,\ n-p)$. □

Lema 2.6. Sean λ y λ^{-1} las raíces de $f(x)$. Entonces uno de los siguientes tres pares de condiciones se cumplen:

$$I)\ \lambda^n\ = -\varepsilon_3\ \ y\ \ \lambda^{m-p} = -\varepsilon_1\varepsilon_2,$$

$$II)\ \lambda^m = -\varepsilon_1\varepsilon_3\ \ y\ \ \lambda^{n-p} = -\varepsilon_2$$

$$III)\, \lambda^p = -\varepsilon_2\varepsilon_3 \;\; y \;\; \lambda^{n-m} = -\varepsilon_1$$

Demostración. Las condiciones $f(\lambda) = 0$ y $f(\lambda^{-1}) = 0$ pueden ser expresadas como

$$\lambda^n + \varepsilon_1\lambda^m + \varepsilon_2\lambda^p + \varepsilon_3 = 0, \qquad \lambda^n + \varepsilon_2\varepsilon_3\lambda^{n-p} + \varepsilon_1\varepsilon_2\lambda^{n-m} + \varepsilon_3 = 0.$$

Mediante la sustracción de una ecuación de la otra obtenemos

$$\varepsilon_2\varepsilon_3\lambda^{n-p} + \varepsilon_1\varepsilon_3\lambda^{n-m} - \varepsilon_1\lambda^m - \varepsilon_2\lambda^p = 0,$$

es decir

$$\left(\varepsilon_2\lambda^{m-p} + \varepsilon_1\right)\left(\varepsilon_3\lambda^{n-m} - \varepsilon_1\varepsilon_2\lambda^p\right) = 0$$

y por lo tanto sea $\lambda^p = -\varepsilon_1\varepsilon_2\lambda^m \quad ó \quad \lambda^p = \varepsilon_1\varepsilon_2\varepsilon_3\lambda^{n-m}$. Sustituyendo estos valores de λ^p en la relación $f(\lambda) = 0$ obtenemos ya sea $\lambda^n = \varepsilon$ o

$$\left(\lambda^m + \varepsilon_1\varepsilon_2\right)\left(\lambda^{n-m} - \varepsilon_1\right) = 0.$$

□

Teorema 2.8. *a*) Si el polinomio $f(x)$ no tiene raíces que son raíces de la unidad, entonces $f(x)$ es irreducible.

b) Si el polinomio $f(x)$ tiene exactamente q raíces que son raíces de la unidad, entonces $f(x)$ puede ser representada como el producto de dos polinomios con coeficientes enteros uno de los cuales es de grado q y sus raíces son las raíces dadas de la unidad, mientras que el otro polinomio es irreducible.

Demostración. Sea $f(x) = \varphi(x)\,\psi(x)$, donde φ, $\psi \in \mathbb{Z}[x]$. Podemos suponer que si λ es una raíz de φ, entonces λ^{-1} es también una raíz de φ. Por el Lema 2.6 se sigue que λ es una raíz de la unidad. Si no todas las raíces de f son las raíces de la unidad, entonces ψ es irreducible sobre $\mathbb{Z}$ o $\psi = \psi_1\psi_2$, donde ψ_1, $\psi_2 \in \mathbb{Z}[x]$ y todas las raíces de ψ_1 son las raíces de la unidad mientras que ψ_2 tiene una raíz que no es raíz de la unidad. En este caso todas las raíces de $\varphi\psi_1$ son las raíces de la unidad. Al continuar los mismos argumentos ya aplicados a ψ_2 obtenemos la factorización deseada de f. □

Capítulo 3

Polinomios de una forma particular.

En los polinomios de la forma particular nos enfocaremos a revisar parte de los polinomios simétricos, polinomios de valores enteros, polinomios ciclotómicos y polinomios de Chebyshev, en su debido momento daremos la definición y propiedades que los caracterizan a cada uno.

En matemática, los polinomios de Chebyshev, nombrados en honor a Pafnuti Chebyshev, son una familia de polinomios ortogonales. Usualmente los polinomios de Chebyshev de primer tipo son denotados por T_n. La letra T es usada por la transliteración alternativa del nombre Chebyshev como Tchebychef o Tschebyscheff.

Los polinomios de Chebyshev T_n son polinomios de grado n y la sucesión de polinomios de Chebyshev de cualquier tipo conforma una familia de polinomios.

Los polinomios de Chebyshev son importantes en la teoría de la aproximación porque las raíces de los polinomios de Chebyshev de primer tipo, también llamadas nodos de Chebyshev, son usadas como nodos en interpolación polinómica.

3.1. Polinomios Simétricos.

3.1.1 Ejemplos de polinomios simétricos.

Definición 3.1. Un polinomio $f(x_1,\, x_2, ..., x_n)$ es llamado polinomio simétrico si, para cualquier permutación $\sigma \in S_n$ tenemos que

$$\sigma \circ f\left(x_1,\ x_2, \ldots, x_n\right) = f\left(x_{\sigma(1)}, \ldots,\ x_{\sigma(n)}\right) = f\left(x_1, \ldots,\ x_n\right).$$

.

Ejemplo 3.1. Sea $f(x_1,\, x_2,\, x_3) = x_1^2 x_2 - x_3$ y sean $\rho = (1,3)$ $\sigma = (123)$. Entonces

$$\begin{aligned}\rho \circ f(x_1,\, x_2,\, x_3) &= f(x_{\rho(1)},\, x_{\rho(2)},\, x_{\rho(3)}) \\ &= f(x_3,\, x_2,\, x_1) \\ &= x_3^2 x_2 - x_1\end{aligned}$$

y

$$\begin{aligned}\sigma \circ f(x_1,\, x_2,\, x_3) &= f(x_{\sigma(1)},\, x_{\sigma(2)},\, x_{\sigma(3)}) \\ &= f(x_2,\, x_3,\, x_1) \\ &= x_2^2 x_3 - x_1. \qquad .\end{aligned}$$

Estos polinomios no son simétricos, en cambio estos otros si cumplen con la definición

$f(x_1,\, x_2,\, x_3) = x_1x_2x_3 - 2x_1x_2 - 2x_1x_3 - 2x_2x_3$ y sean $\rho = (31)$ y $\alpha = (231)$.

Entonces

$$\begin{aligned}\rho \circ f(x_1,\, x_2,\, x_3) &= f\left(x_{\rho(1)},\, x_{\rho(2)},\, x_{\rho(3)}\right) \\ &= f\left(x_3,\, x_2,\, x_1\right) \\ &= x_3x_2x_1 - 2x_3x_2 - 2x_3x_1 - 2x_2x_1 \\ &= f(x_1,\, x_2,\, x_3)\end{aligned}$$

y

$$\begin{aligned}\alpha \circ f(x_1,\, x_2,\, x_3) &= f\left(x_{\alpha(1)},\, x_{\alpha(2)},\, x_{\alpha(3)}\right) \\ &= f\left(x_2,\, x_3,\, x_1\right) \\ &= x_2x_3x_1 - 2x_2x_3 - 2x_2x_1 - 2x_3x_1 \\ &= f(x_1,\, x_2,\, x_3). \qquad .\end{aligned}$$

Otros ejemplos de polinomios simétricos son los polinomios simétricos elementales en n variables son la suma de todos los productos posibles de tamaño k; con

$(k = 1,\, 2,\, \ldots,\, n)$ de las variables involucradas. Se acostumbra denotarlos con la letra sigma subindicada:

$$\sigma_k(x_1, ..., x_n) = \sum_{i_1<...<i_k} x_{i_1}...x_{i_k}.$$

Para 2 variables tenemos

$\sigma_1(x_1,\, x_2) = x_1 + x_2$ y $\sigma_2(x_1,\, x_2) = x_1x_2$

y para tres variables tenemos

$\sigma_1(x_1,\, x_2,\, x_3) = x_1 + x_2 + x_3$, $\sigma_2(x_1,\, x_2,\, x_3) = x_1x_2 + x_2x_3 + x_3x_1$ y $\sigma_1(x_1,\, x_2,\, x_3) = x_1x_2x_3$

donde $1 \leq k \leq n$.

En general para n variables tenemos:

$$\begin{aligned}
\sigma_1(x_1, ..., x_n) &= x_1 + x_2 + \cdots + x_n \\
\sigma_2(x_1, ..., x_n) &= x_1x_2 + \cdots + x_1x_n \\
&\vdots \\
\sigma_n(x_1, ..., x_n) &= x_1x_2...x_n.
\end{aligned}$$

Es conveniente establecer que $\sigma_0 = 1$ y $\sigma_k(x_1, ..., x_n) = 0$ para $k > n$.

Si $x_1, ..., x_n$ son las raíces del polinomio $x^n + a_1x^{n-1} + \cdots + a_n$, entonces

$$\sigma_k(x_1, ..., x_n) = (-1)^k a_k.$$

A continuación se ilustra este hecho para el caso cuando $n = 3$, si

$$f(x) = x^3 + a_1x^2 + a_2x + a_3,$$

y x_1, x_2, x_3 son las raíces entonces

$$\begin{aligned}
(x - x_1)(x - x_2)(x - x_3) &= (x^2 - x_1x - x_2x + x_1x_2)(x - x_3) \\
&= x^3 - x_1x^2 - x_2x^2 + x_1x_2x - x_3x^2 + x_1x_3x + x_2x_3x - x_1x_2x_3 \\
&= x^3 - (x_1 + x_2 + x_3)x^2 + (x_1x_2 + x_2x_3 + x_3x_1)x - x_1x_2x_3
\end{aligned}$$

De aquí se puede asignar los valores para cada coeficiente del polinomio, comparándolos con los coeficientes de este nuevo polinomio:

$$\begin{aligned}
\sigma_1(x_1,\, x_2,\, x_3) &= -(x_1 + x_2 + x_3) = (-1)^1 a_1 = -a_1. \\
\sigma_2(x_1,\, x_2,\, x_3) &= (x_1x_2 + x_2x_3 + x_3x_1) = (-1)^2 a_2 = a_2 \\
\sigma_3(x_1,\, x_2,\, x_3) &= -x_1x_2x_3 = (-1)^3 a_3 = -a_3 \\
\\
\Rightarrow \sigma_k(x_1,\, x_2,\, x_3) &= (-1)^k a_k \; para \, k = 1,\, 2,\, 3.
\end{aligned}$$

Esto ocurre cuando hay tres raíces, de manera similar se puede generalizar para cuando hayan n raíces.

Otro ejemplo de polinomios simétricos está dada por los polinomios simétricos homogéneos completos

$$p_k(x_1, ..., x_n) = \sum x_1^{i_1}, ..., x_n^{i_n}$$

Ejemplo 3.2. Sea $P(x_1,\, x_2,\, x_3) = x_1x_2x_3 + x_1^2x_3 + x_2x_3^2 + x_1^2x_2$

Su función generadora es de la forma

$$p(t) = \sum_{k=0}^{\infty} p_k t^k$$

Un ejemplo importante de polinomios simétricos está dada por la suma de potencias

$$s_k(x_1, ..., x_n) = x_1^k + \cdots + x_n^k.$$

La función generadora es de la forma

$$s(t) = \sum_{k=0}^{\infty} s_k t^{k-1}$$

A veces se utilizan monomios simétricos de la siguiente forma

$$m_{i_1 ... i_n}(x_1, ..., x_n) = \sum_{\sigma \in s_n} x_{\sigma(1)}^{i_1} \cdots x_{\sigma(n)}^{i_n}.$$

3.1.2 Más Teoremas sobre polinomios simétricos.

Lema 3.1. Sea $g \in A[x_1, ..., x_n]$. Entonces $g(\sigma_1, ..., \sigma_n) = 0$ si y sólo si $g(x_1, ..., x_n) = 0$.

Demostración. " $\Rightarrow$ " La prueba se hará de por inducción y luego aplicaremos contradicción.

Por inducción sobre n. Si n=1 el resultado es trivial, porque $g(\sigma_1) = 0$ es decir que $\sigma_1 = x_1$ entonces $g(x_1) = 0$. Supongamos que el resultado es cierto para $n-1$ indeterminadas entonces probemos para n indeterminadas y aplicamos contradicción a lo supuesto por inducción entonces tendríamos que se cumple para el caso base y cierto para $n-1$ indeterminadas y por contradicción supongamos que para n es resultado es falso, es decir que $\exists\, g \in A[x_1, ..., x_n]$ tal que $g(\sigma_1, ..., \sigma_n) = 0$ y $g(x_1, ..., x_n) \neq 0$.

Sea g el polinomio de grado mínimo, que cumpla lo anterior y escribimos a g como un polinomio en x_n con coeficientes en $x_1, ..., x_{n-1}$:

$g(x_1, ..., x_n) = g_0(x_1, ..., x_{n-1}) + g_1(x_1, ..., x_{n-1})x_n + \cdots + g_{d-1}(x_1, ..., x_{n-1})x_n^{d-1} + g_d(x_1, ..., x_{n-1})x_n^d.$

Sustituyendo x_i por σ_i en el polinomio g tenemos:

$g(\sigma_1, ..., \sigma_n) = g_0(\sigma_1, ..., \sigma_{n-1}) + g_1(\sigma_1, ..., \sigma_{n-1})x_n + \cdots + g_{d-1}(\sigma_1, ..., \sigma_{n-1})x_n^{d-1} + g_d(\sigma_1, ..., \sigma_{n-1})x_n^d.$

Por hipótesis $g(\sigma_1, ..., \sigma_n) = 0$.

Sustituyendo ahora $x_n = 0$ obtenemos $0 = g_0((\sigma_1)_{x_n=0}, ..., (\sigma_{n-1})_{x_n=0})$. Pero los $(\sigma_i)_{x_n=0}$ son los polinomios simétricos elementales en $x_1, ..., x_{n-1}$. Por inducción

$g_0(x_1, ..., x_{n-1}) = 0$. Ya que $0 = g_0((\sigma_1)_{x_n=0}, ..., (\sigma_{n-1})_{x_n=0})$ podemos escribir $g = f.x_n$ con $f \in A[x_1, ..., x_n]$ y por tanto $f(\sigma_1, ..., \sigma_n)\sigma_n = 0$, luego $f(\sigma_1, ..., \sigma_n) = 0$ y f es de grado estrictamente menor que g, lo cual es imposible, por tanto se cumple la primera implicación.

" $\Leftarrow$ " Es trivial, dado que $g(x_1, ..., x_n) = 0$, es el polinomio nulo, y al evaluar cada σ_i en el polinomio g, siempre genera como resultado 0, es decir $g(\sigma_1, ..., \sigma_n) = 0$. □

Teorema 3.1 (Teorema fundamental de polinomios simétricos). Sea $f(x_1, x_2, ..., x_n)$ un polinomio simétrico, entonces existe un polinomio $g(y_1, y_2, ..., y_n)$ tal que

$$f(x_1, x_2, ..., x_n) = g(\sigma_1, \sigma_2, ..., \sigma_n).$$

Este polinomio g es único.

Demostración. Sea f simétrico, apliquemos el siguiente algoritmo:

1) Seleccionar el monomio $kx_1^{\alpha_1}x_2^{\alpha_2}...x_n^{\alpha_n}$ (algunos α_i pueden ser nulos) que tiene mayor grado en x_1, si todavía hubiera varios escójase entre ellos el de mayor grado en x_2 y si hubiera varios el de mayor grado en x_3, etc. Por la simetría de f se tiene $\alpha_1 \geq \alpha_2 \geq ... \geq \alpha_n$.

2) Sea $f_1 = f - k\sigma_1^{\alpha 1-\alpha 2}\sigma_2^{\alpha 2-\alpha 3}...\sigma_n^{\alpha_n}$. Entonces $f = f_1 + k\sigma_1^{\alpha 1-\alpha 2}\sigma_2^{\alpha 2-\alpha 3}...\sigma_n^{\alpha_n}$ y ahora se repite todo el proceso con f_1 hasta llegar a $f_1 = 0$.

Obsérvese que el monomio seleccionado en 1) no aparece en f_1 y que el algoritmo siempre termina porque al aplicarlo sucesivas veces o bien el grado en x_1 se ha reducido o ha quedado igual, y en este último caso el grado en x_2 se habrá reducido o habrá quedado igual, etc.

Para probar la unicidad, usaremos el lema anterior

Sea $f(x_1, ..., x_n)$ simétrico entonces por teorema existe $g(y_1, ..., y_n)$ tal que

$$f(x_1, x_2, ..., x_n) = g(\sigma_1, \sigma_2, ..., \sigma_n) \qquad (1)$$

y supongamos que existe otro, es decir $g´(y_1, ..., y_n)$ tal que

$$f(x_1, x_2, ..., x_n) = g´(\sigma_1, \sigma_2, ..., \sigma_n) \qquad (2)$$

La diferencia de polinomios simétricos es simétricos, entonces restamos (1) − (2) y obtenemos

$$0 = g(\sigma_1, \sigma_2, ..., \sigma_n) - g´(\sigma_1, \sigma_2, ..., \sigma_n)$$

por lema anterior

$$0 = g(x_1,\, x_2, ..., x_n) - g\,'(x_1,\, x_2, ..., x_n)$$

por tanto

$$g\,'(x_1,\, x_2, ..., x_n) = g(x_1,\, x_2, ..., x_n)$$

. □

Ejemplo 3.3 (Aplicando el algoritmo). Sea el polinomio simétrico

$f(x_1,\, x_2,\, x_3) = (x_1 + x_2)(x_1 + x_3)(x_2 + x_3) = x_1^2x_2 + x_1^2x_3 + 2x_1x_2x_3 + x_2^2x_1 + x_2^2x_3 + x_3^2x_1 + x_3^2x_2$

Elegimos el monomio que tenga mayor exponente en x_1 y como hay dos monomios $x_1^2x_2$ y $x_1^2x_3$ elegimos entre estos el que tenga mayor grado en x_2 y así sucesivamente. Entonces el monomio sería $x_1^2x_2x_3^0$, y sus exponentes $\alpha_1 = 2 \geq \alpha_2 = 1 \geq \alpha_3 = 0$.

Luego:

$f_1 = f - \sigma_1^{2-1}\sigma_2^{1-0}\sigma_3^0 \Rightarrow f_1 = f - (x_1+x_2+x_3)(x_1x_2+x_1x_3+x_2x_3) = -x_1x_2x_3$ entonces $f = f_1 + (x_1+x_2+x_3)(x_1x_2+x_1x_3+x_2x_3)$, ahora aplicamos el mismo proceso para f_1 y se toma el único monomio que existe con sus exponentes $\alpha_1 = 1 \geq \alpha_2 = 1 \geq \alpha_3 = 1$

$$f_2 = f_1 - (-1)\sigma_1^{1-1}\sigma_2^{1-1}\sigma_3^1) \Rightarrow f_2 = f_1 + x_1x_2x_3 = 0. \quad Así \quad f_1 = f_2 - x_1x_2x_3.$$

Al formar el polinomio $f = f_2 - x_1x_2x_3 + (x_1 + x_2 + x_3)(x_1x_2 + x_1x_3 + x_2x_3) = (x_1 + x_2 + x_3)(x_1x_2 + x_1x_3 + x_2x_3) - x_1x_2x_3 = \sigma_1\sigma_2 - \sigma_3; \quad f = \sigma_1\sigma_2 - \sigma_3$

A partir de la demostración del teorema anterior se tiene que, si $f(x_1, ..., x_n)$ es un polinomio simétrico con coeficientes enteros, entonces $f(x_1, ..., x_n) = g(\sigma_1, ..., \sigma_n)$, donde los coeficientes de g también son números enteros. Para polinomios simétricos homogéneos completos p_1, ..., p_k se puede obtener un algoritmo similar en términos de σ_k esto se puede hacer análogo a la demostración del teorema anterior.

En cuanto a las sumas de las potencias, una expresión de la forma $f(x_1, ..., x_n) = g(s_1, ..., s_n)$ también existe, pero los coeficientes de g ahora no son números enteros. Por ejemplo,

$$x_1x_2 = \frac{(x_1 + x_2)^2 - (x_1^2 + x_2^2)}{2} = \frac{s_1^2 - s_2}{2}.$$

El teorema principal de polinomios simétricos implica que, si $x_1, ..., x_n$ son las raíces del polinomio

$$f(x) = x^n + a_1x^{n-1} + \cdots + a_n,$$

así D se define como una cantidad numérica,

$$D = \prod_{i<j}(x_i - x_j)^2.$$

Ya que está representada a través de las raíces $x_1, ..., x_n$ del polinomio simétrico f, esto puede ser expresado polinómicamente en términos de un $a_1, ..., a_n$. Esta cantidad se llama el discriminante de f.

