

**TESIS PARA OPTAR EL TÍTULO PROFESIONAL DE
LICENCIADO EN MATEMÁTICA**

AUTORES:

- **Br. LUIS ARMANDO MÁRQUEZ GARCÍA**
- **Br. HÉCTOR BEDOYA DÍAZ**

ASESOR:

LIC. JUAN CORNETERO CAPITAN

LAMBAYEQUE, PERÚ

Enero 2 016

HOJA DE CONFORMIDAD DEL ASESOR

Quien suscribe Lic. Mat. Cornetero Capitán Juan Antonio, asesor de la tesis titulada:
**Estudio de polinomios de una variable con coeficientes en el campo de los números
complejos y análisis de sus raíces, Lambayeque, 2016.** Manifiesta la conformidad
del informe de tesis, suscribe en la fecha.....de del año dos mil
dieciséis.

Lic. Mat. Cornetero Capitán Juan Antonio

HOJA DE CONFORMIDAD DEL JURADO

Nosotros, los abajo firmantes, designados por la Universidad Nacional Pedro Ruiz Gallo como integrantes del Jurado Examinador de la Tesis titulada: “**Estudio de polinomios de una variable con coeficientes en el campo de los números complejos y análisis de sus raíces**”, Lambayeque, 2016. Presentado por **Br. Luis Armando Márquez García** y el **Br. Héctor Bedoya Díaz**, certificamos que esta tesis cumple con los requisitos exigidos por nuestra Magna Casa de Estudios para optar al título de **Licenciado en Matemática**.

M.Sc. Santos Henry Guevara Quiliche
Presidente del Jurado

Lic. Mat. Miguel Angel Baca Ferreyros

Secretario del Jurado

Lic. Mat. Miriam María Estrada Huancas

Vocal del Jurado

DEDICATORIA

A Dios por brindarme la oportunidad y la dicha de la vida.

A mi Madre y Abuela, quienes fueron las primeras personas en creer en mí, además por apoyarme en las decisiones de mi vida, mi amor y agradecimiento para ustedes Gloria y Laura es muy grande.

A mis hijos Liam y Margareth, que son mi motor y motivo para seguir superándome en mi vida y en mi formación como docente, para llegar a ser un docente universitario y ser un ejemplo y orgullo para ellos.

A mi esposa Vanesa, por su cariño y paciencia.

A mi hermana Elizeth, que es parte de mi superación.

LUIS ARMANDO MÁRQUEZ GARCÍA

A mis padres, por ser la base fundamental en todo lo que soy, en toda mi educación, tanto académica como de la vida, por su incondicional apoyo a través del tiempo. Todo este trabajo ha sido posible gracias a ellos.

HÉCTOR BEDOYA DÍAZ

AGRADECIMIENTO

A Dios por habernos dado la vida, el don y la salud para culminar el grado de Bachiller y estar aquí sustentando esta tesis.

A nuestro asesor de tesis Lic. Mat. Cornetero Capitán Juan Antonio, por su enseñanza, apoyo y amistad para el desarrollo y culminación de esta tesis.

A nuestros maestros, les agradecemos a todos ellos por sus enseñanzas impartidas en el aula, gracias porque ustedes han motivado nuestros sueños y esperanzas.

Los autores

RESUMEN

El presente trabajo de investigación titulado **Estudio de polinomios de una variable con coeficientes en el campo de los números complejos y análisis de sus raíces**. Tuvo como objetivo principal estudiar y analizar los ceros (raíces) de polinomios con coeficientes en el campo de los números complejos con aplicación en los campos de los números reales y racionales.

Para alcanzar nuestro objetivo mencionado arriba, nos encontramos con un famoso teorema llamado: **Teorema Fundamental del Algebra** (TFA) o también llamado teorema de Gauss, quien dio cinco demostraciones distintas de este teorema. En la actualidad existen decenas de demostraciones de este famoso teorema, además cabe mencionar que las demostraciones que se usan citan en alguna medida resultados elementales de análisis. Este teorema en este trabajo tiene una demostración algebraica con teoría de análisis complejo y lo aplicamos en la demostración de las fórmulas generales (conociendo sus coeficientes y uso de las operaciones elementales) para polinomios de grados uno, dos, tres y cuatro. Llegado un momento ocurre que es imposible obtener fórmulas generales para polinomios de grados mayores o iguales a cinco esto gracias al **teorema de Abel**, consecuentemente fue **Galois** quien caracterizo aquellos polinomios que son solubles por radicales.

Además en este trabajo podemos ubicar la vecindad donde se encuentran todos los ceros (raíces) de un polinomio con coeficientes complejos, reales o racionales; esto por medio de la **Cota de Cauchy**.

Finalmente una de las aplicaciones es que se puede determinar la cantidad de raíces reales de un polinomio de una variable con coeficiente en el campo de los números Reales o Racionales, esto por el teorema de **Sturm**.

ÍNDICE GENERAL

Introducción

1. Capítulo 1: PRELIMINARES

1.1 Grupos

1.1.1. Definición de Grupo

1.1.2. Grupo de las raíces n -ésimas de la unidad

1.1.3. Subgrupo

1.1.4. Subgrupo Cíclico

1.1.5. Subgrupo Simétrico

1.1.6. Ciclos de longitud " n " en una Permutación

1.1.7. Ciclos Ajenos

1.1.8. Transposiciones

1.1.9. Permutaciones Pares e Impares

1.1.10. Subgrupo Invariante

1.1.11. Grupo Simple

1.2 Series de Grupos

1.2.1. Serie Subinvariante

1.2.2. Serie Invariante

1.2.3. Refinamiento de una serie

1.2.4. Isomorfismo de dos series

1.2.5. Serie de Composición

1.2.6. Serie Principal

1.2.7. Teorema de Jordan – Hölder

1.2.7. Grupo Soluble

1.3 Anillos

1.3.1. Definición de Anillo

1.3.2. Definición de Campo

1.3.3. Característica de un Anillo

1.3.4. Ideales

1.3.5. Anillo de Polinomios

2. Capítulo 2: TEORÍA DE POLINOMIOS Y ESTUDIO DE SUS RAÍCES EN $K[x]$

2.1 Teoría de Polinomios

2.1.1. Definición de Polinomio

2.1.2. Teorema (Algoritmo de División)

2.1.4. Divisibilidad de Polinomios

2.1.4.1. Teoremas de Divisibilidad

2.1.5. Factorización de Polinomios

2.1.5.1. Polinomio Irreducible

2.1.6. Máximo Común Divisor

2.1.6.1. Algoritmo de Euclides

2.1.7. Polinomios Coprimos

2.1.7.1. Primalidad de Polinomios

2.1.8. Teorema Fundamental de la Aritmética

2.2 Raíces de Polinomios en $K[x]$

2.2.1. Definición de raíz de un polinomio

2.2.2. Análisis de raíces de polinomios

2.2.3. Raíces múltiples de un polinomio

2.2.4. Relación entre la multiplicidad de raíces de un polinomio y su derivada

2.2.5. Cantidad de raíces de un polinomio

3. Capítulo 3: RAÍCES DE POLINOMIOS EN $C[x]$ Y APLICACIONES DEL TFA

3.1 Teorema Fundamental del Álgebra

3.2 Cota de Cauchy

3.3 Fórmula General, Aplicaciones del TFA

3.3.1. Polinomios de Grado 1

3.3.2. Polinomios de Grado 2

3.3.3. Polinomios de Grado 3: Fontana - Cardano

3.3.4. Polinomios de Grado 4: Ferrari

3.3.4.1. Ecuación Cúbica Resolvente

3.4 Polinomio Soluble Por Radicales

3.4.1. Grupo $G(E/F)$

3.4.2. Extensión por Radicales

3.4.3. Polinomio soluble por Radicales

3.4.4. Condiciones para que un polinomio de grado mayor o igual a 5 sea soluble o insoluble por Radicales

3.4.4.1. Primera Condición

3.4.4.2. Segunda Condición

3.4.4.3. Tercera Condición

4. Capítulo 4: APLICACIONES DE RESULTADOS EN $\mathbb{Q}[x]$ Y $\mathbb{R}[x]$

4.1 Polinomios con coeficientes en \mathbb{Q}

4.1.1. Cálculo de raíces en \mathbb{Q}

4.1.2. Lema uno de Gauss y aplicación

4.1.3. Irreducibilidad en $\mathbb{Q}[x]$

4.1.4. Lema dos de Gauss

4.1.5. Criterio de Eisenstein

4.2 Polinomios con coeficientes en \mathbb{R}

4.2.1. Raíces de un polinomio de grado impar

4.2.2. Raíces complejas y conjugadas

4.2.3. Cantidad de raíces reales de un polinomio real

4.2.4. Regla de signos de Descartes

4.2.5. Sucesión de Sturm

4.2.6. Aplicación del teorema de Sturm

Conclusiones y Sugerencias

Bibliografía

INTRODUCCIÓN

Muchas veces al plantear en términos matemáticos problemas de distintas áreas como: Ingeniería, Física, Economía, Administración, Biología, etc. Nos encontramos en el caso que debemos encontrar los ceros (raíces) de polinomios, donde generalmente para las aplicaciones estos polinomios tienen coeficientes reales y más aún trata de encontrar ceros reales. Pero debido a la estructura de los números con los cuales trabajan las computadoras, estos polinomios suelen tener coeficientes racionales y los ceros que seremos capaces de calcular serán números racionales que aproximan suficientemente una verdadera solución al problema, esto justifica y fundamenta el desarrollo de esta tesis que además del cálculo de raíces, permite interpretar y analizar los polinomios en el campo que se trabaje. Las aplicaciones de los polinomios son cuantiosas, podemos modelar muchos fenómenos reales mediante polinomios. La referida tesis se ha estructurado de la siguiente manera:

En el Capítulo 1, abarca lo concerniente a la teoría de Grupos, donde destacamos el grupo de permutaciones el cual nos lleva a una aplicación posterior juntamente con la teoría de series de grupos, aquí además hablamos de Anillos, Campos y Anillo de polinomios.

El Capítulo 2, en este capítulo se desarrolla una sólida base teórica general de los polinomios como: El algoritmo de la división, teorema del resto, se demuestra el algoritmo de Euclides usando propiedades del máximo común divisor, se define polinomios primos como polinomios irreducibles en un campo \mathbb{K} , si el polinomio tiene una cierta raíz en un determinado campo \mathbb{K} , entonces el polinomio no necesariamente es reducible en dicho cuerpo, se define también el cero (raíz) de un

polinomio y finalmente se define las raíces múltiples de un polinomio y la relación con las derivadas del polinomio.