Definición 3.2. Un polinomio $f(x_1,\ x_2, ..., x_n)$ es llamado simétrico-oblicuo sí

$$f(..., x_i, ..., x_j, ...) = -f(..., x_j, ..., x_i, ...),$$

es decir, bajo la transposición de cualquiera de dos indeterminadas x_i y x_j se cambia su signo, el polinomio

$$\triangle(x_1,\ x_2, ..., x_n) = \prod_{i<j}(x_i - x_j)$$

es un ejemplo de un polinomio simétrico-oblicuo.

Ejemplo 3.4. El polinomio $P(x_1,\ x_2,\ x_3) = x_1^2(x_2 - x_3) + x_2^2(x_3 - x_1) + x_3^2(x_1 - x_2)$, es simétrico-oblicuo

Demostración. Nótese que al intercambiar cualquier par de variables, el polinomio P altera su signo.

Es decir $P(x_1,\ x_2,\ x_3) = -P(x_2,\ x_1,\ x_3)$. Así el polinomio es simétrico-oblicuo de grado 3. Además, para $x_1 = x_2$ se tiene $P(x_1,\ x_2,\ x_3) = 0$ entonces $(x_1 - x_2)$ es un factor de $P(x_1,\ x_2,\ x_3)$. Análogamente, $(x_2 - x_3)$, $(x_3 - x_1)$ son factores de P. □

Teorema 3.2 Cualquier polinomio simétrico-oblicuo $f(x_1,\ x_2, ..., x_n)$ puede representarse de la forma

$$\triangle(x_1,\ x_2, ..., x_n).g(x_1,\ x_2, ..., x_n)$$

donde g es un polinomio simétrico.

Demostración. Basta con comprobar que f es divisible por Δ. En efecto, si $\frac{f}{\Delta}$ es un polinomio, entonces este polinomio es simétrico, dado que f y $\triangle$ son simétricos y la división de simétricos es simétricos, mostremos por ejemplo que f es divisible por $x_1 - x_2$. Hacemos el cambio de variables $x_1 = u + v, \quad x_2 = u - v$. Como resultado obtenemos

$$f(x_1,\, x_2,\, x_3,\, ...,\, x_n) = f_1(u,\, v\,, x_3,\, ...,\, x_n).$$

Si $x_1 = x_2$, entonces $u = 0$ y por lo tanto $f_1(0, v, x_3, ..., x_n) = 0$. Esto significa que f_1 es divisible por u, es decir, f es divisible por $x_1 - x_2$. Similar probaremos que f es divisible por $x_i - x_j$ para todo $i < j$. □

3.2. Polinomios de valores enteros.

3.2.1 Una base en el espacio de polinomios de valores enteros.

Definición 3.3. El polinomio $p(x)$ es llamado valor-entero si x, toma valores enteros y al evaluarlo genera un número entero.

Definición 3.4. Para cualquier número real x y cualquier número natural k definimos el coeficiente binomial generalizado $\begin{pmatrix} x \\ k \end{pmatrix}$ por

$$\begin{pmatrix} x \\ k \end{pmatrix} = \frac{x(x-1)(x-2)...(x-k+1)}{k!}$$

Y además

$$\begin{pmatrix} n+1 \\ k+1 \end{pmatrix} = \begin{pmatrix} n \\ k \end{pmatrix} + \begin{pmatrix} n \\ k+1 \end{pmatrix}$$

La demostración de esta propiedad de combinatorio se realiza de la siguiente forma: Supongamos que $A = \{a_1,\, a_2, ..., a_n,\, a_{n+1}\}$ es un conjunto de cardinal $n+1$, y queremos ver cuántos subconjuntos de $k+1$ elementos tiene.

Si queremos elegir un subconjunto X de A con $k+1$ elementos, tenemos dos opciones, mutuamente excluyentes: que $a_{n+1} \in X$ o que $a_{n+1} \notin X$. En el primer caso, está determinado por los k elementos de $\{a_1,\, a_2, ..., a_n,\, a_n\}$ que pertenecen a X. Podemos entonces elegir un total de $\begin{pmatrix} n \\ k \end{pmatrix}$ subconjuntos con estas condiciones. En el segundo caso, está determinado por los $k+1$ elementos que pertenecen a él, y que sabemos con seguridad que están en el conjunto $\{a_1,\, a_2, ..., a_n\}$. Podemos por tanto hacer la

elección de $\begin{pmatrix} n \\ k+1 \end{pmatrix}$formas. El principio de la suma nos asegura entonces que:

$$\begin{pmatrix} n+1 \\ k+1 \end{pmatrix} = \begin{pmatrix} n \\ k \end{pmatrix} + \begin{pmatrix} n \\ k+1 \end{pmatrix},$$

como se quería demostrar.

Teorema 3.3 Sea p_k un polinomio de grado k tomando valores enteros para $x = n$, $n+1$, $...\, n+k$ donde n es un número entero. Entonces

$$p_k(x) \;=\; c_0 \begin{pmatrix} x \\ k \end{pmatrix} + c_1 \begin{pmatrix} x \\ k-1 \end{pmatrix} + c_2 \begin{pmatrix} x \\ k-2 \end{pmatrix} + ... + c_k,$$

donde c_0, c_1, ... , c_k son enteros.

Demostración. Los polinomios

$$\begin{pmatrix} x \\ 0 \end{pmatrix} = 1, \quad \begin{pmatrix} x \\ 1 \end{pmatrix} = x, \quad \begin{pmatrix} x \\ 2 \end{pmatrix} = \frac{x^2}{2} - \frac{x}{2}, \quad ..., \quad \begin{pmatrix} x \\ k \end{pmatrix} = \frac{x^k}{k!} + ...$$

forman una base en el espacio de los polinomios de grado no mayor que k, y por lo tanto

$$p_k(x) = c_0 \begin{pmatrix} x \\ k \end{pmatrix} + c_1 \begin{pmatrix} x \\ k-1 \end{pmatrix} + ... + c_k$$

donde c_0, c_1, ..., c_k son algunos números. Sólo queda probar que todos los números son enteros.

Por inducción sobre k. Para $k = 0$, el polinomio $p_0(x) = c_0$ asume un valor entero en $x = n$, para cualquier n, y así c_0 es un número entero. Supongamos ahora que el enunciado es cierto para todos los polinomios de grado no mayor que k. Sea el polinomio

$$p_{k+1}(x) = c_0 \begin{pmatrix} x \\ k+1 \end{pmatrix} + ... + c_{k+1}$$

toma valores enteros en $x = n$ para cualquier n, $n+1$,..., $n+k+1$. Entonces el polinomio

$$\triangle p_{k+1}(x) = p_{k+1}(x+1) - p_{k+1}(x) = c_0 \begin{pmatrix} x \\ k \end{pmatrix} + c_1 \begin{pmatrix} x \\ k-1 \end{pmatrix} + ... + c_k.$$

Toma valores enteros en $x = n,\ n+1,\ ...,\ n+k$. Por lo tanto $c_0,\ c_1,\ c_2,\ ...,\ c_k$ son enteros y por lo tanto también lo es

$$c_{k+1} = p_{k+1}(n) - c_0 \begin{pmatrix} n \\ k+1 \end{pmatrix} - c_1 \begin{pmatrix} n \\ k \end{pmatrix} - ... - c_k \begin{pmatrix} n \\ 1 \end{pmatrix}.$$

□

Teorema 3.4. Sea $R(x)$ una función racional que toma valores enteros para todo número entero x. Entonces, $R(x)$ es un polinomio de valores enteros.

Demostración. Podemos escribir a $R(x) = \frac{f(x)}{g(x)}$, donde f y g son polinomios. Habiendo dividido f por g nos quedaría un residuo, que lo podemos ver de la forma

$$R(x) = p_k(x) + r(x)$$

donde $p_k(x)$ es un polinomio de grado k y $r(x) \to 0$ cuando $x \to \infty$. Por lo tanto, para valores grandes de n, el valor difiere en $p_k(n)$, en los números enteros. Mostremos que $p_k(x)$ es un polinomio de valor entero. Esto se realiza casi como el mismo argumento que se uso en la prueba del teorema anterior.

Expresemos a $p_k(x)$ de la forma

$$p_k(x) = c_0 \begin{pmatrix} x \\ k \end{pmatrix} + ... + c_k.$$

Para $k = 0$, el número c_0 es un número entero.

El polinomio

$$\triangle p_k(x) = p_k(x+1) - p_k(x) = c_0 \begin{pmatrix} x \\ k-1 \end{pmatrix} + ... + c_{k-1}.$$

Asumimos también valores enteros para los x grandes y si el grado es igual $k-1$, aplicamos la hipótesis inductiva para poder ver que $c_0,\ c_1,\ c_2,\ ...,\ c_{k-1}$ son enteros, es claro que el número

$$c_k = p_k(n) - c_0 \begin{pmatrix} n \\ k \end{pmatrix} - ... - c_{k-1} \begin{pmatrix} n \\ 1 \end{pmatrix},$$

es entero. Así queda por demostrar que $r(x) = 0$. Como ya sabemos $r(n) \in \mathbb{Z}$ para $n \in \mathbb{Z}$ y $r(n) \to 0$ cuando $n \to \infty$. Por lo tanto $r(n) = 0$ para todos los n suficientemente grandes. Pero toda función racional con una infinidad de ceros es idénticamente cero. □

3.2.2 Polinomios de valores enteros en varias variables.

Teorema 3.5. El polinomio $p_{d_1,...,d_n}(x_1, ..., x_n)$ de grado d_i con respecto a x_i toma valores enteros para $x_1 = a_1$, $a_1 + 1$,..., $a_1 + d_1$,..., $x_n = a_n$, $a_n + 1$,..., $a_n + d_n$ si y solo sí

$$p_{d_1,...,d_n}(x_1, ..., x_n) = \sum c_{k_1}...c_{k_n} \begin{pmatrix} x_1 \\ k_1 \end{pmatrix} ... \begin{pmatrix} x_n \\ k_n \end{pmatrix},$$

donde $c_{k_1}...{}_{k_n}$ son enteros. En particular, tal polinomio asume valores enteros en todos los puntos enteros $(x_1, ..., x_n)$.

Demostración. Consideremos el caso cuando $n = 2$, ya que el caso general es similar. Para un fijo $x_1 \in \{a_1, ..., a_1 + d_1\}$, el polinomio $p_{d_1 d_2}(x_1, x_2)$ toma valores enteros para $x_2 = a_2$, ..., $a_2 + d_2$. Por tanto por el teorema 3.4 para $x_1 = a_1, ..., a_1 + d_1$, tenemos la identidad

$$p_{d_1 d_2}(x_1, x_2) = \sum_{k_2=0}^{d_2} c_{k_2}(x_1) \begin{pmatrix} x_2 \\ k_2 \end{pmatrix}, \qquad (1)$$

donde $c_{k_2}(a_1)$, ..., $c_{k_2}(a_1 + d_1)$ son enteros. Si ahora consideramos la relación (1) para el polinomio con las variables x_1 y x_2, entonces es claro que $c_{k_2}(x_1)$ es un polinomio de forma única. Así hemos demostrado que este polinomio (de grado no mayor que d_1) asume valores enteros para $x_1 = a_1$, ..., $a_1 + d_1$ como se quería demostrar. □

3.3. Polinomios Ciclotómicos.

3.3.1 Definición y propiedades de polinomios ciclotómicos.

Definición 3.5. Las raíces $n - ésimas$ de la unidad son los números complejos z que verifican $z^n = 1$, es decir, los números complejos de la forma: $\varepsilon_n^k = e^{\frac{2\pi ik}{n}}$. De esta manera tenemos una descomposición en $\mathbb{C}[X]$:

$$x^n - 1 = \prod (x - \varepsilon_n^k)$$

Definición 3.6. Una raíz $n - ésima$ de la unidad puede ser raíz $m - ésima$ de la unidad para algún m divisor de n. Las raíces primitivas $n - ésimas$ de la unidad son aquellas tales que el mínimo entero positivo para el que $z^m = 1$ es n. Equivalentemente, son los números complejos de la forma:

$$\varepsilon_n^k = e^{\frac{2\pi ik}{n}}, \quad \text{con}(k,\, n) = 1.$$

Definición 3.7. El polinomio ciclotómico $n - ésimo$ es el polinomio mónico cuyas raíces son las raíces primitivas de la unidad, es decir:

$\phi_n(x) = \prod(x - \varepsilon_n^k)$ donde $\varepsilon_n^k = e^{\frac{2\pi ik}{n}}$

Además $\varepsilon_n^1,\ \varepsilon_n^2,\ ...\varepsilon_n^{\rho(n)}$ son las n raíces primitivas de la unidad y el grado del polinomio ciclótomico lo define la función $\varphi(n)$. Recordar que la función $\varphi(n) = \#\{(k, n) = 1 \text{ con } k \in \mathbb{N} \ \wedge \ k \leq n\}$. Conocida como "la función de Euler".

Para cada raíz $n-ésima$ de la unidad ε_n^k existe un entero positivo mínimo m, divisor de n, para el que $(\varepsilon_n^k)^m = 1$ (exactamente $m = n/(k;\, n)$), de manera que esa raíz será raíz $m - ésima$ primitiva de la unidad. Clasificar las raíces $n - ésimas$ de la unidad según este valor m es equivalente a la descomposición:

$$x^n - 1 = \prod_{m/n} \phi_m(x),$$

de manera que,

$$\phi_n(x) = \frac{x^n - 1}{\prod_{m/n,\ m<n} \phi_m(x)} \qquad (1)$$

A continuación se ilustran los primeros 6 polinomios ciclotómicos.

$\phi_1(x) = x - 1.$

$\phi_2(x) = \frac{x^2-1}{\phi_1(x)} = \frac{x^2-1}{x-1} = x + 1.$

$\phi_3(x) = \frac{x^3-1}{\phi_1(x)} = \frac{x^3-1}{x-1} = x^2 + x + 1.$

$\phi_4(x) = \frac{x^4-1}{\phi_1(x)\phi_2(x)} = \frac{x^4-1}{(x-1)(x+1)} = \frac{(x^2-1)(x^2+1)}{(x^2-1)} = x^2 + 1.$

$\phi_5(x) = \frac{x^5-1}{\phi_1(x)} = \frac{x^5-1}{x-1} = x^4 + x^3 + x^2 + x + 1.$

$\phi_6(x) = \frac{x^6-1}{\phi_1(x)\phi_2(x)\phi_3(x)} = \frac{x^6-1}{(x^3-1)(x+1)} = \frac{(x^3-1)(x^3+1)}{(x^3-1)(x+1)} = x^2 - x + 1$

Observación: El grado del polinomio ciclotómico $\phi_m(x)$ no es m.

Teorema 3.6 Sea $n > 1$ impar. Entonces

$$\phi_{2n}(x) = \phi_n(-x)$$

Demostración. Se usará el método de inducción pero antes de usarlo clasifiquemos los divisores de $2n$ en dos conjuntos S_1 y S_2; donde S_1 es el conjunto de todos los divisores impares (que son todos los divisores de n) y S_2 es el conjunto de los divisores pares (que son de la forma $2d$ donde d es divisor de n).

Por (1) tenemos que

$$x^{2n}-1=\prod_{d\in S_1}\phi_d(x)\prod_{d\in S_2}\phi_d(x)=(x^n-1)\prod_{d\in S_2}\phi_d(x)$$

Dividiendo por (x^n-1) tenemos:

$$x^n+1=\prod_{k/n}\phi_{2k}(x)$$

Luego sustituimos x por $-y$, y multiplicamos por -1 ambos lados de la igualdad.

Dado que n es impar entonces

$$y^n-1=-\prod_{k/n}\phi_{2k}(-y)$$

Del término de la derecha lo expandimos, dado que los divisores de n, son: $1,\ k_1,\ k_2, ..., k_n,\ n$

$$y^n-1=-\left(\phi_2(-y)\phi_{2k_1}(-y)\phi_{2k_2}(-y)...\phi_{2k_n}(-y)\phi_{2n}(-y)\right)$$

Un caso particular para $\phi_2(-y)$=$-y+1$=$-(y-1)$=-$\phi_1(y)$ y sustituimos

$$y^n-1=\left(\phi_1(y)\phi_{2k_1}(-y)\phi_{2k_2}(-y)...\phi_{2k_n}(-y)\phi_{2n}(-y)\right)$$

Ahora por inducción supongamos cierto el teorema para $k_i<n$ es decir que $\phi_{2k_i}(-y)=\phi_{k_i}(y)$.

Sustituyendo tenemos

$$\begin{aligned} y^n-1 &= \left(\phi_1(y)\phi_{k_1}(y)\phi_{k_2}(y)...\phi_{k_n}(y)\phi_{2n}(-y)\right)\\ y^n-1 &= \prod_{k/n,\,k<n}\phi_k(y)\phi_{2n}(-y)\\ \frac{y^n-1}{\prod_{k/n,\,k<n}\phi_k(y)} &= \phi_{2n}(-y)\end{aligned}$$

Por tanto

$\phi_n(y)=\phi_{2n}(-y)\Rightarrow\phi_n(-x)=\phi_{2n}(x)$ así queda demostrado el teorema. □

Ejemplo 3.5. Para $n=3$, tenemos que

$\phi_3(-x)=\frac{(-x)^3-1}{\phi_1(-x)}=\frac{-x^3-1}{-x-1}=x^2-x+1$, y

$\phi_6(x)=\frac{x^6-1}{\phi_1(x)\phi_2(x)\phi_3(x)}=\frac{x^6-1}{(x^3-1)(x+1)}=\frac{(x^3-1)(x^3+1)}{(x^3-1)(x+1)}=x^2-x+1$

Por tanto $\phi_6(x)=\phi_3(-x)$

3.4. Polinomios de Chebyshev

3.4.1 Definición y más propiedades de los polinomios de Chebyshev.

Los polinomios de Chebyshev $T_n(x)$ constituyen una de las familias más importantes de los polinomios. Y a menudo aparecen en diversas ramas de las matemáticas para la aproximación de funciones o polinomios.

Se discutirán varias propiedades importantes de Polinomios de Chebyshev.

Definiremos los polinomios de Chebyshev a todos los que cumplen la condición que $\cos(n\rho)$ es un polinomio expresado en términos de $\cos(\rho)$ es decir, existe un polinomio $T_n(x)$ tal que

$$T_n(x) = \cos(n\rho) \ para \ x = \cos(\rho).$$

De hecho, lo anterior se deduce de la fórmula $T_n(x) = \cos(\cos^{-1}(nx))$ y de la siguiente identidad trigonométrica

$$\cos(n+1)\rho + \cos(n-1)\rho = 2\cos\rho\cos(n\rho).$$

muestra que los polinomios de Chebyshev $T_n(x)$ están definidos de forma recursiva por la relación

$$\begin{aligned} T_0(x) &= 1 \\ T_1(x) &= x \\ T_{n+1}(x) &= 2xT_n(x) - T_{n-1}(x) \end{aligned}$$

El hecho que $T_n(x) = \cos(n\rho) \quad para \quad x = \cos\rho$ quiere decir que $|T_n(x)| \leq 1$ para $x \leq 1$. La recurrencia anterior implica que

$$T_n(x) = 2^{n-1}x^n + a_1x^{n-1} + \cdots + a_n, \qquad (*)$$

donde a_1, a_2, ..., a_n son enteros.

Las propiedades más importantes de los polinomios de Chebyshev son las siguientes.

Teorema 3.7. Sea $P_n(x) = x^n + a_1x^{n-1} + \cdots + a_n$ un polinomio mónico de grado n, tal que $|P_n(x)| \leq \frac{1}{2^{n-1}}$ para $|x| \leq 1$. Entonces $P_n(x) = \frac{T_n(x)}{2^{n-1}}$. En otras palabras el polinomio $\frac{T_n(x)}{2^{n-1}}$ es el polinomio mónico de grado n que tiene la menor derivación de ceros en el intervalo $[-1, 1]$.

Demostración. Usaremos la propiedad del polinomio $(*)$, sabiendo que el factor,

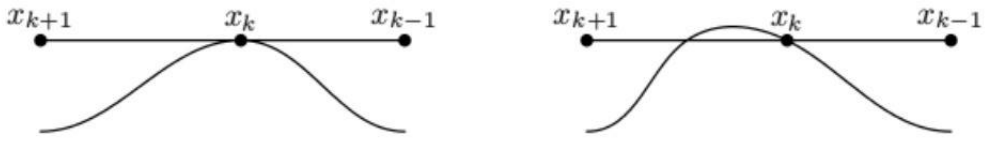
$$T_n\left(\cos\left(\frac{k\pi}{n}\right)\right) = \cos(k\pi) = (-1)^k \ para \ k = 0, 1, ..., n.$$

Considerar el polinomio

$$Q(x) = \frac{1}{2^{n-1}} T_n(x) - P_n(x).$$

Su grado no excede a $n-1$ ya que los principales términos de $\frac{1}{2^{n-1}} T_n(x)$ y $P_n(x)$ son iguales.