El Capítulo 3, se comienza con el teorema fundamental del algebra, se demuestra este teorema mediante teoría de campos y conocimiento de análisis complejo, este teorema en resumen nos dice que “ cualquier polinomio en el campo de los complejos de grado n , tiene n raíces complejas”, de esto se logra dar casos generales para polinomios de grados menores o iguales a cuatro. Para polinomios de grado 5 a más , no existe una fórmula general en radicales, para ello desarrollamos y la teoría de Galois y mencionamos el teorema de Abel, que dice que es imposible encontrar dicha fórmula general si el polinomio es de grado mayor o igual a cinco. Demostramos y aplicamos también la Cota de Cauchy.

En el Capítulo 4, se estudia el cálculo y análisis de las raíces de polinomios con coeficientes en los campos de los números \mathbb{R} (reales) y \mathbb{Q} (rationales) , se aplican procedimientos para calcular las raíces racionales, se establece criterios para la irreducibilidad de polinomios en \mathbb{Q} , se aplica el criterio de descartes para dar el número de raíces positivas o negativas. Finalmente se concluye con la aplicación del teorema de Sturm que permite determinar el número de raíces reales de un polinomio.

Finalmente, se presentan las conclusiones y las referencias bibliográficas con los autores y obras consultadas, que dan sustento teórico a este trabajo de investigación.

Capítulo 1: PRELIMINARES

1.1 Grupos

1.1.1. Definición de Grupo

Un grupo $(G, *)$. Es un conjunto G , junto con una operación binaria $*$: $G \times G \rightarrow G$, tal que verifica los siguientes axiomas:

1. Asociatividad: para todo $g_1, g_2, g_3 \in G$ tal que
$$(g_1 * g_2) * g_3 = g_1 * (g_2 * g_3)$$

2. Elemento neutro (identidad): existe $e \in G$ tal que
$$e * g = g * e = g \quad \forall g \in G$$

3. Elemento inverso: $\forall g \in G, \exists g' \in G$ tal que
$$g * g' = g' * g = e$$

Observaciones

1) el elemento neutro de un grupo es único, porque si e y \bar{e} son dos neutros, entonces $e = e * \bar{e} = \bar{e}$ la igualdad de la izquierda es porque \bar{e} es neutro "a derecha" y la segunda igualdad es porque e es neutro "a izquierda".

2) Un inverso g' de un elemento g es único, ya que si g' y g'' son dos inversos para un mismo g entonces
$$g' = g' * e = g' * (g * g'') = (g' * g) * g'' = e * g'' = g''$$

Al único inverso de un elemento g se lo denotará g^{-1} .

3) El grupo $(G, *)$ por simplicidad lo demostraremos solo por G .

4) Un grupo G es abeliano o conmutativa si:
 $g * h = h * g$, es decir su operación binaria es conmutativa.

1.1.2. Grupo de las raíces n-ésimas de la unidad

Sea $n \in \mathbb{N}$, $G_n = \{\text{raíces } n\text{-ésimas de la unidad}\}$, con la operación producto de números Complejos, entonces (G_n, \cdot) es un grupo.

En efecto:

Sea $G_n = \{W \in \mathbb{C} / W^n = 1\}$, debemos demostrar que (G_n, \cdot) es un grupo se sabe que, las raíces n-ésimas distintas la unidad son:

$$w_k = \cos\left(\frac{2k\pi}{n}\right) + i \operatorname{sen}\left(\frac{2k\pi}{n}\right)$$

donde: $k = 0, 1, 2, \dots, (n - 1)$

Luego: se tiene las raíces

$$w_0 = \cos 0 + i \operatorname{sen} 0 = 1$$

$$w_a = \cos\left(\frac{2a\pi}{n}\right) + i \operatorname{sen}\left(\frac{2a\pi}{n}\right)$$

$$w_b = \cos\left(\frac{2b\pi}{n}\right) + i \operatorname{sen}\left(\frac{2b\pi}{n}\right)$$

$$w_c = \cos\left(\frac{2c\pi}{n}\right) + i \operatorname{sen}\left(\frac{2c\pi}{n}\right)$$

Es claro que como $w_0 = 1$

$$\text{Luego: } w_a \cdot w_0 = w_a$$

$$w_b \cdot w_0 = w_b$$

$$w_c \cdot w_0 = w_c$$

Así que el elemento neutro es $w_0 = 1$

Ahora probemos la asociatividad:

$$(w_a \cdot w_b) \cdot w_c = w_a \cdot (w_b \cdot w_c)$$

$$(w_a \cdot w_b) \cdot w_c = \left[\cos\left(\frac{2a\pi}{n}\right) + i \operatorname{sen}\left(\frac{2a\pi}{n}\right) \right] \left[\cos\left(\frac{2b\pi}{n}\right) + i \operatorname{sen}\left(\frac{2b\pi}{n}\right) \right] \left[\cos\left(\frac{2c\pi}{n}\right) + i \operatorname{sen}\left(\frac{2c\pi}{n}\right) \right]$$

$$= [(\cos \alpha + i \operatorname{sen} \alpha)(\cos \beta + i \operatorname{sen} \beta)](\cos \theta + i \operatorname{sen} \theta)$$

$$= (\cos \alpha \cdot \cos \beta + i \cos \alpha \cdot \operatorname{sen} \beta + i \operatorname{sen} \alpha \cos \beta - \operatorname{sen} \alpha \operatorname{sen} \beta)(\cos \theta + i \operatorname{sen} \theta)$$

$$= [(\cos \alpha \cdot \cos \beta - \operatorname{sen} \alpha \operatorname{sen} \beta) + i (\cos \alpha \operatorname{sen} \beta + \operatorname{sen} \alpha \cos \beta)](\cos \theta + i \operatorname{sen} \theta)$$

$$= \frac{\cos(\alpha + \beta)}{A} + i \frac{\operatorname{sen}(\alpha + \beta)}{A} (\cos \theta + i \operatorname{sen} \theta)$$

$$= \cos A \cos \theta + i \cos A \operatorname{sen} \theta + i \operatorname{sen} A \cos \theta - \operatorname{sen} A \cos \theta$$

$$\begin{aligned}
&= (\cos A \cos \theta - \operatorname{sen} A \operatorname{sen} \theta) + i(\cos A \operatorname{sen} \theta + \operatorname{sen} A \cos \theta) \\
&= \cos(A + \theta) + i \operatorname{sen}(A + \theta) \\
&= \cos(\alpha + \beta + \theta) + i \operatorname{sen}(\alpha + \beta + \theta) \\
&= \cos(\alpha + (\beta + \theta)) + i \operatorname{sen}(\alpha + (\beta + \theta)) \\
&= (\cos \alpha + i \operatorname{sen} \beta) (\cos(\beta + \theta) + i \operatorname{sen}(\beta + \theta)) \\
&= w_a \cdot ((\cos \beta + i \operatorname{sen} \beta) \cdot (\cos \theta + i \operatorname{sen} \theta)) \\
&= w_a \cdot (w_b \cdot w_c)
\end{aligned}$$

Por lo tanto es asociativo.

Ahora determinemos su inverso para ello sea

$$w_a = \cos\left(\frac{2a\pi}{n}\right) + i \operatorname{sen}\left(\frac{2a\pi}{n}\right), \text{ debemos buscar } w_a' \text{ tal que}$$

$$w_a \cdot w_a' = 1$$

Sea:

$$w_a' = w_{(n-a)} = \cos\left(\frac{2(n-a)\pi}{n}\right) + i \operatorname{sen}\left(\frac{2(n-a)\pi}{n}\right)$$

Efectuando:

$$\begin{aligned}
w_a \cdot w_a' &= \left[\cos\left(\frac{2a\pi}{n}\right) + i \operatorname{sen}\left(\frac{2a\pi}{n}\right) \right] \left[\cos\left(\frac{2(n-a)\pi}{n}\right) + i \operatorname{sen}\left(\frac{2(n-a)\pi}{n}\right) \right] \\
&= \cos\left(\frac{2a\pi}{n}\right) \cos\left(\frac{2(n-a)\pi}{n}\right) + i \cos\left(\frac{2a\pi}{n}\right) \operatorname{sen}\left(\frac{2(n-a)\pi}{n}\right) + i \operatorname{sen}\left(\frac{2a\pi}{n}\right) \cos\left(\frac{2(n-a)\pi}{n}\right) - \\
&\quad \operatorname{sen}\left(\frac{2a\pi}{n}\right) \operatorname{sen}\left(\frac{2(n-a)\pi}{n}\right)
\end{aligned}$$

Agrupando:

$$\begin{aligned}
&= \cos\left(\frac{2a\pi}{n} + \frac{2(n-a)\pi}{n}\right) + i \operatorname{sen}\left(\frac{2a\pi}{n} + \frac{2(n-a)\pi}{n}\right) \\
&= \cos\left(\frac{2a\pi}{n} + \frac{2n\pi - 2a\pi}{n}\right) + i \operatorname{sen}\left(\frac{2a\pi}{n} + \frac{2n\pi - 2a\pi}{n}\right) \\
&= \cos\left(\frac{2n\pi}{n}\right) + i \operatorname{sen}\left(\frac{2n\pi}{n}\right) \\
&= \cos 2\pi + i \operatorname{sen} 2\pi \\
&= 1
\end{aligned}$$

$\therefore (G_n, \cdot)$ es un grupo además abeliano.

1.1.3. Subgrupo

Dado un grupo $(G, *)$ y $H \subseteq G$. Un subgrupo de G es $(H, */_{H \times H})$ es un grupo.

O en forma equivalente:

1. $*$ es cerrado en H , i.e $\forall h_1, h_2 \in H, h_1 * h_2 \in H$
2. $e \in H$
3. $\forall h \in H, h^{-1} \in H$

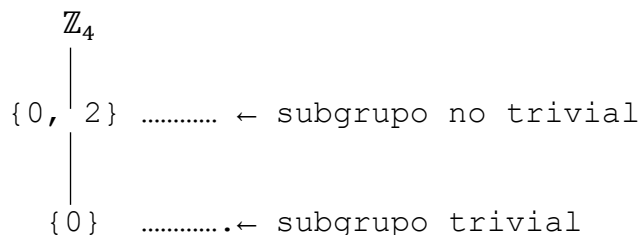
Si H es su subgrupo de G lo denotaremos por $H \leq G$

Ejemplo: Dado el grupo $(\mathbb{Z}_4, +)$, donde $\mathbb{Z}_4 = \{0, 1, 2, 3\}$

Se define la operación en la siguiente tabla

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Veamos mediante diagramas reticular los subgrupos de \mathbb{Z}_4



1.1.4. Subgrupo Cíclico

Sea G un grupo y sea $a \in G$. $H = \{a^n / n \in \mathbb{Z}\}$ es el subgrupo cíclico de G generado por a y se denotan por $\langle a \rangle$

Observación

- Un elemento a de un grupo G es un generador de G si $\langle a \rangle = G$. Un grupo G es cíclico si existe algún elemento a en G que genera G .

Ejemplo:

Sea el grupo \mathbb{Z}_4 . Entonces \mathbb{Z}_4 es cíclico y tanto 1 como 3 son generadores, esto es $\langle 1 \rangle = \langle 3 \rangle = \mathbb{Z}_4$

En efecto: $H = \{na / n \in \mathbb{Z}\}$

$$\begin{aligned} 0 + 3 &= 3 \\ 1 + 3 &= 0 \\ 2 + 3 &= 1 \\ 3 + 3 &= 2 \\ 4 + 3 &= 3 \\ 5 + 3 &= 0 \\ &\vdots \end{aligned}$$

Luego $\langle 3 \rangle = \mathbb{Z}_4$. De manera análoga para $\langle 1 \rangle = \mathbb{Z}_4$.

1.1.5. Subgrupo Simétrico

Si $A = \{1, 2, 3, \dots, n\}$ entonces el grupo de todas las permutaciones de A es el grupo simétrico y se denota por S_n . Además S_n tiene $n!$ elementos.

Ejemplo:

Si $A = \{1, 2, 3\}$ entonces el grupo de permutaciones de A es S_3 que tiene $3! = 6$ elementos.

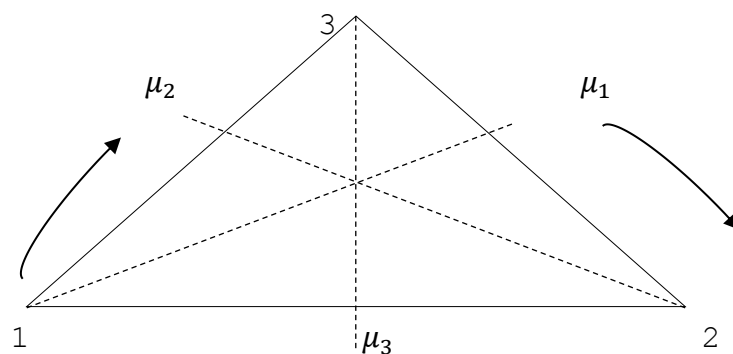
En efecto:

$$\begin{aligned} P_0 &= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} & \mu_1 &= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \\ P_1 &= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} & \mu_2 &= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \\ P_2 &= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} & \mu_3 &= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \end{aligned}$$

Donde

P_i : Rotaciones

μ_i : Imágenes reflejadas en bisectrices de los ángulos.



Tenemos la siguiente tabla:

.	P_0	P_1	P_2	μ_1	μ_2	μ_3
P_0	P_0	P_1	P_2	μ_1	μ_2	μ_3
P_1	P_1	P_2	P_0	μ_2	μ_3	μ_1
P_2	P_2	μ_3	P_1	μ_3	μ_1	μ_2
μ_1	μ_1	μ_3	μ_2	P_0	P_2	P_1
μ_2	μ_2	μ_1	μ_3	P_1	P_0	P_2
μ_3	μ_3	μ_2	μ_1	P_2	P_1	P_0

Veamos como hemos construido la tabla

$$P_0 P_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = P_2$$

Luego:

- $1 (P_0 P_2) = (1 P_0) P_2 = (1 P_2) = 3$
- $2 (P_0 P_2) = (2 P_0) P_2 = (2 P_2) = 1$
- $3 (P_0 P_2) = (3 P_0) P_2 = (3 P_2) = 2$

Además tomamos otros valores cualesquiera de la tabla

$$\mu_2 P_1 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \mu_1$$

- $1(\mu_2 P_1) = 1(\mu_2) P_1 = (3 P_1) = 1$
- $2(\mu_2 P_1) = 2(\mu_2) P_1 = (2 P_1) = 3$
- $3(\mu_2 P_1) = 3(\mu_2) P_1 = (1 P_1) = 2$

De manera análoga se llena toda la tabla dada en la parte de arriba.

$\therefore S_3$: es el grupo de simetrías de un triángulo equilátero.

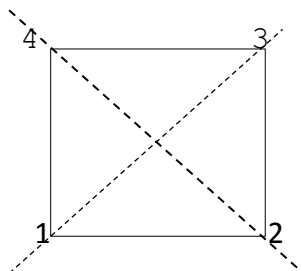
Ejemplo:

Sea D_4 : grupo de simetrías del cuadrado, conocido también como grupo octal donde las permutaciones

P_i : Rotaciones

μ_i : Imágenes reflejadas en bisectrices perpendiculares a los lados

δ_i : Reflejo en las diagonales



Genera 8 permutaciones:

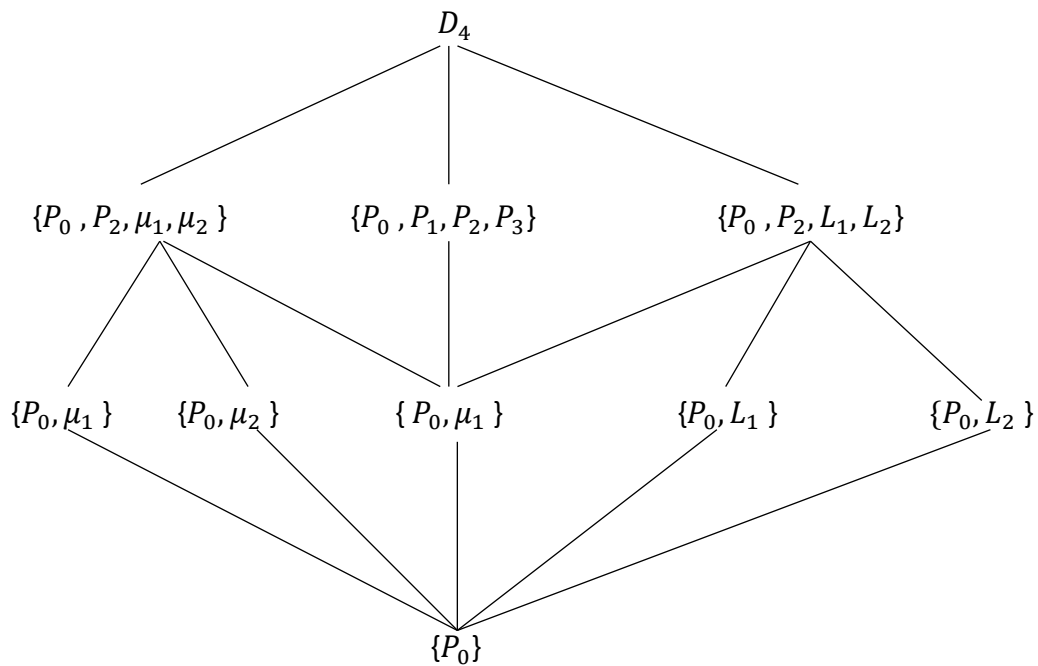
$$\begin{aligned}
 P_0 &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} & \mu_1 &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \\
 P_1 &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} & \mu_2 &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \\
 P_2 &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} & L_1 &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} \\
 P_3 &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} & L_2 &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}
 \end{aligned}$$

Genera la tabla siguiente:

.	P_0	P_1	P_2	P_3	μ_1	μ_2	δ_1	δ_2
P_0	P_0	P_1	P_1	P_3	μ_1	μ_2	δ_1	δ_2
P_1	P_1	P_2	P_3	P_0	δ_2	δ_1	μ_1	μ_2
P_2	P_2	P_3	P_0	P_1	μ_2	μ_1	δ_2	δ_1
P_3	P_3	P_0	P_1	P_2	δ_1	δ_2	μ_2	μ_1
μ_1	μ_1	δ_1	μ_2	δ_2	P_0	P_2	P_1	P_3
μ_2	μ_2	δ_2	μ_1	δ_1	P_2	P_0	P_3	P_1
δ_1	δ_1	μ_2	δ_2	μ_1	P_3	P_1	P_0	P_2
δ_2	δ_2	μ_1	δ_1	μ_2	P_1	P_3	P_2	P_0

Los valores en el interior de la tabla se consiguieron del mismo modo que se mostró en la tabla anterior.

Además tenemos los subgrupos de D_4



1.1.6. Ciclos de longitud "n" en una Permutación

Una permutación σ de un conjunto A es un ciclo de longitud n si existen $a_1, a_2, \dots, a_n \in A$ tales que: $a_1\sigma = a_2, a_2\sigma = a_3, \dots, a_{n-1}\sigma = a_n, a_n\sigma = a_1$ y $x\sigma = x$; $\forall x \in A$ tal que $x \notin \{a_1, a_2, \dots, a_n\}$. Escribimos $\sigma = (a_1, a_2, \dots, a_n)$ "notación cíclica"

Ejemplo:

Si $A = \{1, 2, 3, 4, 5\}$, entonces
 $(3, 5, 4, 1) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 1 & 4 \end{pmatrix}$, es un ciclo de longitud 4.

Por otro lado, el producto de dos ciclos no necesariamente es un ciclo.

Ejemplo:

Sean $(1, 4, 5, 6)$ y $(2, 1, 5)$ ciclos en S_6 de $A = \{1, 2, 3, 4, 5, 6\}$. Entonces

$$(1, 4, 5, 6)(2, 1, 5) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 3 & 2 & 6 & 5 \end{pmatrix}$$

$$(2, 1, 5)(1, 4, 5, 6) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 3 & 5 & 2 & 1 \end{pmatrix}$$

Ninguna de estas dos permutaciones es un ciclo.

1.1.7. Ciclos Ajenos

En una colección de ciclos, estos son ajenos cuando ningún elemento de A aparece en las notaciones de dos ciclos diferentes de la colección; esto es, si dos ciclos diferentes de la colección no mueven a ningún elemento de A. Además cada permutación σ de un conjunto finito A es un producto de ciclos ajenos.

Ejemplo:

Consideremos la permutación

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 2 & 4 & 3 & 1 \end{pmatrix} = (1, 6)(2, 5, 3)$$

1.1.8. Transposiciones

Un ciclo de longitud 2 es una transposición. Una transposición deja fijos todos los elementos excepto dos y lleva a cada uno de estos en el otro. Un cálculo muestra que $(a_1, a_2, a_3, \dots, a_n) = (a_1, a_2) (a_1, a_3) \dots (a_1, a_n)$.