Dado que $|P_n(x)| \leq \frac{1}{2^{n-1}}$ para $|x| \leq 1$, se deduce que en el punto $x_k = \cos(\frac{kx}{n})$ y el signo de $Q(x_k)$ coincide con el signo de $T_n(x_k)$. Por lo tanto, en los puntos extremos de cada segmento $[x_{k+1},\ x_k]$, el polinomio $Q(x)$ toma valores de signos opuestos, y por lo tanto $Q(x)$ tiene una raíz en cada uno de estos segmentos.



Si $Q(x_k) = 0$, se necesita un poco más de argumentos. En este caso, ya sea x_k una raíz doble o dentro de uno de los segmentos $[x_{k+1},\ x_k]$ o $[x_k,\ x_{k-1}]$ es la misma raíz. Esto se deduce del hecho que al evaluar x_{k+1} y x_{k-1} en el polinomio $Q(x)$ tienen el mismo signo según la figura anterior.

El número de segmentos de $[x_{k+1},\ x_k]$ es igual a n, y por lo tanto el polinomio $Q(x)$ tiene al menos n raíces. Para un polinomio de grado no mayor que $n-1$, esto significa que es idénticamente cero, es decir, $P_n(x) = \frac{1}{2^{n-1}} T_n(x)$, así queda demostrado el teorema. □

Si $z = \cos\rho + i\sin\rho$, entonces $z + z^{-1} = 2\cos\rho$, ya que $z = \cos\rho + i\sin\rho = e^{i\rho}$ de donde $z^{-1} = e^{-i\rho} = \cos\rho - i\sin\rho$ y luego al realizar la suma de $z \quad y \quad z^{-1}$ obtenemos que $z + z^{-1} = 2\cos\rho$. Así podemos generalizarlo para n tenemos que $z^n = \cos(n\rho) + i\sin(n\rho) = e^{ni\rho}$ y si $z^{-n} = \cos(n\rho) - i\sin(n\rho) = e^{-ni\rho}$ obtenemos que $z^n + z^{-n} = 2\cos(n\rho)$

Por lo tanto

$$T_n\left(\frac{z + z^{-1}}{2}\right) = \frac{z^n + z^{-n}}{2}.$$

Usando esta propiedad se puede probar la siguiente teorema.

Teorema 3.8. Sea $m = \left[\frac{n}{2}\right]$. Entonces

$$T_n(x) = \sum_{j=0}^{m} \binom{n}{2j} x^{n-2j} \left(x^2 - 1\right)^j$$

Demostración. Sea $x = \frac{1}{2}(z + z^{-1})$ y $y = \frac{1}{2}(z - z^{-1})$, así $x^2 = \frac{1}{4}(z^2 + 2zz^{-1} + z^{-2})$ y $y^2 = \frac{1}{4}(z^2 - 2zz^{-1} + z^{-2})$ entonces

$$y^2 - x^2 = -1 \Rightarrow y^2 = x^2 - 1$$

y

$$\begin{aligned}
z^n + z^{-n} &= (x+y)^n + (x-y)^n \\
&= x^n + \binom{n}{n-1} x^{n-1}y + \binom{n}{n-2} x^{n-2}y^2 + ... + \binom{n}{1} y^{n-1}x + y^n \\
&\quad + x^n - \binom{n}{n-1} x^{n-1}y + \binom{n}{n-2} x^{n-2}y^2 - ... + \binom{n}{1} y^{n-1}x - y^n \\
&= 2x^n + 0x^{n-1}y + 2\binom{n}{n-2} x^{n-2}y^2 + ... + 2\binom{n}{1} xy^{n-1} + 0y^n \\
&= (1+(-1)^0)\binom{n}{n} x^n + (1+(-1)^1)x^{n-1}y + (1+(-1)^2)\binom{n}{n-2} x^{n-2}y^2 + \\
&\quad ... + (1+(-1)^{n-1})\binom{n}{1} xy^{n-1} \\
&= \sum_{i=0}^{n} \binom{n}{i} (1+(-1)^i) x^{n-i}y^i,
\end{aligned}$$

por hipótesis $m = \left[\frac{n}{2}\right]$ entonces i tomará valores de la forma $2j$, entonces

$$\begin{aligned}
z^n + z^{-n} &= \sum_{j=0}^{m} \binom{n}{2j} (1+(-1)^{2j}) x^{n-2j}y^{2j} \\
&= 2\sum_{j=0}^{m} \binom{n}{2j} x^{n-2j}(x^2-1)^j
\end{aligned}$$

Sólo resta observar que

$$T_n(x) = \frac{1}{2}(z^n + z^{-n}).$$

□

Corolario 3.1. Sea p un primo impar. Entonces

$$T_p(x) \equiv T_1(x) \,(mod\, p)\,.$$

Demostración. Sea $p = 2m + 1$. Entonces

$$T_p(x) = \sum_{j=0}^{m} \begin{pmatrix} p \\ 2j \end{pmatrix} x^{p-2j} \left(x^2 - 1\right)^j .$$

Si $j > 0$, entonces $\begin{pmatrix} p \\ 2j \end{pmatrix}$ es divisible por p. Por lo tanto

$$T_p(x) = x^p (mod\, p) \equiv x (mod\, p) = T_1(x).$$

□

Para cualquier par de polinomios P, Q se puede definir la composición natural así

$$P \circ Q(x) = P(Q(x)).$$

El polinomio P y Q se dice que conmutan si $P \circ Q = Q \circ P$ es decir que.

$$P(Q(x)) = Q(P(x))$$

Teorema 3.9. Los polinomios $T_n(x)$ *y* $T_m(x)$ conmutan.

Demostración. Sea $x = \cos\rho$. Entonces $T_n(x) = \cos(n\rho) = y$ y $T_m(y) = \cos(m\rho)$. Por lo tanto $T_m(T_n(x)) = \cos(mn\rho)$. Similarmente, $T_n(T_m(x)) = \cos(mn\rho)$. Por lo tanto la identidad $T_m(T_n(x)) = T_n(T_m(x))$ para $|x| < 1$ y por lo tanto cumple para todo x. □

Los polinomios de Chebyshev son el único ejemplo no trivial de polinomios conmutativos. De hecho, el siguiente teorema hace una clasificación de los polinomios pares que conmutan. Sea $l(x) = ax + b$, donde a, $b \in \mathbb{C}$ y $a \neq 0$. Diremos que el par de polinomios $l \circ f \circ l^{-1}$ y $l \circ g \circ l^{-1}$ son equivalentes al par de polinomios f y g.

Teorema 3.10 Si ambos α y $\cos(\alpha\pi)$ son racionales, entonces $2\cos(\alpha\pi)$ es un entero, es decir $\cos(\alpha\pi) = 0, \pm\frac{1}{2}$ *ó* ± 1.

Demostración. Sea $\alpha = \frac{m}{n}$ una fracción irreducible y $x_0 = 2\cos(t)$, donde $t = \alpha\pi$. Entonces:

$$P_n(x_0) = 2\cos(nt) = 2\cos(n\alpha\pi) = 2\cos(m\pi) = \pm 2$$

.

Por lo tanto x_0 es una raíz del polinomio con coeficientes enteros

$$P_n(x) \mp 2 = x^n + b_1 x^{n-1} + ... + b_n.$$

Sea $x_0 = 2\cos(\alpha\pi) = \frac{p}{q}$ será una fracción irreducible. Entonces

$$p^n + b_1 p^{n-1} q + ... + b_n q^n = 0,$$

y por lo tanto p^n es divisible por q. Pero $p\, y\, q$ son primos relativos, y así $q = \pm 1$, es decir $2\cos(\alpha\pi)$ es un entero. □

3.4.2 Polinomios Ortogonales.

Los polinomios $f_k(x),\ k = 0, 1, ...$ se dice que son polinomios ortogonales en el intervalo $[a, b]$ con la función de peso $\omega(x) \geq 0$ si $f_k(x) = k$ y

$$\int_a^b f_m(x) f_n(x) \omega(x) dx = 0$$

para $m \neq n$.

En el espacio V^{n+1} de los polinomios de grado $\leq n$, definimos el producto interior por:

$$(f,\ g) = \int_a^b f(x) f(x) \omega(x) dx.$$

Los polinomios ortogonales $f_0,\ f_1,\ ...,\ f_n$ forman una base ortogonal en el espacio V^{n+1} con el producto interior.

Teorema 3.11. Los polinomios de chebyshev forman un sistema ortogonal sobre el intervalo $[-1,\ 1]$ con función de peso $\omega(x) = \frac{1}{\sqrt{1-x^2}}$

Demostración. Haciendo un cambio de variable $x = \cos\rho$, tenemos y haremos uso de la fórmula $cos(n\rho + m\rho) = cos(n\rho)cos(m\rho) - sen(n\rho)sen(m\rho)$ y
$cos(n\rho - m\rho) = cos(n\rho)cos(m\rho) + sen(n\rho)sen(m\rho)$

$$\begin{aligned} \int_{-1}^{1} T_n(x) T_m(x) \frac{dx}{\sqrt{1-x^2}} &= \int_0^{\pi} \cos(n\rho)\cos(m\rho) d\rho \\ &= \int_0^{\pi} \frac{\cos((n+m)\rho) + \cos((m-n)\rho)}{2} d\rho. \end{aligned}$$

Queda por observar que

$\int_0^\pi \cos(k\rho)d\rho = 0 \quad si \quad k \neq 0.$ □

Teorema 3.12 Los polinomios de Chebyshev pueden ser definidos desde la fórmula

$$T_n(x) = \frac{(-1)^n\sqrt{1-x^2}}{1.3.5...(2n-1)}\frac{d^n}{dx^n}(1-x^2)^{n-1/2}.$$

Demostración. Por inducción sobre m se puede demostrar fácilmente que para $m \leq n$

$$\frac{d^m}{dx^m}(1-x^2)^{n-1/2} = P_m(x)(1-x^2)^{n-m-1/2}$$

donde $P_m(x)$ es un polinomio de grado m tal que

$$\begin{aligned} P_0(x) &= 1 \\ P_1(x) &= -(2n-1)x, \\ &\vdots \\ P_{m+1} &= 1-x^2-(2n-2m-1)xP_m(x) \ para \ m \geq 1. \end{aligned}$$

Por lo tanto

$$\sqrt{1-x^2}\frac{d^n}{dx^n}(1-x^2)^{n-1/2} = P_n(x)$$

es un polinomio de grado n.

Se verificará que $P_n(x) = \lambda T_n(x)$, es decir

$$\int_{-1}^{1} x^k \frac{d^n}{dx^n}(1-x^2)^{n-1/2}dx = 0$$

para $k = 0, 1, ..., n-1$. Integrando por partes tenemos que

$\int_{-1}^{1} x^k \frac{d^n}{dx^n}(1-x^2)^{n-1/2}dx = x^k P_n(x)(1-x^2)^{n-1/2} \mid_{-1}^{1} - \int_{-1}^{1} kx^{k-1}\frac{d^{n-1}}{dx^{n-1}}(1-x^2)^{n-1/2}dx.$

El primer término de la derecha desaparece puesto que $1-x^2 = 0 \ \ en \ \ x = \pm 1$. Luego integramos por partes el término y repetimos el proceso. Con el fin de obtener 0 al final, tenemos que integrar por partes $k+1$ veces. En el último paso obtenemos la derivada $\frac{d^{n-k-1}}{dx^{n-k-1}}$. Esto significa que $n-k-1$ en caso de ser no negativo, es decir $k \leq n-1$.

Queda verificar que $\lambda = (-1)^n 1.3.5...(2n-1)$. La recurrencia

$$P_{m+1}(x) = 1-x^2-(2n-2m-1)xP_m(x)$$

Toma la forma

$$P_{m+1}(1) = -(2n - 2m - 1)P_m(1)$$

Por lo tanto $P_n(1) = (-1)^n 1.3.5...(2n-1)$. También es claro que $T_n(1) = 1$. Así queda demostrado el teorema. □

3.4.3 Desigualdades de los polinomios de Chebyshev.

Teorema 3.13. Sea el polinomio $p(x) = a_0 + a_1 x + \cdots + a_n x^n$, donde $a_i \in \mathbb{C}$ tal que $|p(x)| \leq 1$ para $-1 \leq x \leq 1$. Entonces $\left|p^{(k)}(x)\right| \leq \left|T_n^{(k)}(x)\right|$ para $|x| \geq 1$, $x \in \mathbb{R}$.

Demostración. Se utilizará el hecho de que $p(x_i) \leq 1$ para $x_i = \cos\left(\frac{(n-i)\pi}{n}\right)$, donde $i = 0, 1, ..., n$. El polinomio $p(x)$ está completamente determinado por los valores $p(x_i)$. De hecho

$$p(x) = \sum_{i=0}^{n} \frac{p(x_i)}{g_i(x_i)} g_i(x) \qquad (1)$$

donde

$$g_i(x) = \prod_{j \neq i} (x - x_j).$$

Al diferenciar (1) k veces obtenemos

$$P^{(k)}(x) = \sum_{i=0}^{n} \frac{p(x_i)}{g_i(x_i)} g_i^{(k)}(x).$$

Puesto que $|p(x_i)| \leq 1$, resulta que

$$\left|p^{(k)}(x)\right| \leq \sum_{i=0}^{n} \left| \frac{g_i^{(k)}(x)}{g_i(x_i)} \right|. \qquad (2)$$

El valor de $T_n(x)$ para x_i es $\cos(n-i)\pi = (-1)^{n-i}$. Además

$$\left|T_n^{(k)}(x)\right| = \left| \sum_{i=0}^{n} \frac{(-1)^{n-i}}{g_i(x_i)} g_i^{(k)}(x) \right|$$

Esta claro que el $sgn\, g_i(x_i) = (-1)^{n-i}$. Además, para $|x| \geq 1$, el signo de $g_i^{(k)}(x)$ no depende de i. En efecto todas las raíces de $g_i(x)$ pertenecen a $[-1, 1]$, y además todas las raíces de $g_i^{(k)}(x)$ también pertenecen a este intervalo. Por lo tanto

$$sgn g_i^{(k)}(x) = \begin{cases} 1 & para\ x \geq 1 \\ (-1)^{n-k} & para\ x \leq 1 \end{cases}$$

Como resultado de $|x| \geq 1$ obtenemos

$$\left|T_n^{(k)}(x)\right| = \left|\sum_{i=0}^{n} \frac{g_i^{(k)}(x)}{g_i(x_i)}\right|.$$

□

Teorema 3.14 Sea $p(x) = a_0 + a_1x + \cdots + a_nx^n$, donde $a_i \in \mathbb{C}$ tal que $|p(x)| \leq 1$ para $-1 \leq x \leq 1$. Entonces $|a_n| \leq 2^{n-1}$.

Demostración. Recordar que $T_n(x) = b_0 + b_1x + \cdots + b_nx^n$ donde $b_n = 2^{n-1}$. Por lo tanto aplicando el teorema anterior para $k = n$, se deduce que $|a_n| \leq |b_n| = 2^{n-1}$. □

Teorema 3.15. Para $x \leq -1$ y $x \geq 1$ se tiene que

$$\left|T_{n-1}^{(k)}(x)\right| \leq \left|T_n^{(k)}(x)\right|.$$

Demostración. El polinomio $p(x) = T_{n-1}(x)$, cumple las condiciones del teorema 3.14 y entonces $\left|T_{n-1}^{(k)}(x)\right| = |p(x)| \leq \left|T_n^{(k)}(x)\right|$. □

Teorema 3.16. Para x, $y \geq 1$, se tiene que

$$T_n(xy) \leq T_n(x)T_n(y)$$

Demostración. Fijando $y \geq 1$ y considerar el polinomio $p(x) = \frac{T_n(xy)}{T_n(y)}$. Vamos a verificar que el polinomio cumple las condiciones del teorema 3.15 es decir, $|p(x)| = \frac{|T_n(xy)|}{T_n(y)} \leq 1$ para $|x| \leq 1$. Para el real s, la función $|T_n(s)|$ solo depende de $|s|$. Por otra parte sí $|s| \geq 1$, entonces $|T_n(s)|$ es monótona creciente con $|s|$. Claramente $|T_n(s)| \leq 1 \leq T_n(y)$ para $|s| \leq 1$. Por lo tanto, si $y \geq 1$ y $|x| \leq 1$, tenemos $|T_n(xy)| \leq T_n(y)$.

Por el teorema 3.15 para $x \geq 1$, se tiene $|p(x)| \leq T_n(x)$ es decir, $T_n(xy) \leq T_n(x)T_n(y)$.

□

Teorema 3.17. Para $-1 \leq x \leq 1$ y $|z| \leq 1$ se tiene que

$$(a) \qquad 2\sum_{n=1}^{\infty}\frac{T_n(x)}{n}\,z^n = -\ln(1-2xz+z^2)$$

$$(b) \qquad 1+2\sum_{n=1}^{\infty}T_n(x)\,z^n = \frac{1-z^2}{1-2xz-z^2}$$

Demostración. a) Sea $x=\cos\rho$. Entonces

$$1-2xz+z^2=(1-e^{i\rho}z)(1-e^{-i\rho}z).$$

Además $\ln(1-2xz+z^2)=\ln\left((1-e^{i\rho}z)(1-e^{-i\rho}z)\right)=\ln(1-e^{i\rho}z)+\ln(1-e^{-i\rho}z)$. Y considerar que

$$-\ln(1-e^{\pm i\rho}z)=\sum_{n=1}^{\infty}\frac{e^{\pm in\rho}}{n}z^n$$

para $|z|<1$. Además

$$-\ln\left(1-2xz+z^2\right)=\sum_{n=1}^{\infty}\frac{2\cos(n\rho)}{n}z^n=2\sum_{n=1}^{\infty}\frac{T_n(x)}{n}z^n$$

b) Al diferenciar ambas partes de (a) con respecto a z obtenemos

$$2\sum_{n=1}^{\infty}T_n(x)z^{n-1}=\frac{2x-2z}{1-2xz+z^2}.$$

por lo tanto

$$1+2\sum_{n=1}^{\infty}T_n(x)z^n=1+\frac{z(2x-2z)}{1-2xz+z^2}=\frac{1-z^2}{1-2xz+z^2}.$$

□

Teorema 3.18. Sea $n\geq 1$ y $m=\left[\frac{n}{2}\right]$. Entonces

$$T_n(x)=\frac{1}{2}\sum_{k=0}^{\infty}(-1)^k\frac{n}{n-k}\left(\begin{array}{c}n-k\\k\end{array}\right)(2x)^{n-2k}.$$

Demostración. Por el teorema 3.17 (a).

Tenemos que

$$\begin{aligned}2\sum_{n=1}^{\infty}\frac{T_n(x)}{n}z^n &= -\ln(1-2xz+z^2)=\sum_{p=1}^{\infty}\frac{(2xz-z^2)^p}{p}\\ &= \sum_{p=1}^{\infty}\sum_{k=O}^{p}(-1)^k\frac{1}{p}\left(\begin{array}{c}p\\k\end{array}\right)z^{p+k}(2x)^{p-k}.\end{aligned}$$

Por lo tanto

$$\begin{aligned} T_n(x) &= \frac{1}{2}\sum_{p+k=n}(-1)^k\frac{n}{p}\left(\begin{array}{c} p \\ k \end{array}\right)(2x)^{p-k} \\ &= \frac{1}{2}\sum_{k=0}^{M}(-1)^k\frac{n}{n-k}\left(\begin{array}{c} n-k \\ k \end{array}\right)(2x)^{n-2k}. \end{aligned}$$

La suma se realiza hasta $n-2k \geq 0$, y por lo tanto $M = \left[\frac{n}{2}\right] = m$. □

Capítulo 4

Teoría de Galois

En esta sección nuestro objetivo es presentar la Teoría de Galois, las extensiones finitas de cuerpos $L \mid K$ asociada a su grupo de automórfismos $G(L \mid K)$, llamado grupo de *Galois de* $L \mid K$; así como los subgrupos H de $G(L \mid K)$ asociado a un cuerpo intermediario, llamado *cuerpo fijo de* H, definido por

$$L_H = \{\ x \in L;\ \varphi(x) = x;\ \ para\ \ \varphi \in H\},$$

con $K \subset L_H \subset H$.