Por tanto, cualquier ciclo es el producto de transposiciones. Luego cualquier permutación de un conjunto finito de al menos dos elementos es un producto de transposiciones.

Ejemplo: Dada la permutación

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 2 & 4 & 3 & 1 \end{pmatrix} = (1, 6) (2, 5) (2, 3)$$

1.1.9. Permutaciones Pares e Impares

Una permutación de un conjunto finito es par o impar de acuerdo con que puede expresarse como el producto de un número par de transposiciones o como el producto de un número impar de transposiciones, respectivamente.

De la definición anterior, se tiene que para $n \geq 2$, el número de permutaciones pares en S_n es igual al número de permutaciones impares; es decir, S_n se descompone equitativamente y ambos números son $\frac{n!}{2}$. De esto último sea A_n el conjunto de permutaciones pares en S_n y sea B_n el conjunto de permutaciones impares para $n \geq 2$, luego A_n y B_n tiene el mismo número de elementos que es $\frac{n!}{2}$.

Teorema: si $n \geq 2$, A_n es un subgrupo del grupo simétrico S_n con orden $\frac{n!}{2}$

Debemos demostrar:

1. A_n es cerrado bajo la operación binaria de S_n .
2. La identidad de S_n está en A_n .
3. $\forall \sigma \in A_n, \sigma^{-1} \in A_n$.

En efecto:

Sea τ cualquier transposición fija en S_n que existe porque $n \geq 2$. Podemos suponer que $\tau = (1, 2)$

Definimos la función

$$\lambda_{\mathcal{T}} : A_n \rightarrow B_n$$

$$\sigma \mapsto \sigma \lambda_{\mathcal{T}} = \mathcal{T} \sigma = (1, 2) \sigma$$

i. λ_{τ} es uno a uno

Sean $\sigma \in A_n$ y $\mu \in A_n$, luego si $\sigma \lambda_{\mathcal{T}} = \mu \lambda_{\mathcal{T}} \Rightarrow \sigma = \mu$

En efecto:

$$(1, 2) \sigma = (1, 2) \mu, \text{ como } S_n \text{ es grupo}$$

$$\sigma = \mu$$

Además $\tau = (1, 2) = \tau^{-1}$

ii. λ_{τ} es sobre si $\rho \in B_n$ entonces $\tau^{-1} \rho \in A_n$

En efecto:

$$(\mathcal{T}^{-1} \rho) \lambda_{\mathcal{T}} = \tau(\mathcal{T}^{-1} \rho) = \rho$$

De (i) y (ii) existe una correspondencia biunívoca.

De lo anterior existe

$$\tau^{-1} \rho_1 \in A_n \text{ y } \mathcal{T}^{-1} \rho_2 \in A_n$$

Luego

$$\underbrace{(\mathcal{T}^{-1} \rho_1)}_{\text{par}} \underbrace{(\mathcal{T}^{-1} \rho_2)}_{\text{par}}, \text{ es decir el producto de dos}$$

permutaciones pares es par.

Además: como $n \geq 2$, tiene dos elementos a y b :

$(a, b)(a, b) = 1$ es una permutación par.

Por último si

$$\sigma = (a_1, a_2) (a_1, a_3) \dots (a_1, a_n) \in A_n$$

Luego:

$$\sigma^{-1} = (a_2, a_1) (a_3, a_1) \dots (a_n, a_1) \in A_n$$

Es decir, si σ es una permutación par, σ^{-1} también debe ser par. Por tanto A_n es un grupo con orden $\frac{n!}{2}$

Al grupo A_n se le conoce como "grupo alternante".

1.1.10. Subgrupo Invariante

Un subgrupo H de un grupo G es un subgrupo normal (o invariante) si $g^{-1}Hg = H$, $\forall g \in G$. Se denota por $H \triangleleft G$.
Donde $H = g^{-1}Hg = \{g^{-1}Hg/h \in H\}$

Definición: Dado un grupo G y un subgrupo normal N , a la construcción G/N se le llama "grupo cociente de G por H " (o G módulo H)

Ejemplo: Sea $m\mathbb{Z}$ considerado como subgrupo de $(\mathbb{Z}, +)$,

$$\text{entonces } \mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}_m.$$

Por otro lado: $G/\{e\} \cong G$ y $G/G \cong \{e\}$

1.1.11. Grupo Simple

Un grupo es simple si no tiene subgrupos invariantes propios no triviales.

Teorema: El grupo alternante A_n es simple para $n \geq 5$

Demostración:

A_n Contiene a todo 3 - ciclo si $n \geq 3$

En efecto: $(a_1, a_2, a_3) = (a_1, a_2) (a_1, a_3) \in A_n$

Además: A_n está generado por los 3-ciclos para $n \geq 3$

En efecto: $(a, b, c) = (a, b) (a, c)$ además

$$(a, cd) (ac, d) = (a, b) (c, d)$$

Luego sean r y s fijos de $\{1, 2, 3, \dots, n\}$ para $n \geq 3$. Entonces

A_n está generado por los n - ciclos especiales de orden 3 de la forma (r, s, i) para $1 \leq i \leq n$. Es decir; todo 3 - ciclo es producto de 3 - ciclos especiales teniendo en cuenta:

$$(r, s, i)^2, (r, s, i)^2 (r, s, j), (r, s, i) (r, s, j)^2 \quad \text{y}$$

$$(r, s, i) (r, s, j)^2 \quad (r, s, k) (r, s, i)^2$$

Se tiene que estos productos dan todos los tipos posibles de 3 - ciclos.

Por otro lado si $N \triangleleft A_n$ para $n \geq 3$ y si además N contiene algún 3 - ciclo entonces $N = A_n$.

En efecto:

Como N es un subgrupo normal se tiene el siguiente producto, además contiene algún 3 - ciclos, es decir

$$(r, s, i) \in N \left((i, j) (r, s) \right)^{-1} (r, s, i)^2 \left((i, j) (r, s) \right), \text{ luego se tiene}$$

que: $(r, s, j) \in N$ para $1 \leq j \leq n$.

Por lo tanto, por lo anterior: A_n es simple para $n \geq 5$

1.3 Series de Grupos

1.2.1. Serie Subinvariante

Una serie subnormal (o subinvariante) de un grupo G es una sucesión finita H_0, H_1, \dots, H_n de subgrupos de G tal que

$H_i < H_{i+1}$ y H_i es un subgrupo normal de H_{i+1} , con $H_0 = \{e\}$ y $H_n = G$.

1.2.2. Serie Invariante

Una serie normal (o invariante) de G es una sucesión finita H_0, H_1, \dots, H_n de subgrupos normales de G tal que $H_i < H_{i+1}$, Con $H_0 = \{e\}$ y $H_n = G$

Ejemplo: Considérese el grupo D_4 luego

$\{P_0\} < \{P_0, \mu_1\} < \{P_0, P_2, \mu_1, \mu_2\} < D_4$ es una serie subnormal,

puesto que $\{P_0, \mu_1\}$ es no normal en D_4

Ejemplo: Dada siguiente serie

$\{0\} < 72\mathbb{Z} < 8\mathbb{Z} < \mathbb{Z}$ es una serie normal.

1.2.3. Refinamiento de una serie

Una serie subinvariante (invariante) $\{k_j\}$ es un

refinamiento de una serie subinvariante (invariante) $\{H_i\}$

de un grupo G si $\{H_i\} \subseteq \{k_j\}$, esto es, si cada H_i es una de las k_j .

Ejemplo: Dada la serie:

$$\begin{array}{cccc} \{0\} & < & 8\mathbb{Z} & < & 4\mathbb{Z} & < & \mathbb{Z} \\ \downarrow & & \downarrow & & \downarrow & & \downarrow \\ H_0 & < & H_1 & < & H_2 & < & H_3 \end{array}$$

Un refinamiento de la serie dada anteriormente es la serie dada a continuación.

$$\begin{array}{ccccccc} \{0\} & < & 72\mathbb{Z} & < & 24\mathbb{Z} & < & 8\mathbb{Z} & < & 4\mathbb{Z} & < & \mathbb{Z} \\ \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\ K_0 & < & K_1 & < & K_2 & < & K_3 & < & K_4 & < & K_5 \end{array}$$

En el ejemplo se observa claramente que cada H_i es una de las K_j .

1.2.4. Isomorfismo de dos series

Dos series subinvariante (invariante) $\{H_i\}$ y $\{K_j\}$ del mismo grupo G son isomorfas, si existe una correspondencia uno a uno entre las colecciones de grupos factores $\{H_{i+1}/H_i\}$ y $\{K_{j+1}/K_j\}$ tal que los grupos factores correspondiente son isomorfas, además deben tener el mismo número de grupos.

Ejemplo: Dadas las dos series de \mathbb{Z}_{15}

$$\begin{array}{ccccc} \{0\} & < & \langle 5 \rangle & < & \mathbb{Z}_{15} & & \{0\} & < & \langle 3 \rangle & < & \mathbb{Z}_{15} \\ \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\ H_0 & < & H_1 & < & H_2 & & K_0 & < & K_1 & < & K_2 \end{array}$$

Estas dos series son isomorfas

En efecto: Se tiene los grupos factores

$$\{H_2 / H_1, H_1 / H_0\} \qquad \{K_1 / K_2, K_1 / K_0\}$$

Luego:

$$\begin{aligned} \left\{ \mathbb{Z}_{15} / \langle 5 \rangle, \langle 5 \rangle / \{0\} \right\} &\rightarrow \left\{ \mathbb{Z}_{15} / \langle 5 \rangle, \langle 5 \rangle \right\} \\ \left\{ \mathbb{Z}_{15} / \langle 3 \rangle, \langle 3 \rangle / \{0\} \right\} &\rightarrow \left\{ \mathbb{Z}_{15} / \langle 3 \rangle, \langle 3 \rangle \right\} \end{aligned}$$

Luego:

$$\mathbb{Z}_{15} / \langle 5 \rangle \cong \mathbb{Z}_5 \quad \text{y} \quad \langle 3 \rangle \cong \mathbb{Z}_5$$

Además: $\mathbb{Z}_{15}/\langle 3 \rangle \cong \mathbb{Z}_3$ y $\langle 5 \rangle \cong \mathbb{Z}_3$

Observación: Dos series subinvariante (invariante) de un grupo G tienen refinamientos isomorfos.

En efecto:

Dadas las series normales

$$\{0\} < 72\mathbb{Z} < 8\mathbb{Z} < \mathbb{Z} \quad \text{y} \quad \{0\} < 18\mathbb{Z} < \mathbb{Z}$$

Cuyos refinamientos son respectivamente

$$\{0\} < 72\mathbb{Z} < 8\mathbb{Z} < 4\mathbb{Z} < \mathbb{Z} \quad \text{y} \quad \{0\} < 72\mathbb{Z} < 18\mathbb{Z} < 9\mathbb{Z} < \mathbb{Z}$$

Donde los grupos factores son

$$\left\{ \mathbb{Z}/4\mathbb{Z}, 4\mathbb{Z}/8\mathbb{Z}, 8\mathbb{Z}/72\mathbb{Z}, 72\mathbb{Z}/\{0\} \right\} \text{ y}$$

$$\left\{ \mathbb{Z}/9\mathbb{Z}, 9\mathbb{Z}/18\mathbb{Z}, 18\mathbb{Z}/72\mathbb{Z}, 72\mathbb{Z}/\{0\} \right\}$$

Estos grupos factores son isomorfos a: $\mathbb{Z}_4, \mathbb{Z}_2, \mathbb{Z}_9$ y $72\mathbb{Z}$

1.2.5. Serie de Composición

Una serie subinvariante $\{H_i\}$ de un grupo G es una serie de composición si todos los grupos factores H_{i+1}/H_i son simples.

1.2.6. Serie Principal

Una serie invariante $\{H_i\}$ de G es una serie principal si todos los grupos factores H_{i+1}/H_i son simples.

Ejemplo: Dadas las series

$$\{0\} < \langle 5 \rangle < \mathbb{Z}_{15} \quad \text{y} \quad \{0\} < \langle 3 \rangle < \mathbb{Z}_{15}$$

Son series de composición y además series principales de \mathbb{Z}_{15} puesto que los grupos factores

$$\mathbb{Z}_{15}/\langle 5 \rangle \cong \mathbb{Z}_5 \text{ además } \mathbb{Z}_5 \text{ es simple}$$

$\langle 5 \rangle / \{0\} \cong \langle 5 \rangle$ además $\langle 5 \rangle$ es simple de manera análoga la otra serie.

1.2.7. Teorema de Jordan - Hölder

Cualesquiera dos series de composición son isomorfas.

Demostración:

Sean $\{H_i\}$ y $\{K_j\}$ dos series de composición (principales) de G , estas series tienen refinamientos isomorfos por lo anterior, además por definición de series de composición (principales) sus grupos factores son simples entonces estas series no tienen más refinamientos, así $\{H_i\}$ y $\{K_i\}$ son isomorfas.

Teorema: si G tiene una serie de composición (principal) y si N es un subgrupo normal propio de G , entonces existe una serie de composición (principal) que contiene a N .

Demostración:

Sea la serie $\{e\} < N < G$ es una serie subnormal y normal, por hipótesis, G tiene una serie de composición $\{H_i\}$, entonces existe un refinamiento de $\{e\} < N < G$ a una serie subnormal isomorfa a un refinamiento de $\{H_i\}$, pero por ser $\{H_i\}$ serie de composición no puede tener mayor refinamiento, luego $\{e\} < N < G$ puede refinarse a una serie subnormal, cuyos Grupos factores son todos ellos simples, esto es, a una

serie de composición, de forma análoga si la serie es principal de G .

Es aquí a donde queríamos llegar en esta primera parte, pues la siguiente definición es fundamental para el capítulo III, ya que tratara de la solución de ecuaciones polinomiales en términos de radicales y además relacionaremos toda la teoría descrita en este capítulo con grupos solubles o no solubles involucrando polinomios.

1.2.7. Grupo Soluble

Un grupo G es soluble si tiene una serie de composición $\{H_i\}$ tal que todos los grupos factores H_{i+1}/H_i son Abelianos.

Ejemplo: El grupo S_3 es soluble
En efecto: Dada la serie de composición

$$\{e\} < A_3 < S_3$$

Cuyos grupos factores son:

$$\left\{ S_3/A_3, A_3/\{e\} \right\}$$

Estos grupos factores son isomorfos a \mathbb{Z}_2 y \mathbb{Z}_3 que son simples y además abelianos, entonces S_3 es soluble.

Ejemplo: el grupo S_5 no es soluble.
En efecto: Sea la serie

$$\{e\} < A_5 < S_5$$

Es una serie de composición puesto que $A_5/\{e\} \cong A_5$ es simple pero A_5 no es abeliano, entonces S_5 no es soluble.

En el capítulo III se determinara que este hecho está relacionado con el hecho de que una ecuación polinomial de grado 5 no es, en general, soluble por radicales, pero una ecuación polinomial de grado ≤ 4 si lo es.

1.3 Anillos

1.3.1. Definición de Anillo

Un anillo es un conjunto A junto con dos operaciones binarias $+, \cdot$; es decir es un terna $(A, +, \cdot)$ que cumple las siguientes axiomas.

1. $(a, +)$ es un grupo abeliano
2. $(a \cdot b) \cdot c = a \cdot (b \cdot c)$; $\forall a, b, c \in A$
3. $a(b + c) = ab + ac$; $\forall a, b, c \in A$
4. $(a + b)c = ac + bc$; $\forall a, b, c \in A$

Un anillo $(A, +, \cdot)$ por simplicidad lo denotaremos por A .

Son ejemplos de anillos: \mathbb{Z} , \mathbb{Q} , \mathbb{R} , \mathbb{C} , \mathbb{Z}_n , $n\mathbb{Z}$

Observación:

sea A un anillo con unitario. Un elemento u en A es una unidad de A si tiene un inverso multiplicativo en A . si todo elemento distinto de cero en A es una unidad, entonces A un anillo con división.

1.3.2. Definición de Campo

Un campo es un anillo conmutativo con división.

Son ejemplos de campos: \mathbb{Q} , \mathbb{R} , \mathbb{C} , \mathbb{Z} no es un campo pues por ejemplo 7 no tiene inverso multiplicativo, de modo que 7 no es una unidad en \mathbb{Z} .

Observación:

Un dominio entero D es un anillo conmutativo unitario no contiene divisores de cero.

Son ejemplos de dominio entero: \mathbb{Z} , \mathbb{Z}_p , donde p es un primo, en general todo campo es un dominio entero.

En nuestro trabajo esta observación es importante porque los coeficientes de nuestros polinomios pertenecen un dominio entero que son \mathbb{C} , \mathbb{R} y \mathbb{Q} , podemos resolver, un ecuación polinomial en la cual se puede factorizar el polinomio en factores lineales, haciendo, como es usual, cada factor igual a 0.

1.3.3. Característica de un Anillo

Si para un anillo A existe algún entero positivo n tal que $n \cdot a = 0, \forall a \in A$ (donde $n \cdot a = a + a + \dots + a$, n sumandos), entonces, el menor de dichos enteros positivos es la característica del anillo A . Si no existen dichos enteros positivos, entonces es de característica 0.

La característica de \mathbb{Z}_5 es 5. En efecto

$$\begin{aligned}5 \cdot 0 &= 0 + 0 + 0 + 0 + 0 = 0 \\5 \cdot 1 &= 1 + 1 + 1 + 1 + 1 = 5 = 0 \\5 \cdot 2 &= 2 + 2 + 2 + 2 + 2 = 10 = 0 \\5 \cdot 3 &= 3 + 3 + 3 + 3 + 3 = 15 = 0 \\5 \cdot 4 &= 4 + 4 + 4 + 4 + 4 = 20 = 0\end{aligned}$$

En general la característica de \mathbb{Z}_n es n .

Por otro lado todo $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ tiene característica 0.

1.3.4. Ideales

Un subgrupo $(N, +)$ de un anillo A que cumple

$$aN \subseteq N \text{ y } Na \subseteq N, \forall a \in A$$

es un ideal (o ideal bilateral) de A .

Observaciones:

1. Un ideal es a un anillo lo que un subgrupo invariante es a un grupo.
2. Los únicos ideales de un campo F es $\{0\}$ o F .

1.3.5. Anillo de Polinomios

Sea $A^{\mathbb{N}}$: conjuntos de todas las sucesiones de A que terminen en ceros, donde A es un anillo conmutativo unitario.

Así: $(a_0, a_1, \dots, a_n, 0, 0, \dots) \in A^{\mathbb{N}}$.

Se define:

$$(a_0, a_1, \dots, a_n, 0, \dots) + (b_0, b_1, \dots, b_n, 0, \dots) = (a_0 + b_0, a_1 + b_1, \dots, a_n + b_n, 0, \dots)$$

$$\begin{aligned}&(a_0, a_1, \dots, a_n, 0, \dots) \cdot (b_0, b_1, \dots, b_n, 0, \dots) \\&= (a_0 b_0, a_1 b_0 + a_0 b_1, a_2 b_0 + a_1 b_1 + a_0 b_2, \dots)\end{aligned}$$

$$= (c_0, c_1, \dots, c_r, 0, \dots)$$

donde $c_n = \sum a_i b_{n-i}$, a este producto se le llama "producto de convolución" en forma general se tiene

$$(u * v)_n = \sum_{i=0}^n \mu_i v_{n-i} = \sum_{i+j=n} \mu_i v_j$$

- Distributiva:

$$(\mu * (v + w))_n = \sum_{i+j=n} \mu_i (v + w)_j$$

$$= \sum_{i+j=n} (\mu_i v + \mu_i w_j)$$

$$i+j=n$$

$$= \sum_{i+j=n} \mu_i v_j + \sum_{i+j=n} \mu_i w_j$$

$$i+j=n \quad i+j=n$$

$$= (\mu * v)_n + (\mu * w)_n$$

- Unitaria:

La identidad es el elemento $(1, 0, 0, \dots)$.

Por lo tanto $(A^{\mathbb{N}}, +, *)$ es un anillo conmutativo unitario.

Se llama "anillo de los polinomios" en una indeterminada sobre A al "anillo conmutativo unitario" $A^{\mathbb{N}}$ que se llama simplemente "anillo de los polinomios sobre A".

Así que un elemento no es otra cosa que una sucesión finita: tal sucesión se llama "polinomio" cuando se trabaja con las leyes del anillo precedente, el producto de convolución se llama entonces producto de polonios. Para todo polinomio no nulo, el índice del último término no nulo es su grado, no se le atribuye grado al polinomio 0.