Las resoluciones de ecuaciones por medido de radicales estarán relacionados al concepto de grupos solubles. Mostraremos la imposibilidad de la resolubilidad de la ecuación de quinto grado por medio de radicales.

4.1. El teorema de Lagrange y los resolventes de Galois.

4.1.1 El teorema de Lagrange.

Definición 4.1. Sea K un campo de característica 0 y sea φ una función racional en las variables $x_1, x_2, ..., x_n$ sobre K. Sea S_n el grupo de permutaciones de n elementos. Podemos asignar a φ el estabilizador de φ, es decir, el grupo

$$G_\varphi = \left\{\sigma \in S_n \mid \varphi\left(x_{\sigma(1)},\ x_{\sigma(2)}, ...,\ x_{\sigma(n)}\right) = \varphi\left(x_1,\ x_2, ...,\ x_n\right)\right\}$$

Teorema 4.1. Sea $\varphi,\ \psi \in K\left[x_1, ..., x_n\right]$ y $G_\varphi \subset G_\psi$. Entonces $\psi = R\left(\varphi\right)$, donde R es una función racional cuyos coeficientes son funciones simétricas en $x_1,\ x_2, ..,\ x_n$.

Demostración. Dividamos a G_ψ es clases laterales que no se intersectan

$h_1G_\varphi = G_\varphi,\ h_2G_\varphi, \ldots,\ h_kG_\varphi$. A cada clase lateral h_iG_φ corresponde una función φ_i, la imagen de φ bajo la acción de esta clase lateral; claramente, $\varphi_i \neq \varphi_j$ para $i \neq j$. La función ψ es $G_{\varphi-\text{invariante}}$, y entonces, a cada función ψ_i le corresponde únicamente la clase lateral h_iG_φ; si $G_\varphi \neq G_\psi$, algunas de estas funciones coinciden.

La función $\sum_{i=1}^{k} \frac{\psi_i}{t-\varphi_i}$ es invariante respecto a la acción de todas las permutaciones de S_n. Por lo tanto

$$\sum_{i=1}^{k} \frac{\psi_i}{t-\varphi_i} = \frac{F(t)}{\Omega(t)},$$

donde

$$\Omega(t) = (t-\varphi_1) \cdot \cdots \cdot (t-\varphi_k)$$

y $F(t)$ es un polinomio en t cuyos coeficientes son funciones simétricas en $x_1, \ldots, x_n$. Como $\varphi_i \neq \varphi_j$ para $i \neq j$, se deduce que $\Omega'(\varphi) \neq 0$.

Claramente,

$$\lim_{t\to\varphi_i} \frac{\Omega(t)}{t-\varphi_i} = \lim_{t\to\varphi_i} \frac{\Omega(t)-\Omega(\varphi_i)}{t-\varphi_i} = \Omega'(\varphi_i).$$

Por lo tanto

$$\lim_{t\to\varphi_i} \frac{\Omega(t)}{\Omega'(t)(t-\varphi_i)} = \begin{cases} 0 & para\ \varphi_i \neq \varphi; \\ 1 & para\ \varphi_i = \varphi. \end{cases}$$

Entonces

$$\frac{F(\varphi)}{\Omega'(\varphi)} = \sum_{i=1}^{k} \psi_i \frac{\Omega(\varphi)}{\Omega'(\varphi)(\varphi-\varphi_i)} = \psi.$$

□

4.1.2 El resolvente de Galois

En esta sección, se define como

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

a un polinomio sobre el campo K de característica 0 y $\alpha_1, \ldots, \alpha_n$ sus raíces. Supongamos que f no tiene raíces múltiples. Consideremos una función racional

$$\psi(x_1, \ldots,\ x_n) = m_1x_1 + \cdots + m_nx_n,$$

donde $m_1, \ldots, m_n$ son enteros. Los números $m_1, \ldots, m_n$, pueden ser seleccionados de tal manera que los $n!$ valores $\psi_\sigma = \psi\left(\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(n)}\right)$ son distintos.

En efecto, consideremos la función

$$D\left(t_1,\ldots,\ t_n\right)=\prod_{\sigma,\tau}\sum_{i=1}^{n}t_i\left(\alpha_{\sigma(i)}-\alpha_{\tau(i)}\right),$$

donde los productos se extienden sobre todas los pares distintos de las permutaciones de σ y τ.

Lema 4.1. Cualquier polinomio simétrico en las raíces $\alpha_2,....,\alpha_n$ de f, es polinomicamente expresado en términos de la raíz α_1 y los coeficientes $a_0,...,a_{n-1}$

Demostración. Cualquier polinomio simétrico en las raíces $\alpha_2,....,\alpha_n$, es expresado en términos de los coeficientes del polinomio
$(x-\alpha_2)....(x-\alpha_n)=\frac{f(x)}{x-\alpha_1}=x^{n-1}+b_{n-2}x^{n-2}+\cdots+b_0$
Aquí tenemos

$$a_{n-1}=b_{n-2}-\alpha_1,$$

$$a_{n-2}=b_{n-3}-b_{n-2}\alpha_1,$$

$$a_{n-3}=b_{n-4}-b_{n-3}\alpha_1,$$

es decir,

$$b_{n-2}=a_{n-1}+\alpha_1,$$

$$b_{n-3}=a_{n-2}-\alpha_1a_{n-1}+\alpha_1^2$$

$$b_{n-4}=a_{n-3}+\alpha_1a_{n-2}+\alpha_1^2a_{n-1}+\alpha_1^3$$

Por lo tanto los coeficientes $b_0,...,b_{n-2}$ se expresan polinomicamente en términos de la raíz α_1 y los coeficientes $a_0,...,a_{n-1}$. □

Se seleccionarán los números $m_1,...,m_n$ de modo que los $n!$ valores

$$\psi_\sigma=m_1\alpha_{\sigma(1)}+\cdots+m_n\alpha_{\sigma(1)}$$

sean distintos y consideremos el polinomio

$$F\left(x\right)\prod_{\sigma\in s_n}\left(x-m_1\alpha_{\sigma(1)}-\cdots-m_n\alpha_{\sigma(n)}\right)$$

Los coeficientes de este polinomio son polinomios simétricos con coeficientes enteros en las raíces de f, y por lo tanto están expresadas de forma racional en términos de los coeficientes de f. Entonces si f es un polinomio sobre K, entonces también lo es F.

Se factorizará a F como producto de factores mónicos irreducibles sobre K. Cualquier factor irreducible G es llamado un resolvente de Galois de f.

Claramente, todas las resolventes de Galois se obtienen unos de otros por permutaciones de las raíces. Habiendo numerado las raíces podemos fijar el resolvente de Galois, que corresponde a la permutación identidad. Supongamos que G tiene una raíz

$$\psi = m_1\alpha_1 + \cdots + m_n\alpha_n$$

Teorema 4.2 (Galois). Cualquier raíz de f se expresa racionalmente (*sobre* K) en términos de una de las raíces de G.

Demostración. Consideremos el polinomio

$$F_1(x) = \prod_{\{\sigma\in S_n/\sigma_{(1)}=1\}} \left(x - m_1\alpha_1 - m_2\alpha_{\sigma(2)} - \cdots - m_n\alpha_{\sigma(n)}\right)$$

Los coeficientes de F_1 son polinomios simétricos en $\alpha_2, ..., \alpha_n$; entonces por el Lema 4.1, estos son expresados racionalmente (*sobre* K) en términos de α_i, es decir,

$F_1(x) = g(x, \alpha_1)$, donde g es un polinomio en dos variables sobre K . Claramente,

$g(\psi, \alpha_1) = F_1(\psi) = 0$.

Ahora consideremos el polinomio

$$F_2(x) = \prod_{\{\sigma\in S_n/\sigma_{(2)}=2\}} \left(x - m_1\alpha_2 - m_2\alpha_{\sigma(1)} - .... - m_n\alpha_{\sigma(n)}\right)$$

A partir de la prueba del Lema 4.1 vemos que los coeficientes de F_2 son los mismos que para F_1 reemplazando α_1 por α_2, es decir, $F_2(x) = g(x, \alpha_2)$.

Pero por hipótesis

$$\psi = m_1\alpha_1 + ... + m_n\alpha_n \neq m_1\alpha_2 + m_2\alpha_{\sigma(1)} + ... + m_n\alpha_{\sigma(n)}$$

es decir, $F_2(\psi) = 0$. Por lo tanto α_1 es la única raíz en común de los polinomios $f(x)$ y $g(\psi, x)$. Esto significa que el máximo común divisor de $f(x)$ y $g(\psi, x)$ es $x - \alpha_1$. Pero el máximo común divisor de dos polinomios es encontrado por el algoritmo de Euclides, y así α_1 se expresa de forma racional en términos de ψ y los coeficientes de f y g, es decir, α_1 se expresa de forma racional sobre K en términos de ψ. □

Corolario 4.1. Todas las raíces del resolvente de Galois son expresadas racionalmente en términos de una de sus raíces.

Demostración. Cada raíz del resolutivo de Galois es de la forma

$$m_1\alpha_{\sigma(1)} + ... + m_n\alpha_{\sigma(n)}$$

Claramente son expresados racionalmente en términos de $\alpha_1, ..., \alpha_n$. A su vez $\alpha_1, ..., \alpha_n$ son expresados racionalmente en términos de $\psi = m_1\alpha_a + ... + m_n\alpha_n$. □

El siguiente teorema es de considerable importancia para la teoría de Galois.

Teorema 4. 3. Sea $\alpha_1, ..., \alpha_n$ las raíces de un polinomio irreducible f sobre k y sea $\varphi \in k(x_1, ..., x_n)$.

a) Sea $\varphi(\alpha_1, .., \alpha_n) = \varphi\left(\alpha_{\sigma_i(1)}, ..., \alpha_{\sigma_i(n)}\right)$ para cualquier permutación σ_i en el grupo de Galois. Entonces $\varphi(\alpha_1, ..\alpha_n) \in k$.

b) Sea $H = \{\sigma_{i_1}, ..., \sigma_{i_s}\}$ un subgrupo del grupo de Galois $\{\sigma_1, .., \sigma_r\}$ tal que si $\varphi(\alpha_1, ..., \alpha_n) = \varphi\left(\alpha_{\sigma(1)}, ..., \alpha_{\sigma(n)}\right)$ para cualquier permutación $\sigma \in H$, entonces $\varphi(\alpha_1, ..\alpha_n) \in k$. Entonces H coincide con todo el grupo de Galois.

Demostración. a) Las raíces $\alpha_1, ..., \alpha_n$ pueden ser expresadas racionalmente en términos de ψ_1, y entonces $\varphi(\alpha_1, .., \alpha_n) = \Phi(\psi_1)$, donde $\Phi \in k(x)$. Por lo tanto

$$\varphi\left(\alpha_{\sigma_i(1)}, ..., \alpha_{\sigma_i(n)}\right) = \Phi(\psi_i)$$

Así, $\Phi(\psi_1) = ... = \Phi(\psi_r)$, y entonces

$$\Phi(\psi_1) = \frac{1}{r}(\Phi(\psi_1) + ... + \Phi(\psi_r))$$

es una función simétrica en las raíces del resolvente de Galois.

Por lo tanto $\varphi(\alpha_1, ..., \alpha_n) = \Phi(\psi_1) \in k$.

b) Considerar el polinomio

$$g(x) = \prod(x - \sigma(\psi)) = (x - \psi_{i_1}) ..... (x - \psi_{i_1})$$

Sus coeficientes son invariantes con respecto a la $H - acción$, y por lo tanto todos ellos pertenecen a k. Por lo tanto los coeficientes de $g(x)$ se encuentran en k y $g(x)$ tiene raíces en común con un polinomio irreducible sobre k.

$$G(x) = (x - \psi_1) ..... (x - \psi_r).$$

Entonces $g(x) = G(x)$ y $H = \{\sigma_1, ..., \sigma_r\}$. □

4.2. Teoría Básica de Galois.

Definición 4.2 ($K - automorfismo$). Sea $L \mid K$ una extensión de cuerpos. Un automorfismo $\varphi : L \to L$ es un $K - automorfismo$ si, y solamente si, $\varphi(\alpha) = \alpha$,

para todo $\alpha \in K$.

Proposición 4.1. Sea $L \mid K$ una extensión de cuerpos. Entonces,

$G(L \mid K) = \{\varphi :\ L \to L;\ automorfismo\ tal\ que\ \varphi \mid_K = I\}$

es un grupo con la operación composición de funciones.

Demostración. Como una composición de biyecciones es una biyección y una composición de homomorfismos es un homomorfismo, entonces la composición de automorfismos es un automorfismo. Si φ y ψ son $K - automorfismos$ entonces, para todo $\alpha \in K$, tenemos $\varphi(\alpha) = \alpha$ y $\psi(\alpha) = \alpha$ y entonces $(\varphi \circ \psi)(\alpha) = \varphi(\psi(\alpha)) = \varphi(\alpha) = \alpha$, mostrando que $\varphi \circ \psi \in G(L \mid K)$. Además, si $\varphi \in G(L \mid K)$, entonces φ^{-1} es un automorfismo de L tal que, para todo $\alpha \in K$,

$$\alpha = I(\alpha) = \left(\varphi^{-1}\varphi\right)(\alpha) = \varphi^{-1}(\varphi(\alpha)) = \varphi^{-1}(\alpha)$$

mostrando que $\varphi^{-1} \in G(L \mid K)$. Por lo tanto, $G(L \mid K)$ es un grupo. □

Definición 4.3 (*Grupo de Galois de* $L \mid K$). El *Grupo de Galois* de $L \mid K$ es el grupo $G(L \mid K)$.

Ejemplo 4.1. Consideremos la extensión $\mathbb{C} \mid \mathbb{R}$. Sea $\varphi :\ \mathbb{C} \to \mathbb{C}$ un

$\mathbb{R} - automorfismo$. Como $\{1,\ i\ \}$ es una base de $\mathbb{C} \mid \mathbb{R}$, entonces cada $\alpha \in \mathbb{C}$ se escribe de manera única como $\alpha = a + bi$ con $a,\ b \in \mathbb{R}$. Así,

$$\varphi(\alpha) = \varphi(a + bi) = \varphi(a) + \varphi(b)\varphi(i) = a + b\varphi(i).$$

Por lo tanto, φ está perfectamente determinada por $\varphi(i)$.

Como $-1 = i^2\ \ y\ \ -1 = \varphi(-1) = \varphi(i^2) = \varphi(i)^2$, entonces $\varphi(i)$ también es una raíz en $\mathbb{C}$ de $x^2 + 1 \in \mathbb{R}[x]$.

Por lo tanto, $\varphi(i) = i$ o $\varphi(i) = -i$. Tenemos dos $\mathbb{R} - automorfismos$, $I :\ \mathbb{C} \to \mathbb{C}$, con $I(a + bi) = a + bi$, y $\varphi :\ \mathbb{C} \to \mathbb{C}$, con $\varphi(a + bi) = a - bi$, una conjugación compleja. En este caso, $G(\mathbb{C} \mid \mathbb{R}) =< \varphi >= \{I,\ \varphi;\ \varphi^2 = I\}$.

Ejemplo 4.2. Sea $\alpha \in \mathbb{R}$ tal que $\alpha^3 = 2$. Consideremos una extensión $\mathbb{Q}(\alpha) \mid \mathbb{Q}$ y un $\mathbb{Q} - automorfismo\ \varphi :\ \mathbb{Q}(\alpha) \to \mathbb{Q}(\alpha)$. Como $\{1,\ \alpha,\ \alpha^2\}$ es una base de $\mathbb{Q}(\alpha) \mid \mathbb{Q}$, todo elemento de $\mathbb{Q}(\alpha)$ se escribe, de manera única, como

$$\beta = a + b\alpha + c\alpha^2\ \ con\ a,\ b,\ c \in \mathbb{Q}.$$

Entonces,

$$\begin{aligned}\varphi(\beta) &= \varphi(a+b\alpha+c\alpha^2)\\ &= \varphi(a)+\varphi(b\alpha)+\varphi(c\alpha^2)\\ &= a+b\varphi(\alpha)+c\varphi(\alpha)^2.\end{aligned}$$

Así, φ está perfectamente determinada por $\varphi(\alpha)$.

Como $2=\alpha^3$, entonces $2=\varphi(2)=\varphi(\alpha)^3$, luego $\varphi(\alpha)$ también es una raíz en $\mathbb{Q}(\alpha)$ de x^3-2. El único valor posible es $\varphi(\alpha)=\alpha$. Por lo tanto, $\varphi=I$ y $G(\mathbb{Q}(\alpha)\mid\mathbb{Q})=\{I\}$.

Lema 4.2. Sea $f(x)\in K[x]\setminus K$ y sea L un campo de raíces de $f(x)$ sobre K. Sea $\varphi:\ L\to L$ un $K-automorfismo$ de L y α una raíz de $f(x)$, entonces $\varphi(\alpha)$ también es una raíz de $f(x)$.

Demostración. Sea $f(x)=a_0+a_1x+\cdots+a_nx^n$.

Luego, $0=a_0+a_1\alpha+\cdots+a_n\alpha^n$. Aplicando φ, obtenemos

$$\begin{aligned}0=\varphi(0) &= \varphi(a_0)+\varphi(a_1)\varphi(\alpha)+\cdots+\varphi(a_n)\varphi(\alpha)^n\\ &= a_0+a_1\varphi(\alpha)+\cdots a_n\varphi(\alpha)^n\\ &= f(\varphi(\alpha)).\end{aligned}$$

□

Definición 4.4 (*Grupo de Galois de* $f(x)$)**.** Sea $f(x)\in K[x]\setminus K$ y sea L el campo de raíces de $f(x)$ sobre K. El grupo de Galois de $f(x)$ es $G(f(x)\mid K)=G(L\mid K)$.

Teorema 4.4. Si $f(x)\in K[x]\setminus K$ tiene n raíces distintas en su campo de raíces L, entonces $G(L\mid K)$ es isomorfo a un subgrupo de S_n.

Demostración. Sea $\Re=\{\alpha_1,\cdots,\alpha_n\}$ el conjunto de las n raíces de $f(x)$. Por el lema anterior, si $\varphi\in G(L\mid K)$, entonces $\varphi(\alpha_j)$ también es una raíz de $f(x)$, y como φ es inyectiva, $\varphi(\Re)=\Re$, esto es, φ permuta las raíces distintas de $f(x)$.

Consideremos la función

$$G(L\mid K)\longrightarrow S_{\Re}$$

$$\varphi\longrightarrow\varphi\mid_{\Re}.$$

Fácilmente se verifica que esta función es un homomorfismo. Como

$$\begin{aligned}L=K(\alpha_1,\cdots,\alpha_n) &= K[\alpha_1,\cdots,\alpha_n]\\ &= \{h(\alpha_1,\cdots\alpha_n), h(x_1,\cdots,x_n)\in K[x_1,\cdots,x_n]\},\end{aligned}$$

entonces $\varphi\in G(L\mid K)$ está perfectamente determinada por sus valores en $\Re$. Luego, si $\varphi,\ \psi\in G(L\mid K)$ son tales que $\varphi\mid_{\Re}=\psi\mid_{\Re}$, entonces $\varphi=\psi$, mostrando que la función anterior es inyectiva. Por lo tanto, $G(L\mid K)$ es isomorfo a un subgrupo de $S_{\Re}\simeq S_n$. □

Teorema 4.5. Sea$f(x) \in K[x] \setminus K$ un polinomio separable. Sea L el campo de raíces de $f(x)$ sobre K. Entonces, $\mid G(L \mid K) \mid = [L : K]$.

Demostración. Se mostrará que $I : K \to K$ tiene $[L : K]$ extensiones a L. La demostración se hará por inducción sobre $[L : K]$. Si $[L : K] = 1$, entonces, $G(L \mid K) = \{I\}$ y el resultado es válido. Supongamos que $[L : K] > 1$. Entonces, $f(x)$ tiene algún factor irreducible $p(x) \in K[x]$ de grado $d > 1$. Fijemos $\alpha \in L$ una raíz de $p(x)$. Como $f(x)$ es separable, entonces $p(x)$ tiene d raíces distintas, todas en L. Así, cada $\varphi \in G(L \mid K)$ es tal que $\beta = \varphi(\alpha) \in L$, también es una raíz de $p(x)$. Hay exactamente d $K - isomorfismos$ $\varphi : K(\alpha) \to K(\beta)$ extensiones de $I : K \to K$, uno para cada raíz de $p(x)$. Observemos que L es un campo de raíces de $f(x)$ sobre $K(\alpha)$, así como también L es un campo de raíces de $f(x)$ sobre $K(\beta)$. Por el Teorema de extensión de isomorfismos a campos de raíces, cada $\varphi : K(\alpha) \to K(\beta)$ admite una extensión $\tilde{\varphi} : L \to L$. Como $[L : K(\alpha)] = \frac{[L:K]}{[K(\alpha):K]} = \frac{[L:K]}{d} < [L : K]$, por hipótesis inductiva, hay $[L : K(\alpha)] = \frac{[L:K]}{d}$ extensiones de cada uno de los d $K - isomorfismo$ $\varphi : K(\alpha) \to K(\beta)$. Por lo tanto, hay $[L : K]$ d $K - automorfismos$ de L. □

Definición 4.5 (*Campo intermedio*). Sea L una extensión de campos. Se le llama un *campo intermedio* a un campo F, tal que $K \subset F \subset L$.