Ahora asociamos este resultado con la conocida mediante la aplicación.

$$\varphi : A^{\mathbb{N}} \rightarrow A[x]$$

$$(a_0, a_1, \dots, a_n, 0, \dots) \rightarrow a_0 + a_1 x + \dots + a_n x^n$$

Por lo descrito anteriormente se deduce que γ es un homomorfismo biyectivo. Por otro lado se puede decir si X es un elemento primitivo, todo elemento de $A[x]$ se escribe en la forma $a_0 + a_1x + \dots + a_nx^n$, con $a_i \in A$ y $n \in \mathbb{N}$.

De la aplicación e_n es la potencia n -ésima polinomio, tomando dos cosas particulares:

$$e_1 = (0, 1, 0, 0, \dots)$$

$$e_2 = (0, 0, 1, 0, 0)$$

Luego el polinomio $a = (a_n)_{n \in \mathbb{N}}$ se escribe en el anillo de polinomios de la forma $A = \sum_{n \geq 0} a_n e_n$,

$$n \geq 0$$

siendo finita la suma pues los a_i son nulos a partir de un cierto rango, además esta escritura es única.

Por último denotemos con x el elemento $e_1 = (0, 1, 0, 0, \dots)$ para $n \in \mathbb{N}$, el elemento e_n es entonces la potencia x^n (con $x^0 = 1$). A partir de aquí todo polinomio se escribe de modo único en la forma $\sum_{n \geq 0} a_n x^n$

y los productos de convolución se calculan de manera sencilla por distribuidad.

Por lo tanto es lógico denotar $A[x]$ el anillo de los polinomios en A , un lugar de $A^{\mathbb{N}}$.

Un anillo de polinomios nunca es un campo.

En efecto: para que $\sum a_n x^n$ sea invertible en $A[x]$, es necesario que a_0 sea invertible en A , además x no es invertible porque al multiplicar por x corresponde a trasladar de un rango los términos de la sucesión.

Capítulo 2: TEORÍA DE POLINOMIOS Y ESTUDIO DE SUS RAÍCES EN $K[x]$

2.1 Teoría de Polinomios

2.1.1. Definición de Polinomio

Si K denota un campo cualquiera, que puede ser \mathbb{C} , \mathbb{R} o \mathbb{Q} y $|K[x]$ denota el anillo de los polinomios con coeficientes $|K$ en cuyos elementos son polinomios. Un polinomio f es una expresión de la forma:

$$f = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0, \quad n \in \mathbb{N}, \quad a_n \neq 0$$

- Los elementos $a_n, a_{n-1}, \dots, a_1, a_0$ se llaman coeficientes del polinomio f tal que $a_i \in |K$, $0 \leq i \leq n$
- Se llama polinomio nulo, aquel cuyos coeficientes son todos ceros y se denota por $f = 0$.
- Si $f \neq 0$ el grado del polinomio de f es el máximo exponente de x y se denota por ∂f . Como $a_n \neq 0$ entonces $\partial f = n$. Al polinomio nulo no se le asigna un grado y un polinomio constante no nulo tiene grado cero, es decir $f = c$, $c \neq 0$ $c \in |K$ entonces $\partial f = 0$.
- Como $\partial f = n$ entonces " a_n " es el coeficiente principal de f y se denota con $C_p(f) = a_n$.
- Si $C_p(f) = 1$ entonces f es un polinomio Mónico.

2.1.2. Teorema (Algoritmo de División)

Para todo par de polinomios $f, g \in K[x]$, $g \neq 0$ y existen dos polinomios q y r (cociente y resto respectivamente) en $K[x]$ tales que:

$$f = qg + r, \quad \text{con } r = 0 \text{ ó } \partial r < \partial g$$

Además q y r son únicos

Demostración

Existencia

Sean los polinomios f y g con sus respectivos grados, así

$$f = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 ; a_n \neq 0 \rightarrow \partial f = n$$

$$g = b_m x^m + b_{m-1} x^{m-1} + \dots + b_1 x + b_0 ; b_m \neq 0 \rightarrow \partial g = m$$

- Si $\partial f < \partial g$, es decir $n < m$. para que cumpla el algoritmo de división, hasta tomar $q = 0$ y $r = f$.
- Ahora supongamos $\partial f \geq \partial g$, es decir $n \geq m$. utilizando inducción sobre ∂f y dejando fijo ∂g .
- Supongamos que el enunciado es cierto para todo f con $\partial f < n$. para ello sea $q_1 = \frac{a_n}{b_m} x^{n-m}$.

$$\text{Luego: } f_1 = f - q_1 g \rightarrow \partial f_1 = n-1$$

Y por hipótesis de inducción existen q_2 y $r_1 \in K[x]$ tales que:

$$f_1 = q_2 g + r_1 \text{ donde } r_1 = 0 \text{ ó } \partial r_1 < \partial g$$

$$f - q_1 g = q_2 g + r_1$$

$$f = q_1g + q_2g + r_1$$

$$f = (q_1 + q_2)g + r_1$$

$$\text{tomando } q = q_1 + q_2$$

$$r = r_1$$

$$\therefore f = qg + r \quad , \quad r = 0 \quad \text{ó} \quad \partial r < \partial g$$

Unicidad

$$f = qg + r$$

Supongamos que existen q' y $r' \in |K[x]|$ distintos de q y r respectivamente.

$$\text{Se tiene: } f = q'g + r'$$

$$\text{Luego: } r' - r = (q - q')g, \text{ como } \partial(r' - r) < \partial g$$

$$\rightarrow r' - r = 0 \quad \rightarrow \quad r' = r$$

$$\rightarrow q - q' = 0 \quad \rightarrow \quad q = q'$$

$$\therefore q \text{ y } r \text{ son únicos}$$

2.1.3. Teorema del Resto

Dado $f \in |K[x]|$ y $x \in |K|$, se tiene

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

Demostración

Por el teorema 2.1

$$f(x) = q(x)(x - \alpha) + r(\alpha) \quad , \quad r = 0 \quad \text{ó} \quad \partial r < \partial g$$

$$\text{Si } \partial r < \partial g \text{ (} g = x - \alpha \text{)} \rightarrow \partial r = 0 \rightarrow r(x) = r, \quad r \in |K|$$

Luego: $f(x) = q(x)(x-\alpha) + r$

Evaluyendo para $x = \alpha$

$$f(\alpha) = q(\alpha)(\alpha-\alpha) + r = 0 + r$$

$$f(\alpha) = r$$

$$\therefore f(\alpha) = q(x)(x-\alpha) + f(\alpha), \quad \text{si } \partial r < \partial g$$

$$\text{Si } r(x=0) \rightarrow f(k) = q(x)(x-\alpha)$$

$$\rightarrow f(\alpha) = 0$$

$$\rightarrow f(k) = q(x)(x-\alpha) + 0$$

$$\therefore f(k) = q(x)(x-\alpha) + f(\alpha), \text{ Si } r(x) = 0$$

2.1.4. Divisibilidad de Polinomios

Sean $f, g \in |K[x]$ se dice que $g|f$ (g divide a f) si y solo si existe un único $q \in |K[x]$ tal que $f = qg$. En caso contrario g no divide a f y se denota $g \nmid f$.

2.1.4.1. Teoremas de Divisibilidad

Teorema: Dados los polinomios f, g y $h \in |K[x]$. Si $g|f$ y $h|f$ entonces $h|f$.

Demostración

$$\text{Como } g|f \Leftrightarrow f = mg \quad ; \quad m \in |K[x]$$

$$h|g \Leftrightarrow g = nh \quad ; \quad n \in |K[x]$$

$$\text{Luego: } f = m[nh]$$

$$f = [m.n]h \quad ; \quad m.n \in |K[x] \quad \therefore h|f$$

Teorema: Dados los polinomios f, g y $h \in |K[x]$. Si $h \mid f$ y

$h \mid g$, entonces:

i) $h \mid f + g$

ii) $h \mid f - g$

Demostración

Por hipótesis

$$h \mid f \Leftrightarrow f = mh \quad ; \quad m \in |K[x]$$

$$h \mid g \Leftrightarrow g = nh \quad ; \quad n \in |K[x]$$

i) $f + g = mh + nh$

$$f + g = (m+n)h \quad , \quad (m+n) \in |K[x]$$

$$\therefore h \mid f + g$$

ii) $f - g = (m-n)h \quad ; \quad (m-n) \in |K[x]$

$$\therefore h \mid f - g$$

Teorema: Dados los polinomios f, g y $h \in |K[x]$. Si $g \mid f$ entonces $g \mid f.h$, $h \neq 0$ y $h \in |K[x]$

Demostración

$$g \mid f \Leftrightarrow f = mg \quad ; \quad m \in |K[x]$$

Como $h \neq 0$

$$f.h = mg.h$$

$$fh = mhg \quad mh \in |K[x]$$

$$\therefore g \mid fh$$

Consecuencias:

I. Si $g \mid f_1, g \mid f_2, \dots, g \mid f_k$ entonces
 $g \mid f_1g_1 + f_2g_2 + \dots + f_kg_k$, donde $g_1, g_2, \dots, g_k \in K[x]$

II. $g \mid f; \forall f \in K[x]$ y $g = \alpha, g \neq 0$

En efecto:

$$f = \left[\frac{a_n}{\alpha} x^n + \frac{a_{n-1}}{\alpha} x^{n-1} + \dots + \frac{a_0}{\alpha} \right]$$

III. Si $g \mid f$, entonces $\alpha g \mid f$;

Teorema: Dado $f \in K[x]$. Se cumple que $(x-a) \mid f, (x-b) \mid f$ y $(x-c) \mid f$, tal que $a \neq b \neq c$ si y solo si $(x-a)(x-b)(x-c) \mid f$.

Demostración

$$\Rightarrow f = (x-c)q_1, \quad q_1 \in K[x]$$

$$\text{como } (x-b) \mid f \rightarrow q_1 = (x-b)q_2, \quad q_2 \in K[x]$$

$$\text{y } (x-a) \mid f \rightarrow q_2 = (x-a)q_3, \quad q_3 \in K[x]$$

De donde:

$$f = (x-a)(x-b)(x-c)q_3 \quad ; \quad a \neq b \neq c$$

$$\therefore (x-a)(x-b)(x-c) \mid f$$

\Leftarrow La demostración es trivial el mismo razonamiento anterior

Teorema: Si

$$f = (x-a)q_1 + r$$

$$f = (x-b)q_2 + r$$

$$f = (x-c)q_3 + r, \text{ tal que } a \neq b \neq c, \text{ entonces}$$

$$f = (x-a)(x-b)(x-c)q_4 + r$$

Demostración

Se tiene $x-a \mid f-r$

$$x-b \mid f-r$$

$$x-c \mid f-r$$

Por el teorema anterior $(x-a)(x-b)(x-c) \mid f-r$

2.1.5. Factorización de Polinomios

No todos los polinomios se pueden factorizar si se puede factorizar la representación factorizada, es única, salvo el orden de los factores.

2.1.5.1. Polinomio Irreducible

Sea $f \in |K[x]|$ con $\partial f \geq 1$. Se dice que f es irreducible si y solo si no existe ningún $g \in |K[x]|$ con $1 \leq \partial g < \partial f$ además $g \mid f$, en forma equivalente, no existen polinomios $g, h \in |K[x]|$ no constantes con $\partial f > \partial g, \partial h$ tal que $f = gh$. De lo contrario, se dice que f es reducible.

Consecuencia: Cualquier polinomio $f \in |K[x]|$ con $\partial f = 1$ es irreducible en $|K[x]|$, pues no existe otro polinomio g tal que $1 \leq \partial g < \partial f = 1$

Observación: Todo polinomio que está sobre los racionales estará también sobre los reales y los complejos, pero que

esté en los reales o complejos, no implica necesariamente que esté en los racionales.

Ejemplo: Dado el polinomio

$$f = 4x^4 - 1$$

I. No es irreducible en \mathbb{Q} pues

$$f = (2x^2 + 1)(2x^2 - 1)$$

II. $g = 2x^2 + 1$ es irreducible en \mathbb{Q} y \mathbb{R}

pero no en \mathbb{C} pues

$$g = (\sqrt{2}x + i)(\sqrt{2}x - i)$$

III. $h = 2x^2 - 1$

es irreducible en \mathbb{Q} pero no en \mathbb{R} pues

$$h = (\sqrt{2}x + 1)(\sqrt{2}x - 1)$$

2.1.6. Máximo Común Divisor

Sean $f, g \in |K[x]|$ ambos no nulos. El máximo común divisor entre f y g denotado por $\text{mcd}(f, g)$ es el único polinomio Mónico $d \in |K[x]|$ que cumple simultáneamente las dos condiciones siguientes:

1. $d | f$ y $d | g$

2. Si $\tilde{d} \in |K[x]|$ y $\tilde{d} | f$ y $\tilde{d} | g$ entonces $\tilde{d} | d$

Ejemplo: Sean $f, g \in |K[x]|$, $g \neq 0$. Entonces

i) Sea $c \in |K[x]| \setminus \{0\}$, $\text{mcd}(c, g) = 1$

ii) Si $g | f$, $\text{mcd}(f, g) = g / \text{cp}(g)$

Teorema: Sean $f, g \in K[x]$, $g \neq 0$ y sean

$q, r \in K[x]$ con $f = qg + r$, entonces

$$\text{mcd}(f, g) = \text{mcd}(g, r)$$

Demostración:

Sea $d = \text{mcd}(f, g)$

$$d_0 = \text{mcd}(g, r)$$

Luego:

$$d|f \text{ y } d|g \rightarrow d|(f - qg)$$

$$\Rightarrow d|r$$

$$\Rightarrow d|d_0, \text{ por definición de } d_0$$

Por otro lado:

$$d_0|g \text{ y } d_0|r \rightarrow d_0|(qg + r)$$

$$\rightarrow d_0|f, \text{ ademas } d_0|g$$

$$\rightarrow d_0|d$$

$$\text{Así } d_0|d \text{ y } d|d_0 \therefore d = d_0$$

2.1.6.1. Algoritmo de Euclides

Sean $f, g \in K[x]$ polinomios no nulos con $\partial f \geq \partial g$.

Entonces $\text{mcd}(f, g)$ es el último resto r_k no nulo (dividido por su coeficiente principal para volverlo Mónico) que aparece en la sucesión de divisiones siguientes:

$$f = q_1g + r_1 \quad , \quad \partial r_1 < \partial g$$

$$g = q_2r_1 + r_2 \quad , \quad \partial r_2 < \partial r_1$$

$$r_1 = q_3r_2 + r_3 \quad , \quad \partial r_1 < \partial r_2$$

\vdots

$$r_{k-2} = q_k r_{k-1} + r_k \quad , \quad \partial r_k < \partial r_{k-1}$$

$$r_{k-1} = q_{k+1} \cdot r_k$$

Del teorema anterior se tiene

$$\text{mcd}(f, g) = \text{mcd}(g, r_1) = \text{mcd}(r_1, r_2) = \dots = \text{mcd}(r_{k-2}, r_{k-1}) =$$

$$\text{mcd}(r_{k-1}, r_k) = \frac{r_k}{\text{cp}r_k} \text{ esto último por el ejemplo anterior ya}$$

que $r_r \mid r_{k-1}$

Corolario: Dados los polinomios sobre $|K$ f y g existen

$$s, t \in |K[x]| \text{ tales que: } \text{mcd}(f, g) = sf + tg$$

Demostración

Despejando r_k de la antepenúltima igualdad del algoritmo de Euclides y así sucesivamente despejando $r_{k-1}, r_{k-2}, \dots, r_2, r_1$ en las siguientes anteriores se logra escribir

$$r_k = s'f + t'g$$

$$\frac{r_k}{\text{cp}(r_k)} = \frac{s'}{\text{cp}(r_k)}f + \frac{t'}{\text{cp}(r_k)}g$$

$$\therefore \text{mcd}(f, g) = sf + tg \quad , \quad s, t \in |K[x]|$$

Ejemplo: Sean los polinomios

$$f = x^5 + x^4 + 1 \quad \text{y} \quad g = 2x^2 - x^3 - 2x^2 + 3x - 1$$

Determinar $\text{mcd}(f, g)$

En efecto: Aplicando el algoritmo de Euclides tenemos

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

$$g = \left(\frac{8}{7}x - \frac{4}{7}\right) r_1$$

$$\text{De aqu\u00ed: } \text{mcd}(f, g) = \text{mcd}(g, r_1) = \frac{r_1}{\text{cp}(r_1)} = \frac{\frac{7}{4}x^3 - \frac{7}{4}x + \frac{7}{4}}{\frac{7}{4}}$$

$$\therefore \text{mcd}(f, g) = x^3 - x + 1$$

Adem\u00e1s:

$$r_1 = f - qg$$

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

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

$$\therefore \text{mcd}(f, g) = sf + tg$$

Ejemplo: Sean los polinomios

$$f = x^5 + x^4 - 3x^3 + 4x^2 + 2x \quad \text{y}$$

$$g = x^4 + 3x^3 - x^2 - 6x - 2$$

Vamos a determinar su $\text{mcd}(f, g)$

En efecto: Aplicando el algoritmo de Euclides tenemos

$$f = \underbrace{(x-2)}_{q_1} g + \underbrace{4x^3 + 8x^2 - 8x - 4}_{r_1}, \quad \partial r_1 < \partial_g$$

$$g = \underbrace{\left(\frac{1}{4}x + \frac{1}{4}\right)}_{q_2} r_1 + \underbrace{-x^2 - 3x - 1}_{r_2} \quad , \quad \partial r_2 < \partial r_1$$

$$r_1 = \underbrace{(-4x + 4)}_{q_3} r_2$$

$$\text{Luego} \quad \text{mcd}(f, g) = \frac{r_2}{\text{cp}(r_2)} = \frac{-x^2 - 3x - 1}{-1}$$

$$\text{mcd}(f, g) = x^2 + 3x + 1$$

Además:

$$r_2 = g - \left(\frac{1}{4}x + \frac{1}{4}\right) r_1$$

$$r_2 = g - \left(\frac{1}{4}x + \frac{1}{4}\right) [f - (x - 2)g]$$

$$r_2 = g - \left(\frac{1}{4}x + \frac{1}{4}\right)f + \left(\frac{1}{4}x + \frac{1}{4}\right)(x - 2)g$$

$$r_2 = -\left(\frac{1}{4}x + \frac{1}{4}\right)f + \left[1 + \left(\frac{1}{4}x + \frac{1}{4}\right)(x - 2)\right]g$$

$$r_2 = -\left(\frac{1}{4}x + \frac{1}{4}\right)f + \left(\frac{1}{4}x^2 - \frac{1}{4}x + \frac{1}{2}\right)g$$

$$\text{mcd}(f, g) = \frac{r_2}{\text{cp}(r_2)} = \left(\frac{1}{4}x + \frac{1}{4}\right)f + \left(-\frac{1}{4}x^2 + \frac{1}{4}x - \frac{1}{2}\right)g \quad , \quad \text{cp}(r_2) = -1$$

$$\text{mcd}(f, g) = sf + tg$$

2.1.7. Polinomios Coprimos

Dos polinomios f y $g \in \mathbb{K}[x]$ son primos entre sí (coprimos) si cumplen que $\text{mcd}(f, g) = 1$, es decir si ningún polinomios de grado ≥ 1 divide

simultáneamente a f y a g . o equivalentemente si existen polinomios $s, t, \in |K[x]$ tales que

$$1 = sf + tg$$

Proposición: Sean $f, g, h \in |K[x]$, entonces:

$$1. f|h \text{ y } g|h \text{ y } f, g \text{ son coprimos} \rightarrow fg|h$$

$$2. f|gh \text{ y } f, g \text{ son coprimos} \rightarrow f|h$$

Demostración

Como f y g son coprimos $\rightarrow \text{mcd}(f, g) = 1$

$$\rightarrow \exists s, t \in |K[x]| \text{ tal que}$$

$$1 = sf + tg$$

Luego

$$h = sfh + tgh$$

$$\rightarrow \frac{h}{fg} = \frac{sh}{g} + \frac{th}{f}$$

$$\rightarrow \frac{h}{fg} = sq_1 + tq_2 \quad , \quad q_1, q_2 \in |K[x]|$$

$$\therefore fg|h$$

Además: $\frac{h}{f} = \frac{sh}{f} + \frac{tgh}{f}$ por el mismo razonamiento $f|h$

Proposición: Sean $f, g \in |K[x]$, entonces

$$\frac{f}{\text{mcd}(f, g)} \text{ y } \frac{g}{\text{mcd}(f, g)} \text{ son coprimos}$$

Demostración

Sea $\text{mcd}(f, g) = d$, $d|f \rightarrow \exists U \in |K[x]|$ tal que $f = ud$