Proposición 4.2. Sea $L \mid K$una extensión de campos y F un campo intermediario. Entonces, $G(L \mid F)$ es un subgrupo de $G(L \mid K)$. Aún más, si F y F' son campos intermedios y $F \subset F'$, entonces $G(L \mid F) \supset G(L \mid F')$.

Demostración. Si $\varphi \in G(L \mid F)$, entonces φ es un automorfismo de L que fija a $F \supset K$, luego φ es un $K - automorfismo$, mostrando que $G(L \mid F) \subset G(L \mid K)$. Es claro que $G(L \mid F)$ es un subgrupo de $G(L \mid K)$. Sea $\alpha \in G(L \mid F')$ entonces para todo $\varphi \in F'$, se tendrá que α será fijado, es decir, α será fijado por cualquier subconjunto de F', en particular, α será fijado por F, por lo tanto $\alpha \in G(L \mid F)$. Por lo tanto $G(L \mid F) \supset G(L \mid F')$. □

Lema 4.3. Sea $K \subset F \subset L$ una cadena de campos, con $F \mid K$ campo de descomposición sobre K de algún polinomio. Si $\varphi \in G(L \mid K)$, entonces $\varphi \mid_F \in G(F \mid K)$.

Demostración. Es suficiente demostrar que $\varphi(F) = F$. Sean $\alpha_1, \cdots, \alpha_n$ las raíces distintas de $f(x)$ y $\varphi \in G(L \mid K)$. Entonces, $\varphi(f)(x) = f(x)$ y $\varphi(\alpha_i) = \alpha_j$ están en F, pues $F = K(\alpha_1, \cdots, \alpha_n)$, entonces $\varphi(F) = K(\varphi(\alpha_1), \cdots, \varphi(\alpha_n)) \subset F$. Como φ es $K - lineal$ e inyectiva, $[\varphi(F) : K] = [F : K]$, luego $\varphi(F) = F$. □

Teorema 4.6. Sean $K \subset F \subset L$ una cadena de campos, con $F \mid K$ campo de descomposición sobre K de algún polinomio $f(x) \in K[x] \setminus K$, y sea $L \mid K$ campo de descomposición sobre K de algún polinomio $g(x) \in K[x] \setminus K$. Entonces, $G(L \mid F)$ es un subgrupo normal de $G(L \mid K)$ y

$$G(L \mid K)/G(L \mid F) \simeq G(F \mid K).$$

Demostración. Sea $\psi : \ G(L \mid K) \to G(F \mid K)$ tal que $\psi(\varphi) = \varphi \mid_F$. Por el lema anterior, ψ está bien definida. Se verifica fácilmente que ψ es un homomorfismo de grupos, pues para cualquier $\varphi, \sigma \in G(L \mid K)$, tenemos que $(\varphi \circ \sigma) \mid_F = \varphi \mid_F \ \circ \sigma \mid_F$. Dado que Núcleo$(\psi) = \{\varphi \in G(L \mid K) ; \ \varphi \mid_F = I\} = G(L \mid F)$, entonces $G(L \mid F)$ es un subgrupo normal de $G(L \mid K)$. Sea $\tau \in G(F \mid K)$ por teorema de extensión de isomorfismos de campos de raíces, τ se extiende a un $K - automorfismo$ de L, esto es, existe $\varphi \in G(L \mid K)$ tal que $\varphi \mid_F = \tau$, mostrando que es sobreyectiva. Pero por el Teorema Fundamental de Homomorfismo de grupos, se obtiene un isomorfismo de grupos $G(L \mid K)/G(L \mid F) \simeq G(F \mid K)$. □

Proposición 4.3. Sea $L \mid K$ una extensión de campos y $G = G(L \mid K)$. Para cada subgrupo H de G, definimos

$$L_H = \{x \in L; \ \varphi(x) = x, \ \ para\ todo\ \varphi \in H\}.$$

Entonces, L_H es un campo intermedio de $L \mid K$. Aún más, si H y H', son subgrupos de G con $H \subset H'$, entonces $L_H \supset L_{H'}$.

Demostración. Sean , $\alpha, \ \beta \in L_H$ y $\varphi \in H$. Entonces,

$$\begin{aligned} \varphi(\alpha - \beta) &= \varphi(\alpha) - \varphi(\beta) = \alpha - \beta, \\ \varphi(\alpha.\beta) &= \varphi(\alpha)\varphi(\beta) = \alpha.\beta, \\ \varphi(\beta^{-1}) &= \varphi(\beta)^{-1} = \beta^{-1}, \ si\ \beta \neq 0. \end{aligned}$$

para todo $\varphi \in H$, mostrando que L_H es un subcampo de L. Como $H \subset G$, entonces $\varphi \in G$ y para todo $a \in K$, tenemos $\varphi(a) = a$, luego $K \subset L_H$. Por lo tanto, L_H es un cuerpo intermediario de $L \mid K$.

Si $\alpha \in L$ es fijado por todos los elementos de H', entonces es fijado por todos los elementos de cualquier subconjunto de H', en particular, es fijado por todos los elementos de $H \subset H'$, luego $L_H \supset L_{H'}$. □

El diagrama de la izquierda ilustra una función φ haciendo correspondencia entre los campos intermediarios F de $L \mid K$ y los subgrupos de $G(L \mid K)$. El diagrama de la derecha muestra una función ψ haciendo correspondencia entre los subgrupos H de $G(L \mid K)$ y los campos intermediarios de $L \mid K$.

$$\begin{array}{ccc} L & & I \\ | & & | \\ F & \overset{\varphi}{\longmapsto} & H = G(L \mid F) \\ | & & | \\ K & & G = G(L \mid K) \end{array} \qquad \begin{array}{ccc} I & & L \\ | & & | \\ H & \overset{\psi}{\longmapsto} & L_H \\ | & & | \\ G = G(L \mid K) & & K \end{array}$$

Observaciones.

(1) Si $K \subset F \subset L$ y $H = G(L \mid F) = \varphi(F)$, entonces $F \subset L_{G(L|F)} = \psi(\varphi(F))$, pues cada elemento de F es fijado por cada automorfismo que fija a todo F.

(2) Si H es un subgrupo de $G(L \mid K)$, entonces $H \subset G(L \mid L_H) = \varphi(\psi(H))$, pues cada elemento de H fija los elementos que son fijados por todos los elementos de H.

(3) Sea $\mathcal{F}$ el conjunto de campos intermediarios de $L \mid K$ y sea $\mathcal{H}$ el conjunto de subgrupos de $G(L \mid K)$. Las funciones descritas anteriormente son

$$\begin{array}{rccc} \varphi: & \mathcal{F} & \longrightarrow & \mathcal{H} \\ & F & \longmapsto & \varphi(F) = G(L \mid F) \end{array} \qquad \begin{array}{rccc} \psi: & \mathcal{H} & \longrightarrow & \mathcal{F} \\ & H & \longmapsto & \psi(H) = L_H \end{array}$$

y ambas invierten inclusión.

4.2.1 La conexión de Galois

Proposición 4.4. Sea L un campo y $\lambda_1, \cdots, \lambda_n$ automorfismos distintos de L. Entonces el conjunto $\{\lambda_1, \ldots, \lambda_n\}$ es linealmente independiente sobre L.

Demostración. Supongamos, por absurdo, que el conjunto de arriba es linealmente dependiente sobre L. Entonces, existen $a_1, \ldots, a_n \in L$, no todos nulos, tales que

$$a_1\lambda_1(x) + a_2\lambda_2(x) + \cdots + a_n\lambda_n(x) = 0; \ \textit{para todo } x \in L.$$

En este caso, podemos encontrar una relación que tiene el número más bajo de coeficientes no nulos, y renumerando los automorfismos, podemos suponer que

$$a_1\lambda_1(x) + a_2\lambda_2(x) + \cdots + a_m\lambda_m(x) = 0; \ \textit{para todo } x \in L, \qquad (\star)$$

con $a_1, \ldots, a_m$ no nulos, y sea esta la relación minímal.

Se afirma que $m \geq 2$. De hecho, si $m = 1$, entonces λ_1 es linealmente independiente sobre L, pues si $0 = a_1\lambda_1(x)$, $a_1 \in L$, para todo $x \in L$, como $\lambda_1(1_L) = 1_L$, entonces $0 = a_1\lambda_1(1_L) = a_1.1_L = a_1$. Podemos asumir que $m \geq 2$ y que no hay una ecuación del tipo $(\star)$ con menos de m coeficientes no nulos. Como $\lambda_1 \neq \lambda_m$, existe $y \in L$ tal que $\lambda_1(y) \neq \lambda_m(y)$. Sustituyendo x por yx en $(\star)$, obtenemos:

$a_1\lambda_1(y)\lambda_1(x) + a_2\lambda_2(y)\lambda_2(x) + \cdots + a_m\lambda_m(y)\lambda_m(x) = 0, \qquad (1)$

para todo $x \in L$. Multiplicando la ecuación $(\star)$ por $\lambda_1(y)$, obtenemos:

$a_1\lambda_1(y)\lambda_1(x) + a_2\lambda_1(y)\lambda_2(x) + \cdots + a_m\lambda_1(y)\lambda_m(x) = 0, \qquad (2)$

para todo $x \in L$. Restando (2) de (1), tenemos:

$a_2(\lambda_2(y) - \lambda_1(y))\lambda_2(x) + \cdots + a_m(\lambda_m(y) - \lambda_1(y))\lambda_m(x) = 0, \qquad (3)$

para todo $x \in L$. El coeficiente de $\lambda_m(x)$ es $a_m(\lambda_m(y) - \lambda_1(y)) \neq 0$, entonces (3) es una ecuación del tipo $(\star)$ con un número máximo de $m - 1 < m$ escalares no nulos, contradiciendo la hipótesis de arriba.

Consecuentemente la ecuación $(\star)$ es un conjunto linealmente independiente sobre L . □

Teorema 4.7. Sea G un subgrupo finito de un grupo de automorfismos en un campo L y sea L_G el cuerpo fijo de G, esto es, $L_G = \{x \in L;\ \sigma(x) = x,\ \ para\ todo\ \sigma \in G\}$. Entonces, $[L :\ L_G] =\mid G \mid$.

Demostración. Sea $n =\mid G \mid$ y $G = \{I = \sigma_1, \cdots, \sigma_n\}$.

Supongamos, en primer lugar, que $[L :\ L_G] = m < n$. Sea $\{\alpha_1, \cdots, \alpha_m\}$ una base de $L \mid L_G$. Sea A una matriz $m \times n$ con coeficientes en L definida por $A_{ij} = \sigma_j(\alpha_i)$. El sistema $AX = 0$ tiene una solución no nula $(x_1, \ldots, x_n)$ en L^n, tal que

$$\sigma_1(\alpha_i)x_1 + \cdots + \sigma_n(\alpha_i)x_n = 0,\ \ para\ \ todo\ \ i = 1, \ldots,\ m. \qquad (1)$$

Sea $\alpha \in L$.

Entonces, existen $a_1, \ldots,\ a_m \in L_G$, tales que $\alpha = a_1\alpha_1 + \cdots + a_m\alpha_m$. Así,

$$\begin{aligned}
\sigma_1(\alpha)x_1 + \cdots + \sigma_n(\alpha)x_n &= \sigma_1\left(\sum a_i\alpha_i\right)x_1 + \cdots + \sigma_n\left(\sum a_i\alpha_i\right)x_n \\
&= \left(\sum a_i\sigma_1(\alpha_i)\right)x_1 + \cdots + \left(\sum a_i\sigma_n(\alpha_i)\right)x_n \\
&= \sum\left(a_i\sigma_1(\alpha_i)x_1\right) + \cdots + \sum\left(a_i\sigma_n(\alpha_i)x_n\right) \\
&= \sum a_i\left(\sigma_1(\alpha_i)x_1 + \cdots + \sigma_n(\alpha_i)x_n\right) \\
&= \sum a_i.0 \\
&= 0,
\end{aligned}$$

para todo $\alpha \in L$, con $x_1, \ldots, x_n$ no todos nulos.

Por lo tanto los automorfismsos distintos $\sigma_1, \ldots, \sigma_n$ son linealmente dependientes sobre L contradiciendo la *proposición* 4.4. Consecuentemente, $m \geq n$. Supongamos que $[L :\ L_G] > n$. Entonces, existen $\alpha_1, \ldots, \alpha_{n+1}$ en L linealmente independientes sobre L_G. Consideremos una matriz $n \times (n+1)$ con coeficientes el L definida por $A_{ij} = \sigma_i(\alpha_j)$. Entonces, el sistema $AX = 0$ tiene una solución no nula $(x_1, \ldots, x_{n+1}) \in L^{n+1}$ y

$$\sigma_i(\alpha_1)x_1 + \cdots + \sigma_i(\alpha_{n+1})x_{n+1} = 0,\ \ para\ \ todo\ \ i = 1, \ldots, n. \qquad (2).$$

Entre todas las soluciones no nulas, escogemos una relación con menor número de coeficientes no nulos, digamos $x_1, \cdots, x_r$ son no nulos. Así, la ecuación (2) se reescribe como

$$\sigma_i(\alpha_1)x_1 + \cdots + \sigma_i(\alpha_r)x_r = 0, \quad para \;\; todo \;\; i = 1, \ldots, n. \tag{3}$$

Sea $\sigma \in G$. Entonces, $\{\sigma \circ \sigma_1, \ldots, \sigma \circ \sigma_n\} = G$. Aplicando σ en (3), se obtiene

$$\sigma(\sigma_i(1))\sigma(x_1) + \cdots + \sigma(\sigma_i(r))\sigma(x_r) = 0, \quad para\ todo \;\; i = 1, \ldots, n. \tag{4}$$

El sistema de ecuaciones lineales en (4) es equivalente al sistema

$$\sigma_i(\alpha_1)\sigma(x_1) + \cdots + \sigma_i(\alpha_r)\sigma(x_r) = 0, \quad para \;\; todo\ i = 1, \ldots, n. \tag{5}$$

Multiplicando la ecuación (3) por $\sigma(x_1)$ y multiplicando la ecuación (5) por x_1 se tiene, respectivamente,

$$\begin{cases} \sigma_i(\alpha_1)\, x_1\sigma(x_1) + \sigma_i(\alpha_2)\, x_2\sigma(x_1) + \cdots + \sigma_i(\alpha_r)\, x_r\sigma(x_1) & = 0 \\ \sigma_i(\alpha_1)\, \sigma(x_1)\, x_1 + \sigma_i(\alpha_2)\, \sigma(x_2)\, x_1 + \cdots + \sigma_i(\alpha_r)\, \sigma(x_r)\, x_1 & = 0 \end{cases}$$

para todo $i = 1, \ldots, n$.

Restando, obtenemos:

$\sigma_i(\alpha_2)(x_2\sigma(x1) - \sigma(x_2)x_1) + \cdots + \sigma_i(\alpha_r)(x_r\sigma(x_1) - \sigma(x_r)x_1) = 0,$

para todo $i = 1, \ldots, n$.

Este sistema de ecuaciones es del tipo (3) con menos términos nulos, lo que es una contradicción. Por lo tanto, $[L : L_G] < n$.

Por la primera etapa de la demostración, $[L : \ L_G] = n = \mid G \mid$. □

Proposición 4.5. Sea $L \mid K$ una extensión finita y $G = G(L \mid K)$. Si H es un subgrupo de G, entonces

$$[L_H : \ K] = \frac{[L : \ K]}{\mid H \mid}.$$

Demostración. Basta mostrar que $G = G(L \mid K)$ es finito. Así, H también es finito, y por el Teorema anterior, $[L : \ L_H] = \mid H \mid$. Luego,

$[L_H : \ K] = \frac{[L: \ K][L: \ L_H]}{[L: \ L_H]} = \frac{[L: \ K]}{|H|}$.

Se demostrará que $\mid G(L \mid K) \mid \leq [L : \ K]$. Sea $\{\alpha_1, \ldots, \alpha_m\}$ una base de $L \mid K$. Supongamos, por absurdo, que existen $\sigma_1, \ldots, \sigma_{m+1}$ $K - automorfismos$ distintos de L . Sea A una matriz $m \times (m+1)$ con coeficientes en L definida por $A_{ij} = \sigma_j(\alpha_i)$. El sistema $AX = 0$ tiene una solución no nula $(x_1, \ldots, x_{m+1})$ en L^{m+1}, tal que

$\sigma_1(\alpha_i)x_1 + \cdots + \sigma_{m+1}(\alpha_i)x_{m+1} = 0, \quad para\ todo\ i = 1, \ldots, m. \qquad (1)$

Sea $\alpha \in L$.

Entonces, existen $a_1, \ldots, a_m \in K$, tales que $\alpha = a_1\alpha_1 + \cdots + a_m\alpha_m$. Así,

$$\begin{aligned}
\sigma_1(\alpha)x_1 + \cdots + \sigma_{m+1}(\alpha)x_{m+1} &= \sigma_1\left(\sum a_i\alpha_i\right)x_1 + \cdots + \sigma_{m+1}\left(\sum a_i\alpha_i\right)x_{m+1} \\
&= \left(\sum a_i\sigma_1(\alpha_i)\right)x_1 + \cdots + \left(\sum a_i\sigma_{m+1}(\alpha_i)\right)x_{m+1} \\
&= \left(\sum a_i\sigma_1(\alpha_i)x_1\right) + \cdots + \left(\sum a_i\sigma_{m+1}(\alpha_i)x_{m+1}\right) \\
&= \sum a_i\left(\sigma_1(\alpha_i)x_1 + \cdots + \sigma_{m+1}(\alpha_i)x_{m+1}\right) \\
&= \sum a_i.0 \\
&= 0
\end{aligned}$$

para todo $2\alpha \in L$, con $x_1, \ldots, x_n$ no todos nulos contradiciendo la *proposición* 4.4.

Consecuentemente, $\mid G(L \mid K) \mid \leq [L : K]$. □

Teorema 4.8. Sea $L \mid K$ una extensión finita con $G = G(L \mid K)$. Las siguientes condiciones son equivalentes:

(i) $L_G = K$,

(ii) Cada polinomio irreducible $p(x) \in K[x]$ con una raíz en L es separable y tiene todas sus raíces en L,

(iii) L es el campo de descomposición sobre K de algún polinomio separable $f(x) \in K[x]$.

Demostración. $(i) \Longrightarrow (ii)$. Sea $p(x) \in K[x]$ un polinomio mónico irreducible con una raíz $\alpha \in L$. Como $L_G = K$, por Teorema anterior $\mid G \mid = [L : L_G] = [L : K]$.

Consideremos los elementos distintos del conjunto finito $\{\sigma(\alpha);\ \sigma \in G\} \subset L$ con $\alpha = \alpha_1, \ldots, \alpha_n$. Definimos $g(x) \in L[x]$ por

$$g(x) = \prod_{j=1}^{n}(x - \alpha_j) = x^n - s_1x^{n-1} + s_2x^{n-2} + \cdots + (-1)^n s_n, \quad con$$

$$\begin{aligned}
s_1 &= \alpha_1 + \cdots + \alpha_n \\
s_2 &= \sum_{1 \leq i \leq j \leq n} \alpha_i\alpha_j \\
&\vdots \\
s_j &= \sum_{1 \leq i_1 \leq i_j \leq n} \alpha_{i1} \cdots \alpha_{ij} \\
&\vdots \\
s_n &= \alpha_1\alpha_2 \cdots \alpha_n
\end{aligned}$$

Cada $\sigma \in G$ permuta $\{\alpha_1, \cdots, \alpha_n\}$, luego fija a sus funciones simétricas elementales, esto es, $(s_j) = s_j$, para todo $j = 1, \ldots, n$. Como $L_G = K$, entonces $g(x) \in K[x]$

y tiene todas sus raíces distintas. Los polinomios $p(x)$ y $g(x)$ tienen a α como raíz común en L, tenemos que $mcd_{L[x]}(p(x),\ g(x)) \neq 1$, entonces $mcd_{K[x]}(p(x),\ g(x)) \neq 1$. Como $p(x)$ es irreducible en $K[x]$ sigue que $mcd_{K[x]}(p(x),\ g(x)) = p(x)$, luego $p(x)$ divide a $g(x)$. Por lo tanto, todas las raíces de $p(x)$ son distintas.

$(ii) \Longrightarrow (iii)$. En primer lugar, observemos que cada $\alpha \in L$ es algebraico sobre K, porque $L \mid K$ es una extensión finita. Seleccionemos $\alpha_1 \in L$ y sea $p_1(x) \in K[x]$ el polinomio mínimo de α_1 sobre K. Por hipótesis, $p1(x)$ tienen todas sus raíces en L y es separable. Sea $K_1 \subset L$ el campo de descomposición de $p_1(x)$ sobre K. Si $K_1 = L$, ya está. Caso contrario, seleccionamos $\alpha_2 \in L$ tal que $\alpha_2 \notin K_1$. Sea $p_2(x) \in K[x]$ el polinomio mínimo de α_2 sobre K. Por hipótesis, $p_2(x)$ es separable y tiene todas sus raíces en L. Consideremos $K_2 \subset L$ el campo de descomposición del polinomio separable $p_1(x)p_2(x) \in K[x]$. Si $K_2 = L$, ya está. Caso contrario, continuamos el proceso, que tiene que parar, en virtud de que $[L :\ K]$ es finito.

$(iii) \Longrightarrow (i)$. Por **Teorema 4.5**, $\mid G(L \mid K) \mid = [L :\ K]$ y, por **Teorema 4.7**, tenemos que $\mid G(L \mid K) \mid = [L :\ L_G]$. Por tanto, $[L :\ L_G] = [L :\ K]$. Como $K \subset L_G \subset L$, sigue de la multiplicidad de grados que $K = L_G$. □

Lema 4.4. Sea $L \mid K$ una extensión finita, F un campo intermedio y $\sigma \in G(L \mid K)$. Entonces,

$$G(L \mid \sigma(F)) = \sigma G(L \mid F)\sigma^{-1}.$$

Demostración. " $\supset$ " En efecto, tome $\gamma \in G(L \mid K)$ y $\beta \in \sigma(F)$. Entonces, $\beta = \sigma(\alpha)$, para algún $\alpha \in F$ y

$$(\sigma\gamma\sigma^{-1})(\beta) = \sigma\left(\gamma\left(\sigma^{-1}(\beta)\right)\right) = \sigma(\gamma(\alpha)) = \sigma(\alpha) = \beta.$$

Luego, $\sigma\gamma\sigma^{-1} \in G(L \mid \sigma(F))$ y

$$\sigma G(L \mid F)\sigma^{-1} \subset G(L \mid \sigma(F)).$$

" $\subset$ " Análogamente, tomando $\tau \in G(L \mid \sigma(F))$ y $\alpha \in F$, entonces

$$\left(\sigma^{-1}\tau\sigma\right)(\alpha) = \sigma^{-1}(\tau(\sigma(\alpha))) = \sigma^{-1}(\sigma(\alpha)) = \alpha.$$

Luego, $\sigma^{-1}\gamma\sigma \in G(L \mid F)$ y

$$\sigma^{-1}G(L \mid \sigma(F))\sigma \subset G(L \mid F),$$

por tanto

$$\sigma G(L \mid F)\sigma^{-1} \supset G(L \mid \sigma(F)),$$

y el lema está demostrado. □

Teorema 4.10. (*Teorema Fundamental de la Teoría de Galois*)**.** Sea $L \mid K$ una extensión finita normal y separable, con $[L:\ K] = n$, $G = G(L \mid K)$,
$\mathcal{F} = \{F;\ K \subset F \subset L\ y\ F\ un\ campo\}$, $\mathcal{H} = \{H;\ H\ es\ subgrupo\ de\ G\}$. Consideremos

$$\begin{array}{rccc} \varphi: & \mathcal{F} & \longrightarrow & \mathcal{H} \\ & F & \longmapsto & \varphi(F) = G(L \mid F) \end{array} \qquad \begin{array}{rccc} \psi: & \mathcal{H} & \longrightarrow & \mathcal{F} \\ & H & \longmapsto & \psi(H) = L_H \end{array}$$

Entonces,

(i) $\mid G \mid = n$.

(ii) φ y ψ invierten las inclusiones, $\varphi \circ \psi = I_{\mathcal{H}}$ $\quad y \quad$ $\psi \circ \varphi = I_{\mathcal{F}}$.

(iii) Sea F un campo intermedio. Entonces,

$$[L:\ F] = \mid G(L \mid F) \mid \quad y \quad [F:\ K] = \frac{\mid G \mid}{\mid G(L \mid F) \mid} = (G:\ G(L \mid F)).$$

(iv) Sea F un campo intermedio. $F \mid K$ es normal, si y solamente si, $G(L \mid F)$ es subgrupo normal de G.

Demostración. (i). Por **Teorema 4.8**, tenemos que $K = L_G$. Por **Teorema 4.7**, obtenemos $\mid G \mid = [L:\ L_G]$. Por lo tanto, $\mid G \mid = [L:\ K] = n$.

(ii). Ya sabemos que φ y ψ invierten inclusiones, $F \subset L_{G(L|F)} = \psi(\varphi(F))$, así como $H \subset G(L \mid L_H) = \varphi(\psi(H))$.

Como $L \mid K$ es normal y separable, entonces $L \mid F$ es normal y separable y, por el **Teorema 4.8** ,

$$L_{G(L|F)} = F, \qquad (1)$$

esto es, $\psi \circ \varphi = I_{\mathcal{F}}$.

Sea ahora H un subgrupo de $G = G(L \mid K)$. Entonces, por la ecuación (1)

$L_{G(L|L_H)} = L_H$. Por **Teorema 4.7**, tenemos que

$\mid H \mid = [L:\ L_H]$.

Por tanto,

$\mid H \mid = [L:\ L_H] = \left[L:\ L_{G(L|L_H)}\right]$.

Por **Teorema 4.7**,

$$\left[L:\ L_{G(L|L_H)}\right] = \mid G(L \mid L_H) \mid .$$

Luego, como $H \subset G(L \mid L_H)$ y esos grupos son finitos, obtenemos que

$H = G(L \mid L_H) = \varphi(\psi(H))$, que es equivalente a, $\varphi \circ \psi = I_{\mathcal{H}}$.

(iii) Sea F un campo intermediario. Entonces, $L \mid F$ es normal y separable y $F = L_{G(L|F)}$.

Entonces, $[L:\ F] =\mid G(L \mid F) \mid$, por lo tanto
$[F:\ K] = \frac{[L:\ K]}{[L:\ F]} = \frac{|G(L|K)|}{|G(L|F)|}$.
(iv) " $\Longrightarrow$ " Por **Teorema 4.6** si tenemos $K \subset F \subset L$ una cadena de campos. Entonces $G(L \mid F)$ es un subgrupo normal de $G(L \mid K) = G$.

" $\Longleftarrow$ "Recíprocamente, supongamos que $H = G(L \mid F) \lhd G(L \mid K)$. Entonces, $\sigma G(L \mid F)\sigma^{-1} = G(L \mid F)$, para cada $\sigma \in G(L \mid K)$. Pero por el lema anterior, para cada $\sigma \in G(L \mid K)$, $\sigma G(L \mid F)\sigma^{-1} = G(L \mid \sigma(F))$. Luego, $G(L \mid \sigma(F)) = G(L \mid F)$, para cada $\sigma \in G(L \mid K)$. Pero por (ii), $\sigma(F) = L_{G(L|\sigma(F))} = L_{G(L|F)} = F$, para cada $\sigma \in G(L \mid K)$. Por lo tanto $\sigma \mid_F$ es un $K - automorfismo$ de F, para cada $\sigma \in G(L \mid K)$.

Sea $\alpha \in F$ y $p(x) \in K[x]$ el polinomio mínimo de sobre K. Entonces, $p(x)$ es separable y tiene todas sus raíces en L. Si $\beta \in L$ es otra raíz de $p(x)$, entonces existe $\sigma \in G(L \mid K)$ tal que $\sigma(\alpha) = \beta$. Luego, $\beta \in F$. Por el **Teorema 9**, esto es equivalente a que $F \mid K$ es el campo de descomposición de un polinomio sobre K. Por lo tanto, $F \mid K$ es normal. □

4.3. La ecuación General de grado n.

Resolvemos ecuaciones de 2°, 3° y 4° grado escribiendo las raíces de la ecuación como radicales de funciones algebraicas racionales de coeficientes de la ecuación. Para la ecuación general de grado $n \geq 5$ no hay formulas explicitas. Vamos a relacionar la solubilidad de la ecuación por radicales con las propiedades de grupos y automorfismos de su campo de raíces.

Dado $f(x) \in K[x] \setminus K$ asociamos $G(f(x) \mid K)$, a un grupo de automorfismos de un campo de raíces L de $f(x)$ sobre K, llamado *el grupo* de *Galois de* $f(x)$ sobre K. Veremos que si $G(f(x) \mid K)$ es soluble, entonces la ecuación es soluble por radicales. Sea K un campo, con $car(K) = 0$ y $x_1, \ldots, x_n$ indeterminadas sobre K. Consideremos $L = K(x_1, \ldots, x_n)$ y el polinomio
$f(x) = (x - x_1)(x - x_2)\cdots(x - x_n) \in L[x]$.
Consideremos las funciones simétricas elementales

$$\begin{aligned} s_1 &= x_1 + \cdots + x_n \\ s_2 &= \sum_{1\leq j\leq n} x_i x_j \\ s_3 &= \sum_{1\leq j<i<k\leq n} x_i x_j x_k \\ &\vdots \\ s_j &= \sum_{1<i_1<\cdots<i_j\leq n} x_{i_1}\cdots x_{i_j} \\ &\vdots \\ s_n &= x_1 \cdots x_n \end{aligned}$$

Sea $F = K(s_1, \ldots, s_n)$. Entonces, $F \subset L$ y podemos reescribir $f(x)$ como:

$$f(x) = x^n - s_1 x^{n-1} + s_2 x^{n-2} + \cdots + (-1)^n s_n \in F[x].$$

Por lo tanto, $f(x) \in F[x]$ se descompone en producto de factores lineales en $L[x]$, $f(x)$ tiene todas sus raíces en L y $F(x_1, \ldots, x_n) = K(x_1, \ldots, x_n) = L$. Luego, L es el campo de raíces de $f(x)$ sobre F. Cada $\sigma \in S_n$ define, de manera natural, un automorfismo de L de la siguiente manera:

Para cada $r(x_1, \ldots, x_n) \in L = K(x_1, \ldots, x_n)$; existen polinomios con coeficiente en K, $g(x_1, \ldots, x_n)$, $h(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$ tales que

$$r(x_1, \ldots, x_n) = \frac{g(x_1, \ldots, x_n)}{h(x_1, \ldots, x_n)}.$$

Definimos $\sigma : L \longrightarrow L$ por

$$\sigma(r(x_1, \ldots, x_n)) = r\left(x_{\sigma(1)}, \ldots, x_{\sigma(n)}\right) = \frac{g(x_{\sigma(1)}, \ldots, x_{\sigma(n)})}{h(x_{\sigma(1)}, \ldots, x_{\sigma(n)})}.$$

Ejemplo 4.3. Sean $\sigma = (1,\ 2,\ 3) \in S_3$ y $r(x_1,\ x_2,\ x_3) = \frac{X_1+X_2}{X_1+X_2-X_3}$. Entonces,

$(r(x_1,\ ,x_2,\ x_3)) = \frac{X_{\sigma(1)}+X_{\sigma(2)}}{X_{\sigma(1)}+X_{\sigma(2)}-X_{\sigma(3)}} = \frac{X_2+X_3}{X_2+X_3-X_1}$.

Ejemplo 4.4. Para todo $\sigma \in S_n$, tenemos que $\sigma(s_j) = s_j$; para $j = 1, \ldots, n$.

S_n es un grupo de automorfismos de L.

El cuerpo fijo de ese grupo es

$L_{S_n} = \{r(x_1, \ldots, x_n) \in L;\ \ \sigma(r) = r\}$,

es llamado el *cuerpo fíjo de las funciones simétricas.*

Se puede observar que $K \subset L_{S_n}$ y por el ejemplo anterior, $s_1, \ldots, s_n \in L_{S_n}$. Por lo tanto, $F = K(s_1, \ldots, s_n) \subset L_{S_n} \subset L$.

Por otro lado por el **Teorema 4.7**,

$$n! = \mid S_n \mid = [L :\ L_{S_n}] \leq [L :\ F] \leq n!.$$

Por lo tanto, $[L:\ L_{S_n}] = [L:\ F] = n!$, $L_{S_n} = F = K(s_1, \ldots, s_n)$ y
$S_n = G(L \mid K(s_1, \ldots, s_n))$.
Se acaba de demostrar el siguiente Teorema.

Teorema 4.10. Sea K un campo, con $car(K) = 0$, y $x_1, \ldots, x_n$ indeterminadas sobre K, $F = K(s_1, \ldots, s_n)$, donde $s_1, \ldots, s_n$ son las funciones simétricas elementales, y $f(x) = x^n - s_1 x^{n-1} + s_2 x^{n-2} + \cdots + (-1)^n s_n \in F[x]$. Entonces, $L = K(x_1, \ldots, x_n)$ es el campo de raíces de $f(x)$ sobre F y $S_n = G(L \mid F)$ es un grupo de automorfismos de $L \mid F$. □

Definición 4.6 (*Grupo soluble*)**.** Un grupo finito G es soluble, si y solamente si, existe una cadena de subgrupos

$$G = N_0 \supset N_1 \supset N_s = \{e\};$$

tal que $N_{j+1} \lhd N_j$ y $\frac{N_j}{N_{j+1}}$ es abeliano, para $j = 0, \ldots, s-1$.

Ejemplo 4.5. Todo grupo abeliano es soluble. Tomamos $G = N_0 \supset N_1 = \{e\}$.

Hay una descripción alternativa para grupos solubles, usando el conmutador de un grupo.

Definición 4.7 (*Conmutador G' de G*)**.** Sean $(G,\ \centerdot)$ un grupo y $a,\ b \in G$. Definimos el conmutador de $a,\ b$ por

$$[a,\ b] = aba^{-1}b^{-1}.$$

El *Conmutador* de G es el subgrupo G' generado por los conmutadores $[a,\ b]$, para cualesquiera $a,\ b \in G$, esto es,

$$\begin{aligned} G' &= < aba^{-1}b^{-1};\ a,\ b \in G > \\ &= \left\{x_1, \ldots, x_n;\ \ n \geq 1,\ x_j = a_j b_j a_j^{-1} b_j^{-1},\ a_j,\ b_j \in G\right\}. \end{aligned}$$

Ejemplo 4.6. Si $(G,\ \centerdot)$ es abeliano $G' = \{e\}$.

Proposición 4.6 (*Propiedades del conmutador*)**.** Sea $(G,\ \centerdot)$ un grupo y G' su conmutador. Entonces:
(i) G' es normal en G.
(ii) G/G' es abeliano.
(iii) Si N es un subgrupo normal de G, tal que G/N es abeliano, entonces $G' \subset N$.

Demostración. (i) Para cada $c \in G$ y $[a;\ b]$, con $a,\ b \in G$, tenemos

$$\begin{aligned} c[a;\ b]c^{-1} &= c\left(aba^{-1}b^{-1}\right)c^{-1} \\ &= (ca)\left(c^{-1}a^{-1}ac\right)\left(ba^{-1}\right)\left(b^{-1}c^{-1}\right) \\ &= \left(cac^{-1}a^{-1}\right)(acb)\left(a^{-1}b^{-1}c^{-1}\right) \\ &= \left(cac^{-1}a^{-1}\right)\left(a\,(cb)\,a^{-1}\,(bc)^{-1}\right) \end{aligned}$$

Para todo, $c \in G$, $x_j = [a_j,\ b_j]$, $j = 1, \cdots, n$, si $x = x_1 x_2 \cdots x_n$, entonces

$$cxc^{-1} = c(x_1 x_2 \cdots x_n)c^{-1} = \left(cx_1c^{-1}\right)\left(cx_2c^{-1}\right)\cdots\left(cx_nc^{-1}\right) \in G'.$$

(ii) Sean $a,\ b \in G$. Entonces,

$$\begin{aligned} G'aG'b &= G'ab \\ &= G'(ab)(a^{-1}b^{-1}ba) \\ &= G'(aba^{-1}b^{-1})ba \\ &= G'ba \\ &= G'bG'a \end{aligned}$$

(iii) Sea $N \lhd G$ con G/N abeliano. Entonces,

$$\begin{aligned} NaNb = NbNa &\iff Nab = Nba \\ &\iff ab(ba)^{-1} \in N \\ &\iff aba^{-1}b^{-1} \in N. \end{aligned}$$

Luego, $G^{-1} = aba^{-1}b^{-1}$, para cualesquiera $a,\ b \in G \subset N$. □

Procedemos ahora por inducción.

G' es un grupo. Definimos $G^{(2)} = (G')'$ un subgrupo de G' generado por $a'b'a'^{-1}b'^{-1}$ con $a',\ b' \in G'$.

Continuando de este modo definiendo $G^{(m+1)} = \left(G^{(m)}\right)'$.

Tomando $G^{(1)} = G'$. Por la proposición anterior, $G^{(m+1)} \lhd G^{(m)}$ y $G^{(m)}/G^{(m+1)}$ es un grupo abeliano. □

Proposición 4.7. $(G,\ \cdot)$ es un grupo soluble si, y solamente si, $G^{(r)} = \{e\}$, para algún $r \geq 1$.

Demostración. " $\Longleftarrow$ " Sea $r \geq 1$ tal que $G^{(r)} = \{e\}$. Consideremos $N_0 = G$, $N_1 = G^{(1)}, \cdots, N_r = G^{(r)} = \{e\}$. Entonces,

$$G = N_0 \supset N_1 \supset \cdots \supset N_r = \{e\}$$

es una cadena de sugbrupos de G. Por la proposición anterior, obtenemos que $N_{j+1} = G^{(j+1)} \lhd G^{(j)} = N_j$ y $N_{(j)}/N_{(j+1)} = G^{(j)}/G^{(j+1)}$ es abeliano. Por lo tanto G es soluble.

" $\Longrightarrow$ " Supongamos que G es soluble. Entonces, existe una cadena de subgrupos

$$G = N_0 \supset N_1 \supset \cdots \supset N_r = \{e\},$$

tal que $N_{j+1} \lhd N_j$ y $N_{(j)}/N_{(j+1)}$ es abeliano. Pero por ítem (iii) de la proposición anterior, tenemos que $N_j' \subset N_{j+1}$. Luego,

$$\begin{array}{rcccl} N_1 \supset N_0' & = & G' & \Longrightarrow & N_1 \supset G^{(1)} \\ N_2 \supset N_1' \supset (G')' & = & G^{(2)} & \Longrightarrow & N_2 \supset G^{(2)} \\ N_3 \supset N_2' \supset \left(G^{(2)}\right)' & = & G^{(3)} & \Longrightarrow & N_3 \supset G^{(3)} \end{array}$$

Inductivamente, tenemos que $N_j \supset G^{(j)}$ y $\{e\} = N_r \supset G^{(r)} = \{e\}$. Por lo tanto $G^{(r)}\{e\}$. □

Proposición 4.8. (*Propiedades adicionales*) Las siguientes afirmaciones son válidas:

(i) Si H es un subgrupo de G y G es soluble, entonces H es soluble.

(ii) Si G es soluble y $\varphi:\ G \longrightarrow \overline{G}$ es un homomorfismo sobreyectivo, entonces $\overline{G}$ es soluble. En particular si $N \lhd G$ y G es soluble, entonces G/N es soluble.

(iii) Sea $N \lhd G$. Si N es soluble y G/N es soluble, entonces G es soluble.

Demostración. (i) Primeramente observemos que:

$H < G \Longrightarrow H' < G' \Longrightarrow H^{(2)} < G^{(2)}$. Por inducción, $H^{(j)} < G^{(j)}$, para todo $j \geq 1$.

Si G es soluble, entonces existe $r \geq 1$ tal que $G^{(r)} = \{e\}$. Por la observación anterior, $H^{(r)} \subset G^{(r)}$. Luego, $H^{(r)} = \{e\}$ y H es soluble.

(ii) $\overline{G}' = \left\{\overline{x_1}, \ldots, \overline{x_n};\ \overline{x_j} = \overline{a_j}\overline{b_j}\overline{a_j}^{-1}\overline{b_j}^{-1};\ \overline{a_j},\ \overline{b_j} \in \overline{G}\right\}$

Como φ es un homomorfismo sobreyectivo, para cada $\overline{a} \in \overline{G}$, existe $a \in G$ tal que $\overline{a} = \varphi(a)$ y $\overline{a}^{-1} = \varphi(a^{-1})$. Luego

$$\overline{x}_j = \overline{a_j}\overline{b_j}\overline{a_j}^{-1}\overline{b_j}^{-1} = \varphi(a_j)\,\varphi(b_j)\,\varphi\left(a_j^{-1}\right)\varphi\left(b_j^{-1}\right) = \varphi\left(a_j b_j a_j^{-1} b_j^{-1}\right)$$

Así,

$$\overline{G}' = \left\{\overline{x_1}.\cdots.\overline{x_n};\ \overline{x_j} = \varphi\left(a_j b_j a_j^{-1} b_j^{-1}\right);\ a_j,\ b_j \in G\right\} = \varphi(G').$$

Inductivamente, $\overline{G}^{(n)} = \varphi\left(G^{(n)}\right)$, para todo $n \geq 1$. Tomando $r \geq 1$ tal que $G^{(r)} = \{e\}$, tenemos que $\overline{G}^{(r)} = \varphi\left(G^{(r)}\right) = \varphi(e) = \overline{e}$, mostrando que $\overline{G}$ es soluble.

Para la última afirmación, se toma el homomorfismo de grupos sobreyectivo

$\pi:\ G \longrightarrow G/N$.

(iii) Sea $N \lhd G$. Supongamos que N y G/N son solubles.

Sea

$$\overline{G_0} = G/N \supset \overline{G_1} \supset \cdots \supset \overline{G_s} = \{\overline{e}\} \qquad (1)$$

una cadena de subgrupos de G/N, tal que $\overline{G_{j+1}} \lhd \overline{G_j}$ y $\overline{G_j}/\overline{G_{j+1}}$ es abeliano.

Sea

$$N = N_0 \supset N_1 \supset \cdots \supset N_r = \{e\} \qquad (2)$$

La cadena de subgrupos de N, tal que $N_{j+1} \lhd N_j$ y N_j/N_{j+1} es abeliano.
De la cadena (1) tenemos $\overline{G_j} = G_j/N$, donde $N < G_j < G$ y $G_{j+1} \lhd G_j$.
Así, (1) induce una cadena

$$G = G_0 \supset G_1 \supset \cdots \supset G_s = N. \qquad (3)$$

Además, un homomorfismo sobreyectivo

$$\begin{array}{rccccc} \psi: & \overline{G_j} & = & G_j/N & \longrightarrow & G_j/G_{j+1} \\ & & & Nx & \longmapsto & G_{j+1}x \end{array}$$

con $N\acute{u}cleo\,(\psi) = G_{j+1}/N = \overline{G_{j+1}}$, pero por teorema fundamental de homomorfismos, induce un isomorfismo de $\overline{G_j}/\overline{G}_{j+1}$ con G_j/G_{j+1}. Como
$\overline{G_j}/\overline{G_{j+1}}$es abeliano, entonces G_j/G_{j+1} es abeliano.

$$G = G_0 \supset G_1 \supset \cdots \supset G_s = N \qquad (3)$$

Completando la cadena (3) con la cadena (2), obtenemos

$$G = G_0 \supset G_1 \supset \cdots \supset G_s = N = N_0 \supset N_1 \supset \cdots \supset N_r = \{e\},$$

que es la cadena buscada para G. □

Lema 4.6. Sea $G = S_n$, con $n \geq 5$. Entonces, $G^{(r)}$; para $r = 1,\ 2, \cdots$, contiene cada $3-ciclo$ de S_n. En particular, S_n no es soluble, para $n \geq 5$.

Demostración. En primer lugar, observemos que si G es un grupo y $N \lhd G$, entonces $N' \lhd G$.
En efecto, sean $c,\ d \in N$ y $a \in G$. Entonces, $cdc^{-1}d^{-1} \in N'$ y

$$a\left(cdc^{-1}d^{-1}\right)a^{-1} = \underbrace{\left(aca^{-1}\right)}_{c_1}\underbrace{\left(ada^{-1}\right)}_{d_1}\underbrace{\left(ac^{-1}a^{-1}\right)}_{c_1^{-1}}\underbrace{\left(ad^{-1}a^{-1}\right)}_{d_1^{-1}} \in N',$$

pues $c_1\ , d_1,\ c_1^{-1},\ d_1^{-1} \in N$.
Afirmamos ahora que si $n \geq 5$ y N es un subgrupo normal de S_n que contiene cada $3-ciclo$ de S_n, entonces su conmutador N' también contiene cada $3-ciclo$ de S_n.
En efecto, supongamos que $\sigma = (1,\ 2,\ 3)$ y $\tau = (1,\ 4,\ 5)$ están en N.
Entonces, $\sigma^{-1} = (2,\ 1,\ 3)$, $\tau^{-1} = (4,\ 1,\ 5)$ y

$$\begin{array}{rcl} \sigma\tau\sigma^{-1}\tau^{-1} & = & (1,\ 2,\ 3)\,(1,\ 4,\ 5)\,(2,\ 1,\ 3)\,(4,\ 1,\ 5) \\ & = & \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 1 & 5 \end{pmatrix} \qquad = (1,\ 2,\ 4) \in N'. \end{array}$$

Como, $N' \lhd G$ para todo $\xi \in S_n$ tenemos que $\xi(1;2;4)\xi^{-1} \in N'$. Elijamos $\xi \in S_n$ tal que $\xi(1) = i_1$, $\xi(2) = i_2$ y $\xi(4) = i_3$, con $i_1,\ i_2,\ i_3$ distintos, $1 \leq i_1,\ i_2, i_3 \leq n$ y

$\xi(j) = j$, para todo $j \neq 1,\ 2,\ 4$. Entonces,

$$\xi(1,\ 2,\ 4)\xi^{-1} = (i_1,\ i_2,\ i_3) \in N'.$$

Luego, N' contiene todo $3-ciclo$ de S_n.

Tomando $N = G = S_n$, tenemos que $N \lhd G$ y N contiene todos $3-ciclos$ de S_n. Como $G' \lhd G$, entonces $G^{(2)}$ contiene todos los $3-ciclos$ de S_n. Como $G^{(2)} \lhd G$, entonces $G^{(3)}$ contiene todos los $3-ciclos$ de S_n. Continuando de esa manera, $G^{(r)}$, para todo $r \geq 1$, contiene todos los $3-ciclos$ de S_n y, en particular, $G^{(r)} \neq \{I\}$, mostrando que S_n no es soluble para $n \geq 5$. □

Definición 4.8. Una extensión $M \mid K$ se dice que es radical si existe una torre, la cual llamaremos *torre radical simple*, definida de la siguiente manera

$$K = K_0 \subset K_1 \subset \cdots \subset K_s = M,$$

tal que, para $j = 1, \cdots, s$, existen $\alpha_j \in K_j,\ n_j \geq 1$, con $\alpha_j^{n_j} \in K_{j-1}$ y $K_j = K_{j-1}(\alpha_j)$.

Ejemplo 4.7. Son extensiones radicales:

1. $\mathbb{Q}\left(\sqrt[4]{2}\right) \mid \mathbb{Q}$ con $\mathbb{Q} \subset \mathbb{Q}\left(\sqrt[4]{2}\right)$, como torre radical simple.
2. $\mathbb{Q}\left(\sqrt{3},\ \sqrt{\sqrt[3]{5}+\sqrt[3]{2}}\right) \mid \mathbb{Q}$ como lo muestra la siguiente torre radical simple

$$\mathbb{Q} \subset \mathbb{Q}\left(\sqrt{3}\right) \subset \mathbb{Q}\left(\sqrt{3},\ \sqrt[3]{5}\right) \subset \mathbb{Q}\left(\sqrt{3},\ \sqrt[3]{5},\ \sqrt[3]{2}\right) \subset \mathbb{Q}\left(\sqrt{3},\ \sqrt{\sqrt[3]{5}+\sqrt[3]{2}}\right) \mid \mathbb{Q}.$$

Definición 4.99. (*Polinomio soluble por radicales*). Sea $f(x) \in K[x] \setminus K$ y L el campo de raíces de $f(x)$ sobre K. El polinomio $f(x)$ es *soluble por radicales* si, y solamente si, existe una extensión radical $M \mid K$, tal que $L \subset M$.

Proposición 4.99. Sea $M \mid K$ una extensión radical. Entonces, existe una extensión radical normal $N \mid K$, tal que $M \subset N$.

Demostración. Se considera una torre radical simple

$$K = K_0 \subset K_1 \subset \cdots \subset K_s = M,$$

donde para $j = 1, \cdots, s$, existen $\alpha_j \in K_j,\ n_j \geq 1$, con $\alpha_j^{n_j} \in K_{j-1}$ y $K_j = K_{j-1}(\alpha_j)$. Sea N un campo de raíces sobre K de $p_1(x), \cdots, p_s(x)$, donde $p_j(x)$ es el polinomio mínimo de α_j sobre K. Para mostrar que $N \mid K$ es una extensión radical precisamos construir una torre radical simple. Haremos la construcción en el caso de $s = 2$ y la demostración es por inducción sobre s.

Sea $M \mid K$ una extensión radical con $M = K(\beta,\ \gamma)$ $\beta^n \in K$ *y* $\gamma^m \in K(\beta)$.

Así,

$$K \subset K(\beta) \subset K(\beta)(\gamma) = M.$$

es una torre radical simple.

Sean $p(x)$, $q(x)$ los polinomios mínimos de β y γ sobre K. Sean $\beta = \beta_1, \cdots, \beta_r$ y $\gamma = \gamma_1, \cdots, \gamma_s$ las raíces de $p(x)$ y $q(x)$, respectivamente. Vamos a mostrar que $N \mid K$ es radical, donde $N = K(\beta_1, \cdots, \beta_r, \gamma_1, \cdots, \gamma_s)$ es el campo de descomposición de $p(x)q(x)$ sobre K. Una torre radical simple es

$$K \subset K(\beta_1) \subset K(\beta_1)(\beta_2) \subset \cdots \subset K(\beta_1, \ldots, \beta_{r-1})(\beta_r) = L$$

completada con

$$L \subset L(\gamma_1) \subset L(\gamma_1)(\gamma_2) \subset \cdots \subset L(\gamma_1, \ldots, \gamma_{s-1})(\gamma_s) = N.$$

Es claro que $M \subset N$, L el campo de descomposición de $p(x)$ sobre K y $L(\gamma_1, \ldots, \gamma_s)$ es el campo de descomposición de $q(x)$ sobre L.

Para cada $j = 1, \ldots, r$, existe $K - automorfismo\ \tau : N \longrightarrow N$ tal que $\tau(\beta) = \beta_j$. Como $\beta^n = a \in K$, entonces

$$\beta_j^n = \tau(\beta)^n = \tau(\beta^n) = \tau(a) = a \in K \subset K(\beta_1, \ldots, \beta_{j-1}),$$

para cada $j \geq 2$.

Para cada $j = 1, \ldots, s$, existe $K - automorfismo\ \sigma : N \longrightarrow N$ tal que $\sigma(\gamma) = \gamma_j$ y $\sigma \mid_L$ es un $K - automorfismo$ de L, pues $L \mid K$ es normal. Como $\gamma^m = f(\beta) \in K(\beta) \subset L$, para algún polinomio $f(x) \in K[x]$, entonces $\sigma(\beta) \in L$ y

$$\gamma_j^m = \sigma(\gamma)^m = \sigma(\gamma^m) = \sigma(f(\beta)) = f(\sigma(\beta)) \in L \subset L(\gamma_1, \ldots, \gamma_{j-1}),$$

para cada $j \geq 2$. □

Teorema 4.11. Sea K un campo con característica cero, que contiene una $n-ésima$ raíz primitiva de la unidad. Sean $a \in K$, $a \neq 0$, $f(x) = x^n - a \in K[x]$ y L el campo de raíces de $f(x)$ sobre K. Entonces:

(i) $L = K(b)$, donde b es cualquier raíz de $f(x)$.

(ii) $G(L \mid K)$ es abeliano.

Demostración. (i) Sea ω una raíz primitiva $n - ésima$ de la unidad. Entonces, $1, \omega, \ldots, \omega^{n-1}$ son las $n - raíces$ de la unidad y, tomando b tal que $b^n = a$, tenemos que $b\omega^j$, con $j = 0, 1, \ldots, n-1$, son las n raíces de $x^n - a$ y

$$x^n - a = (x - b)(x - b\omega) \cdots \left(x - b\omega^{n-1}\right).$$

Como $\{1,\ \omega, \ldots,\ \omega^{n-1}\} \subset K$, tenemos que $L = K(b)$ es un campo de raíces de $f(x)$ sobre K.

(ii) Sean $\sigma,\ \tau \in G(L \mid K)$. Como $\sigma(b)$ y $\tau(b)$ son raíces de $x^n - a$, entonces $\sigma(b) = b\omega^i$ y $\tau(b) = b\omega^j$, para algún $i,\ j$ con $i \geq 0$, $j \leq n-1$.

Por lo tanto,

$$\begin{array}{rcccccccccc} (\sigma \circ \tau)(b) & = & \sigma(\tau(b)) & = & \sigma(b\omega^j) & = & \omega^j \sigma(b) & = & \omega^j(\omega^i b) & = & \omega^{j+i} b \ \ y \\ (\tau \circ \sigma)(b) & = & \tau(\sigma(b)) & = & \tau(b\omega^i) & = & \omega^i \tau(b) & = & \omega^i(\omega^j b) & = & \omega^{i+j} b. \end{array}$$

Luego $(\sigma \circ \tau)(b) = (\tau \circ \sigma)(b)$. Como $L = K(b)$, entonces $\sigma \circ \tau = \tau \circ \sigma$ en L, mostrando que $G(L \mid K)$ es abeliano. □

Teorema 4.12. Sea $f(x) \in K[x] \setminus K$ es soluble por radicales, entonces $G(L \mid K)$ es soluble, donde L es un campo de raíces de $f(x)$ sobre K.

Demostración. Supongamos que $f(x) \in K[x]$ es soluble por radicales. Entonces existe una torre radical $N \mid K$ tal que

$$K_1 = K \subset K_2 \subset \cdots \subset K_s = N,$$

existen $\alpha_j \in K_j$, $n_j \geq 1$, tales que $\alpha_j^{n_j} \in K_{j-1}$, $K_j = K_{j-1}(\alpha_j)$, para cada $j = 2, \ldots,\ s$ y $L \subset N$.

Por la *proposición* 4.9 podemos suponer que $N \mid K$ es normal. Sea $n = mcd(n_2, \ldots,\ n_s)$ y ω una raíz primitiva $n - ésima$ de la unidad. Consideremos $K_{s+1} = K_s(\omega)$.

Vamos a construir una nueva torre para tener control sobre el grupo de automorfismos y así usar la correspondencia de Galois.

Tomemos $L_0 = K_1 = K$, $L_1 = K(\omega)$ y $L_j = L_{j-1}(\alpha_j)$, para cada $j \geq 2$.

Observamos que $\omega^{\frac{n}{n_j}} \in L_{j-1}$ es una raíz primitiva $n_j - ésima$ de la unidad.

Por inducción tenemos que $L_j = K_j(\omega)$. De modo que $L_s = K_s(\omega) = K_{s+1} = N(\omega)$.

Veamos el diagrama a seguir.

$$\begin{array}{ccc} K_{s+1} = K_s(\omega) & = & L_s = L_{s-1}(\alpha_s) \\ | & \nearrow & | \\ N = K_s & & | \\ | & & \cdots \\ \cdots & & L_2 = L_1(\alpha_2) = K_2(\omega) \\ | & \nearrow & | \\ K_2 & & L_1 = K(\omega) \\ | & \nearrow & \\ K = K_1 = L_0 & & \end{array}$$

Para $j = 2, \cdots, s$ tenemos que $L_j = L_{j-1}(\alpha_j)$ y L_j es campo de descomposición de $x^{n_j} - \alpha_j^{n_j}$ sobre L_{j-1}, pues L_{j-1} tiene raíz primitiva $n_j - ésima$ de la unidad. Luego $L_j \mid L_{j-1}$ es una extensión normal y separable. Pero por el teorema anterior, $G(L_j \mid L_{j-1})$ es abeliano, para $j = 2, \cdots, s$. $L_1 \mid L_0$ es normal y separable, pues $G(L_1 \mid L_0) = G(K(\omega) \mid K)$ es abeliano.

De hecho, cada $\sigma \in G(K(\omega) \mid K)$ esta perfectamente determinado por $\sigma(\omega)$ y $\sigma(\omega)$ debe ser una $n - ésima$ raíz primitiva de la unidad. Por lo tanto existe un único i, con $1 \leq i \leq n$, $mcd(i,\ n) = 1$, tal que $\sigma(\omega) = \omega^i$. Así, $G(K(\omega) \mid K) \simeq subgrupo\ \mathbb{Z}_n^*$ con un homomorfismo inyectivo

$$\begin{array}{rccc} \varphi\ :\ G(K(\omega) \mid K) & \longrightarrow & \mathbb{Z}_n^* \\ \sigma & \longmapsto & \overline{i} = i\ mod(n), \end{array}$$

consideremos una cadena de cuerpos

$$L_0 = K \subset L_1 \subset L_2 \subset \cdots \subset L_{s-1} \subset L_s$$

con $L_s \mid K$ normal y separable.

Tomando $G = G(L_s \mid K)$ y $G_j = G(L_s \mid L_j)$, para la correspondencia de Galois, tenemos la cadena de grupos

$$G \supset G_1 \supset \cdots \supset G_{s-1} \supset G_s = \{I\} \qquad (\star)$$

Como $L_j \mid L_{j-1}$ es normal, entonces $G_j \lhd G_{j-1}$ y $G_{j-1} \mid G_j \simeq G(L_j \mid L_{j-1})$ es abeliano.

Luego, la cadena $(\star)$ de subgrupos de $G(L_s \mid K)$, muestra que $G(L_s \mid K)$ es soluble. Por hipótesis, L, el campo de descomposición de $f(x)$ sobre K

$$K \subset L \subset N \subset L_s.$$

Por teorema de *Galois*, $G(L \mid K) \simeq G(L_s \mid K)/G(L_s \mid L)$. Como $G(L_s \mid K)$ es soluble, entonces su subgrupo $G(L_s \mid L)$ también es soluble. Como $L_s \mid L$ es normal, entonces $G(L_s \mid L) \lhd G(L_s \mid K)$ y el grupo cociente es soluble. □

Corolario 2. El polinomio general de grado $n \geq 5$ no es soluble por radicales.

Demostración. Por el contrarrecíproco del teorema anterior y por *Lema* 5. □

Capítulo 5

Ideales en el anillo de Polinomios.

El teorema de la base de Hilbert apareció en su famoso artículo Hilbert D. “Uber die Theorie der algebraische Formen, Math. Ann. (1890)”. De esta obra surgierón totalmente nuevos métodos, utilizando que se habia demostrado la existencia de una base finita de forma invariante. Anteriormente, en 1868, Gordan demostró la existencia de una base finita sólo para formas binarias. Hilbert, por el contrario, logró resolver una serie de problemas centrales de la teoría invariante. Sus métodos, sin embargo, no fueron constructivas y esto impulsó a Gordan a quejarse: "Esto no es matemática, esto es teología"

5.1. Teorema de la Base de Hilbert y Teorema de los Ceros de Hilbert.

5.1.1 Teorema de la base de Hilbert

Definición 5.1. Un subconjunto $I \subset K[x_1, \ldots, x_n]$ es llamado un *ideal* si cumple las dos condiciones siguientes:

1) $a,\ b \in I \Longrightarrow a + b \in I$

2) $a \in I,\quad f \in K[x_1, \ldots, x_n] \Longrightarrow fa \in I.$

Para cada conjunto $M \subset K[x_1, \ldots, x_n]$ podemos considerar el ideal $I(M)$ generado por M que consta de todas las sumas de la forma $\lambda_1 m_1 + \cdots + \lambda_r m_r$, donde $\lambda_i \in$

$K[x_1, \ldots, x_n]$ y $m_i \in M$.

Definición 5.2. Una colección $\{a_\alpha \mid a_\alpha \in I\}$ es llamado una *base* del ideal I si cualquier elemento $a \in I$ puede ser representado en la forma $a = \lambda_1 a_{\alpha 1} + \cdots + \lambda_t a_{\alpha t}$, donde $\lambda_i \in K[x_1, \cdots, x_n]$. El ideal I es llamado *finitamente generado* si posee una base finita.

Definición 5.3. Un anillo conmutativo A se llama *noetheriano* si todo ideal I de A es finitamente generado.

Definición 5.4. Un anillo A se dice noetheriano si cada cadena ascendente $I_1 \subset I_2 \subset \cdots \subset I_n \subset \cdots$ es estacionaria.

Teorema 5.1 (*Teorema de la base de Hilbert*) . Si A es un anillo noetheriano, entonces el anillo de polinomios $A[x]$ es también noetheriano. En particular, si K es un campo, $K[x]$ es un anilllo noetheriano. De aquí: $K[X, Y] = K[X][Y]$ también es noetheriano; y por un proceso inductivo, $K[X_1, X_2, \ldots, X_n]$ es un anillo noetheriano.

Demostración. Dado el ideal I de $A[x]$, probaremos que I es finitamente generado. En efecto para $j \geq 0$, sea:

$I_j = \{0\} \cup \{r \in A/\ a_0 + a_1 x + \cdots + r x^j \in I\}$; es decir, I_j está formado por el elemento 0 de A y los coeficientes principales de los polinomios de grado j en I.

Afirmación 1

Para todo $j \geq 0$, I_j es un ideal de A y $I_j \subset I_{j+1}$.

En efecto, para r y $t \in I_j$ y $a \in A$. Si $r - t = 0$, se tiene que: $r - t \in I_j$.

Si $r - t \neq 0$, sean

$$f(x) = a_0 + a_1 x + \cdots r x^j \ \ y \ \ g(x) = b_0 + b_1 x + \cdots + t x^j \ en\ I.$$

Entonces:

$$f(x) - g(x) = (a_0 - b_0) + \cdots + (r - t) x^j \in I.$$

De aquí $r - t \in I_j$. Por otro lado

$$a.f(x) = (a a_0) + (a a_1) x + \cdots + (ar) x^j \in I,$$

es decir que $ar \in I_j$.

Luego, I_j es un ideal de A, $\forall j = 0,\ 1, \ldots$

Para ver que $I_j \subset I_{j+1}$, sea $r \in I_j$. Si $r = 0$, entonces $r \in I_{j+1}$.

Si $r \neq 0$, sea $f(x) = a_0 + \cdots + rx^j \in I$, y como $x \in A[x]$ se tiene:

$h(x) = xf(x) = a_0x + \cdots + rx^{j+1} \in I$, es decir: $r \in I_{j+1}$, luego $I_j \subset I_{j+1}$. Lo que completa la afirmación 1.

De la afirmación 1 y la definición 5.4, que para la cadena $I_0 \subset I_1 \subset I_2 \subset \cdots$ de ideales del anillo noetheriano A, existe $m \geq 0$ tal que $I_h = I_m$, $\forall h \geq m$, es decir, la cadena se estaciona; y los ideales $I_0,\ I_1, \ldots,\ I_m$ son finitamente generados, es decir existen $a_{i_1},\ a_{i_2}, \ldots, a_{in_i}$ en A para cada $i = 0,\ 1, \ldots,\ m$, tales que: $I < a_{i_1},\ a_{i_2}, \ldots, a_{in_i} >$ donde cada a_{ij} es 0 ó es coeficiente principal de polinomios $f_{ij}(x)$, para $i = 0,\ 1, \ldots,\ m$ y $j = 0,\ 1, \ldots,\ n_i$ y $f_{ij}(x) \in I$ de grado i.

Afirmación 2.

El ideal I es generado por los polinomios $f_{ij}(x)$ con $i = 0,\ 1, \ldots,\ m$ y

$j = 0,\ 1, \ldots,\ n_i$; es decir $I =< f_{ij}(x) >$.

En efecto, como $f_{ij}(x) \in I$, $\forall i$ y $\forall j$, se tiene:

$$< f_{ij}(x),\ i = 0,\ 1, \ldots,\ m;\ j = 0,\ 1, \ldots,\ n_i > \subset I.$$

Recíprocamente, sea $f(x) = b_0 + b_1x + \cdots +\ b_dx^d \in I$ de grado d.

Considerando inducción sobre d, se tiene para $d = 0$, $f(x) = b_0 \in I_0 \subset < f_{ij}(x) >$

Asumiendo que todo polinomio de grado no mayor que $d-1$ en I es combinación de los polinomios $f_{ij}(x)$, $i = 0,\ 1, \ldots,\ m$ y $j = 0,\ 1, \ldots,\ n_i$. Si $d > m$, entonces $I_d = I_m$. De aquí, cada coeficiente de b_d en I_d es de la forma: $b_d = c_1a_{m_1} + c_2a_{m_2} + \cdots + c_{n_m}a_{mn_m}$, con $c_1, \ldots,\ c_{n_m} \in A$.

Luego:

$$F(x) = f(x) - x^{d-m}\left(c_1f_{m_1}(x) + c_2f_{m_2}(x) + \cdots + c_{n_m}f_{mn_m}(x)\right) \in I,$$

pues $f(x)$ y $f_{ij}(x)$ están en I; además, el coeficiente de x^d en $F(x)$es:

$b_d - \sum_{j=1}^{n_m} c_ja_{mn_j} = 0$,

por lo que el grado de $F(x)$ es menor que d.

Por el proceso inductivo, se tiene que $F(x)$ es una combinación de los polinomios $f_{ij}(x)$. De aquí:

$$f(x) = F(x) + x^{d-m}\left(c_1f_{m_1}(x) + c_2f_{m_2}(x) + \cdots + c_{n_m}f_{mn_m}(x)\right);$$

es decir : $f(x) \in < f_{ij}(x) >$.

Si $d \leq m$, para d_b en I_d, existen $e_1,\ e_2, \ldots,\ e_{n_d}$ en A tal que:

$b_d = e_1a_{d_1} + e_2a_{d_2} + \cdots + e_{n_d}a_{dn_d}$. Luego:

$G(x) = f(x) - e_1 f_{d_1}(x) + e_2 f_{d_2}(x) + \cdots + e_{n_d} f_{dn_d}(x) \in I$ y tiene grado menor que d. De aquí, por proceso inductivo, $G(x)$ es combinación de los

$f_{ij}(x)$; por lo que :

$$f(x) = G(x) + e_1 f_{d_1}(x) + e_2 f_{d_2}(x) + \cdots + e_{n_d} f_{dn_d}(x)$$

es combinación lineal de los $f_{ij}(x)$.

En consecuencia, $I =< f_{ij}(x),\ i = 0,\ 1, \ldots,\ m;\ j = 0,\ 1, \ldots,\ n_i >$, con lo que se asegura el resultado del teorema. □

5.1.2 Teorema de los ceros de Hilbert

Definición 5.5 (*definición de variedad*)**.** Sea k un campo. Una variedad $V \subset k^n$ es un subconjunto de la forma

$$V = V(J) = \{P = (a_1, a_2, ..., a_n) \in k^n / f(P) = 0 \ \ \forall f \in J\},$$

donde $J \subset k[X_1, X_2, ..., X_n]$ es ideal. Hay que notar que $J = (f_1, ..., f_m)$ es finitamente generado, de manera que una variedad V está definida por

$$f_1(P) = \cdots = f_m(P) = 0,$$

es decir, este es un subconjunto $V \subset k^n$ definido como las soluciones simultáneas de un número de ecuaciones polinómicas.

La correspondencia V e I

Una variedad $X \subset k^n$ es por definición igual a $X = V(J)$, donde J es un ideal de $k[X_1, ..., X_n]$; así V induce el mapeo:

$$\begin{array}{ccc} \{Ideales\, de\, k[X_1, X_2, ..., X_n]\} & \xrightarrow{V} & \{Subconjuntos\, X\, de\, k^n\} \\ J & \rightsquigarrow & V(J) \end{array}$$

y también se tiene

$$\begin{array}{ccc} \{Subconjuntos\, X\, de\, k^n\} & \xrightarrow{I} & \{Ideales\, de\, k[X_1, X_2, ..., X_n]\} \\ X & \rightsquigarrow & I(X) \end{array}$$

donde

$$I(X) = \{f \in k[X_1, ..., X_n] / f(P) = 0 \ \ \forall P \in X\}.$$

Se demostrará que $I(X)$ es un ideal de $k[X_1, X_2, ..., X_n]$.

Para ello en primer lugar se probará que $I(X)$ es un subgrupo de $k[X_1,\ X_2, ..., X_n]$.

Sean $f,\ g \in I(X)$ entonces tenemos que

$$f(P) = 0 = g(P), \quad \forall P \in X$$

Sea $P' \in X$ arbitrario entonces

$$(f-g)(P') = f(P') - g(P') = 0.$$

Por lo tanto $I(X)$ es un subgrupo de $k[X_1, X_2, ..., X_n]$.

Ahora, se prueba que $I(X)$ cumple la propiedad de absorción.

Sea $g \in k[X_1, X_2, ..., X_n]$ y $f \in I(X)$. Se probará que $gf \in I(X)$.

Sea $P \in X$ entonces $gf(P) = g(P) f(P) = 0$

$\Rightarrow gf \in I(X)$.

Así se cumple la propiedad de absorción.

Por lo tanto $I(X)$ es un ideal de $k[X_1, X_2, ..., X_n]$.

Propiedades:

- Sean $J, J' \in k[X_1, X_2, ..., X_n]$. Si $J \subset J'$ entonces $V(J) \supset V(J')$ ya que si $P \in V(J')$ entonces $f(P) = 0 \ \forall f \in J' \supset J$ así $P \in V(J)$.
- Si $X \subset Y$ entonces $I(X) \supset I(Y)$ pues si $f \in I(Y)$ entonces $f(P) = 0$ $\forall P \in Y \supset X$ así $f \in I(X)$.

Corolario 5.1. Suponga que k es algebraicamente cerrado. Entonces cada ideal maximal m de $A = k[X_1, X_2, ..., X_n]$ es de la forma

$$m = (X_1 - a_1, ..., X_n - a_n)$$

para algunos $a_1, ..., a_n \in k$.

Demostración. En primer lugar notemos que $(X_1 - a_1, ..., X_n - a_n)$ es un ideal maximal. Para ello sea $f \notin (X_1 - a_1, ..., X_n - a_n)$, aplicamos el algoritmo de la división como sigue:

$$f = A_1 (X_1 - a_1) + B_1,$$

donde $A_1 \in k[X_1, X_2, ..., X_n]$ y $B_1 \in k[X_2, ..., X_n]$. Hay que observar que $B_1 \neq 0$ pues de lo contrario $f \in (X_1 - a_1, ..., X_n - a_n)$.

$$B_1 = A_2 (X_2 - a_2) + B_2,$$

con $A_2 \in k[X_2, ..., X_n]$, $B_2 \in k[X_3, ..., X_n]$, otra vez $B_2 \neq 0$ pues de lo contrario $f \in (X_1 - a_1, ..., X_n - a_n)$.

$$\vdots$$

$$B_{n-1} = A_n (X_n - a_n) + B_n,$$

con $A_n \in k[X_n]$, $B_n \in k$, otra vez $B_n \neq 0$ pues de lo contrario

$f \in (X_1 - a_1, ..., X_n - a_n)$.

Con esto se tiene que:

$$f = A_1 (X_1 - a_1) + A_2 (X_2 - a_2) + ... + A_n (X_n - a_n) + B_n$$

Entonces

$$1 - B_n^{-1} f = 1 - \left[B_n^{-1} A_1 (X_1 - a_1) + ... + B_n^{-1} A_n (X_n - a_n) + B_n^{-1} B_n\right]$$

$$1 - B_n^{-1} f = B_n^{-1} A_1 (X_1 - a_1) + B_n^{-1} A_2 (X_2 - a_2) + ... + B_n^{-1} A_n (X_n - a_n)$$

pero

$$B_n^{-1} A_1 (X_1 - a_1) + ... + B_n^{-1} A_n (X_n - a_n) \in (X_1 - a_1, ..., X_n - a_n)$$

con $B_n^{-1} \in k[X_1, X_2, ..., X_n]$. Por tanto $(X_1 - a_1, ..., X_n - a_n)$ es maximal.

Ahora se observa que m tiene la forma $(X_1 - a_1, ..., X_n - a_n)$ donde m es maximal. Para ello sea $K = k[X_1, ..., X_n]/m$, entonces $k \subset K$ es una extensión algebraica. Pero ya que k es algebraicamente cerrado no tiene extensiones propias y así se tiene que $k = K$.

Si $X_i \in A$ mapea a a_i en el cociente $K = k$ entonces el mismo elemento $a_i \in k \subset A$ también mapea a a_i, entonces $X_i - a_i \in m$ para $i = 1, ..., m$ y entonces $m \supset (X_1 - a_1, ..., X_n - a_n)$.

Como $(X_1 - a_1, ..., X_n - a_n)$ es ideal maximal entonces

$$(X_1 - a_1, ..., X_n - a_n) = m \quad o \quad m = A$$

pero $m \neq A$ ya que es maximal, entonces $(X_1 - a_1, ..., X_n - a_n) = m$. □

Teorema 5.2 (*Teorema de los ceros de Hilbert*)**.** Sea k un campo algebraicamente cerrado

a) Si $J \subsetneq k[X_1, X_2, ..., X_n]$ entonces $V(J) \neq \emptyset$.

b) $I(V(J)) = rad\, J$; en otras palabras para $f \in k[X_1, X_2, ..., X_n]$

$$f(P) = 0\ \forall P \in V \Leftrightarrow f^n \in J\, para\, algún\, n.$$

Demostración. a) Sea J un ideal no trivial, sabemos que todo ideal está contenido en un ideal maximal m pero por el corolario anterior

$$m = (X_1 - a_1, ..., X_n - a_n)$$

$$m = \{P_1(X_1 - a_1) + \cdots + P_n(X_n - a_n)\,/P_j \in k[X_1,\, X_2, ..., X_n]\}$$

como $J \subset m$ todo polinomio de J tiene la forma de los polinomios de m entonces $P = (a_1, ..., a_n) \in V(J)$. Así $V(J) \neq \emptyset$.

b) Primero veamos que $I(V(J)) \supset rad\, J$. Sea $f \in rad\, J$ entonces $\exists\, t \in \mathbb{N}$ tal que $f^t \in J$. Sea $P \in V(J)$ entonces $g(P) = 0\ \forall g \in J$.

Entonces

$$f^t(P) = f(P) \cdots f(P) = 0,$$

entonces $f(P) = 0$ y por tanto $f \in I(V(J))$.

Observemos que $I(V(J)) \subset rad\, J$. Sea $f \in I(V(J))$ tenemos que probar que $\exists r \in \mathbb{N}$ tal que $f^r \in J = (f_1, ..., f_s)$ con $f_1, ..., f_s \in k[X_1,\, X_2, ..., X_n]$, es decir, $f^r = \sum_{i=1}^{s} A_i f_i$ con $A_1, ..., A_s$ polinomios de $k[X_1,\, X_2, ..., X_n]$.

Como $f \in I(V(J))$ entonces $f(P) = 0$ para todo $P \in V(J) = V((f_1, ..., f_s))$ así P anula a $f_1, ..., f_s$ y a todas sus combinaciones.

Consideremos el ideal $\widetilde{I} = (f_1, .., f_s,\, 1 - Yf) \subset k[X_1,\, X_2, ..., X_n,\, Y]$.

Veamos que $V\left(\tilde{I}\right) = \emptyset$. Para ver esto, sea $P' = (a_1, ..., a_n,\, a_{n+1}) \in k^{n+1}$ con $P' \in V\left(\tilde{I}\right)$ entonces $g(P') = 0\ \forall g \in \tilde{I}$.

Entonces dado $g = f_1 + f_2 + ... + f_s + (1 - Yf) \in \tilde{I}$ pueden suceder dos cosas:

Primero que $(a_1, ..., a_n)$ sea un cero común de $f_1, ..., f_s$.

Segundo, que $(a_1, ..., a_n)$ no sea un cero común de $f_1, ..., f_s$, es decir que $(a_1, ..., a_n) \notin V(J)$.

Si $(a_1, ..., a_n)$ es un cero común de $f_1, ..., f_s$ se tiene que $(a_1, ..., a_n) \in V(J)$ entonces $g(P') = f_1(P') + f_2(P') + ... + f_s(P') + (1 - Yf)(P') = 1 - a_{n+1} f(P') = 1$ y esto es una contradicción ya que $g(P') = 0\ \forall g \in \tilde{I}$. Por lo tanto $V\left(\tilde{I}\right) = \emptyset$.

Ahora, sí $(a_1, ..., a_n)$ no es un cero común de $f_1, ..., f_s$, entonces existe $1 \leq i \leq s$ tal que $f_i((a_1, ..., a_n)) \neq 0$ entonces $f_i(P') \neq 0$ entonces $g(P') \neq 0$ y esto es una contradicción ya que $g(P') = 0\ \forall g \in \tilde{I}$. Por lo tanto $V\left(\tilde{I}\right) = \emptyset$.

Por el literal a) como $V\left(\tilde{I}\right) = \emptyset$ entonces $\tilde{I} = k\left[X_1, X_2, ..., X_n, Y\right]$ y así $(f_1, .., f_s, 1 - Yf) = k\left[X_1,\ X_2, ..., X_n,\ Y\right]$.

Como $1 \in k\left[X_1,\ X_2, ..., X_n,\ Y\right] = (f_1, .., f_s, 1 - Yf)$ entonces

$$1 = \sum_{i=1}^{s} P_i\left(X_1,\ X_2,\ ..., X_n,\ Y\right) f_i + q\left(X_1,\ X_2, ..., X_n,\ Y\right)(1 - Yf)$$

para algunos polinomios $P_i,\ q \in k\left[X_1,\ X_2, ..., X_n, Y\right]$.

Ahora usando el truco de Rabinowitsch, reemplazamos la variable Y por $\frac{1}{f(X_1,...,X_n)}$. Entonces implica que

$$1 = \sum_{i=1}^{s} P_i\left(X_1, X_2, ..., X_n, \frac{1}{f}\right) f_i.$$

Multiplicando a ambos lados de la ecuación anterior por una potencia f^r donde r es suficientemente grande para eliminar denominadores, esto nos lleva a

$$f^r = \sum_{i=1}^{s} A_i f_i$$

para algunos $A_i \in k\left[X_1, X_2, ..., X_n\right]$ □

Observación. Hay que notar que el teorema es falso si k no es algebraicamente cerrado: si $f \in k\left[X\right]$ es un polinomio de grado mayor o igual que dos que no tiene raíces en k entonces $(f) \neq k\left[X\right]$ ya que $x \in k\left[x\right]$ pero $x \notin (f)$ y además $V\left((f)\right) = \emptyset$ porque f no tiene raíces en k, pero entonces a) falla.

Además b) falla ya que $I\left(V\left((f)\right)\right) = k\left[x\right]$ pues

$$I\left(V\left((f)\right)\right) = \left\{f \in k\left[x\right] \mid f\left(P\right) = 0\, \forall P \in V\left((f)\right)\right\}$$

pero $V\left(f\right) = \emptyset$ entonces $I\left(V\left((f)\right)\right) = k\left[x\right]$. Si b) no fallara entonces tendríamos que $k\left[x\right] = rad\left((f)\right)$ y por propiedades del radical se tendría que $(f) = k\left[x\right]$ y esto es una contradicción pues $(f) \neq k\left[x\right]$.

Bibliografía

[1] Antoine Chambert-Loir. *A Field Guide to Algebra*. Université de Rennes 1 IRMAR france. Springer. 2005.

[2] J. F. Pommaret. *Differential Galois Theory*. École Polytechnique. 1945.

[3] Andreas Würfl. *Basic Concepts of Differencial Algebra*. 2007.

[4] Guerra Cáceres, Martín Enrique. *Aplicaciones de la teoría de Galois*. Universidad de El Salvador. 1991.

[5] Guillermo Dávila Rascón. *Apuntes de Historia de las Matemáticas*. 2003.

[6] Steven H. Weintraub. *Galois Theory*. Department of Mathematics Lehigh University Bethlem. Springer. 2006.

[7] John M. Howie. *Fields and Galois Theory*. University of St Andrews. Springer. 2006.

[8] Dr. Emil Artin. *Galois Theory*. Princeton University. 1942.

[9] Ian Stewart. *Galois theory*, 3rd ed. 1945.

[10] John B, Fraleigh. *Algebra abstracta primer curso*. Department of Mathematics University of Rhode Island. 1988.