Además $d|g \rightarrow \exists V \in |K[x]|$ tal que $g = vd$

Por corolario anterior se tiene

$$d = sf + tg$$

$$\rightarrow d = sud + tvd$$

$$\rightarrow 1 = su + tv$$

De aquí $\text{mcd}(u, v) = 1$

$$\text{mcd}\left(\frac{f}{d}, \frac{g}{d}\right) = 1$$

$$\therefore \frac{f}{\text{mcd}(f, g)} \text{ y } \frac{g}{\text{mcd}(f, g)} \text{ son coprimos}$$

2.1.7.1. Primalidad de Polinomios

Sean f, g y $h \in |K[x]|$, con f irreducible, entonces

$$1. \text{mcd}(f, g) = \frac{f}{\text{cp}(f)} \quad \text{si } f|g \text{ y}$$

$$\text{mcd}(f, g) = 1 \text{ si } f \nmid g$$

$$2. f|g \rightarrow f|g \text{ ó } f|h$$

Demostración:

1. i) Si $f|g$, $\exists u \in |K[x]|$: $g = uf$, además

por el corolario 2.1, $\exists s, t \in |K[x]|$ tal que

$$\text{mcd}(f, g) = sf + tg$$

$$\begin{aligned} \rightarrow \text{mcd}(f, g) &= sf + tuf \\ &= f(s1 + tu) \\ &= f \text{mcd}(1, u) \\ &= f.1 \end{aligned}$$

$$\text{mcd}(f, g) = f$$

$$\text{luego } \text{mcd}(f, g) = \frac{f}{\text{cp}(f)}$$

ii) Si $f \nmid g$ luego f y g son coprimos

$$\rightarrow \text{mcd}(f, g) = 1$$

2. Si $g = 0$ ó el resultado es obvio

Si $g \neq 0$ y $h \neq 0$, supongamos que $f \nmid g$ debemos demostrar que $f \mid h$. La suposición implica que $\text{mcd}(f, g) = 1$

Por la proposición anterior se tiene que $f \mid h$. Por el mismo razonamiento $f \mid g$.

2.1.8. Teorema Fundamental de la Aritmética

Sea $f \in |K[x]$ un polinomio no constante.

Entonces existe únicos polinomios irreducibles mónicos distintos g_1, g_2, \dots, g_m en $|K[x]$ de manera que:

$$f = c g_1^{k_1} g_2^{k_2} \dots g_m^{k_m}, \quad c \in |K \setminus \{0\}$$

Con $k_1, k_2, \dots, k_m \in \mathbb{N}$, además $C_p(f) = c$

Demostración

Si f es primo en $|K[x]$ se tiene que

$$f = c f_1; \quad c \in |K \setminus \{0\}$$

y $f_1 \in |K[x]$ es Mónico irreducible

Si f no es primo en $|K[x]$ (reducible), entonces

$f = c g_1 g_2 \dots g_n$, pero entre estos factores

g_i para $1 \leq i \leq n$, pueden existir factores que se repiten, luego

$$f = Cg_1^{k_1} g_2^{k_2} \dots g_m^{k_m}, \quad m \leq n, \quad C \in |K \setminus \{0\}| \text{ y } k_i \in |N|, 1 \leq i \leq m$$

La unicidad de los factores se da, salvo el orden de los factores, C resulta ser el coeficiente principal de f .

Observación: Sean $f, g \in |K[x]|$, entonces $\text{mcd}(f, g)$ es el producto de los factores irreducibles nómicos que aparecen en común en las factorizaciones de f y g , a la mínima potencia con la que aparecen.

Ejemplo: Sean los polinomios

$$f = 3x^3(x-1)^2$$

$$g = 2x^2(x-1)^3$$

$$\rightarrow \text{mcd}(f, g) = x^2(x-1)^2$$

Ejemplo: Sean los polinomios

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

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

$$\text{mcd}(f, g) = x^2(x-1)^2$$

La observación precedente puede parecer a primera vista un algoritmo para calcular el mcd entre los polinomios, incluso más simple que el de Euclides, pero en realidad no es así ya que no se conocen algoritmos para factorizar polinomios, por lo menos en los casos $|K| = \mathbb{R}$ o $|K| = \mathbb{C}$.

2.2 Raíces de Polinomios en $K[x]$

2.2.1. Definición de raíz de un polinomio

Se dice que $\alpha \in |K$ es una raíz de f o es un cero de f si $f(\alpha) = 0$

Proposición: $\alpha \in |K$ es raíz de $f \Leftrightarrow (x - \alpha) | f \Leftrightarrow f = (x - \alpha)q$, para algún $q \in |K[x]$

La demostración es trivial por el teorema del resto

2.2.2. Análisis de raíces de polinomios

- f constante: $f = c$ con $C \in |K$

Entonces, o bien $c = 0$ y todo $\alpha \in |K$ es una raíz de f . ó bien $C \neq 0$ y f no tiene ninguna raíz en $|K$.

- f de grado 1: $f = ax + b$ con $a, b \in |K$, $a \neq 0$

Entonces $\frac{-b}{a}$ es raíz de f y $f = a(x - (\frac{-b}{a}))$

- f de grado 2: $f = ax^2 + bx + c$ con $a, b, C \in |K$, $a \neq C$

Supondremos aquí que $2 \neq 0$ en $|K$

(o sea la característica de $|K$ es distinta de 2)

Luego

$$f = a\left(x^2 + \frac{b}{a}x + \frac{c}{a}\right)$$

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

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

Se define el discriminante de f como $\Delta(f) = \Delta = b^2 - 4ac$

Entonces, si existe $\beta \in |K$ tal que $\beta^2 = \Delta$, se tiene que:

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

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

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

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

Consecuencias:

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

- Cuando $|K = \mathbb{R}$, existe $\beta = \sqrt{\Delta}$ si y solo si $\Delta \geq 0$.
Luego $\Delta \geq 0$ entonces el polinomio tiene dos raíces reales (distintos o repetidos cuando $\beta = 0$)

Por otra parte existen polinomios en $\mathbb{R}[x]$ de grado 2 que no tienen raíces reales como $f = 2x^2 + 4$.

- Cuando $|K = \mathbb{Q}$, si Δ tiene una raíz cuadrada en \mathbb{Q} , entonces el polinomio tiene dos raíces racionales pero también existen polinomios de grado 2 en \mathbb{Q} con raíces irracionales, como $f = x^2 - 8$, cuyas raíces son $\alpha_1 = 2\sqrt{2}$ y $\alpha_2 = -2\sqrt{2}$.

- Lo que prueba este ejemplo de polinomios de grado 3 en un cuerpo $|K$ de carácter distinta de 2 es una condición suficiente:

Si existe $\beta \in |K$ tal que $\beta^2 = b^2 - 4ac$, entonces $f = a\alpha^2 + bx + c$, $a \neq 0$ tiene dos raíces en $|K$.

Falta investigar aun la reciproca

Observación: si $f \in |K[x]$ tiene una raíz $\alpha \in |K$, entonces el polinomio $(x - \alpha)$ es uno de los factores irreducibles de f , pues $f = (x - \alpha)q$ esto es por unicidad de la factorización, luego para factorizar f alcanza con factorizar q .

Estamos ahora en condiciones de retomar el ejemplo de los polinomios de grado 2, podemos mostrar ahora que si $f = ax^2 + bx + c$.

Tiene una raíz en k (con característica distinta de 2) entonces $b^2 - 4ac$ es un cuadrado en $|K$. Con esto, concluiremos la demostración de la afirmación:

“Existe $\beta \in |K$ tal que $\beta^2 = b^2 - 4ac$ si y solo si el polinomio $f = ax^2 + bx + c$ tiene dos raíces $|K$ ”

En efecto, si $f = ax^2 + bx + c$ tiene una raíz $\alpha_1 \in |K$, entonces, por la observación anterior, $(x - \alpha_1)$ aparece en la factorización de f , y por razones de grado, el otro factor irreducible Mónico tiene grado uno, y se puede escribir $(x - \alpha_2)$. Por consiguiente, f tiene sus dos raíces $\alpha_1 - \alpha_2$ en $|K$ y se escribe de la forma:

$$f = a(x - \alpha_1)(x - \alpha_2)$$

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

Igualando coeficiente a coeficiente, resulta que

$$b = -a(\alpha_1 + \alpha_2) \text{ y } c = a \alpha_1 \alpha_2.$$

Por lo tanto

$$\begin{aligned} b^2 - 4ac &= [-a(\alpha_1 + \alpha_2)]^2 - 4a \alpha_1 \alpha_2 \\ &= a^2(\alpha_1 + \alpha_2)^2 - 4a^2 \alpha_1 \alpha_2 \\ &= a^2(\alpha_1 + \alpha_2)^2 + 2 \alpha_1 \alpha_2 - 4 \alpha_1 \alpha_2 \\ &= a^2(\alpha_1 - \alpha_2)^2 \end{aligned}$$

$$b^2 - 4ac = [a(\alpha_1 - \alpha_2)]^2$$

Resulta ser un cuadrado en $|K$

2.2.3. Raíces múltiples de un polinomio

Sea $f \in |K[x]$ y $\alpha \in |K$ raíz de f , Se dice que:

- α es raíz simple de f si y solo si $f(\alpha) = 0$
pero $(x - \alpha)^2 \nmid f$ o sea
 $f = (x - \alpha)q$, con $q(\alpha) \neq 0$
- α es raíz doble de f si y solo si
 $(x - \alpha)^2 \mid f$, o sea $f = (x - \alpha)^2 q$, con $q(\alpha) \neq 0$
- α es raíz de multiplicidad k de f si y solo si
 $(x - \alpha)^k \mid f$ pero $(x - \alpha)^{k+1} \nmid f$, o sea $f = (x - \alpha)^k q$ con
 $q(\alpha) \neq 0$.

Ejemplo: Sea $f = 2x^2(x+1)(x^2-1)^3$

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

Luego

$$\alpha_1 = 0 \quad \text{raíz doble}$$

$$\alpha_2 = -1 \quad \text{raíz de multiplicidad 4}$$

$$\alpha_3 = 1 \quad \text{raíz de multiplicidad 3}$$

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

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

Sea $|K|$ un campo de característica 0 es decir \mathbb{Q} , \mathbb{R} ó \mathbb{C} , que son los cuerpos que nos interesan.

2.2.4. Relación entre la multiplicidad de raíces de un polinomio y su derivada

Sea $|K|$ un cuerpo de característica 0 es decir \mathbb{Q}, \mathbb{R} ó \mathbb{C}

1. α es raíz doble de $f \Leftrightarrow \alpha$ es simultáneamente raíz de

f y de f' . Equivalente: α es raíz simple de $f \Leftrightarrow$

$$f(\alpha) = 0 \text{ y } f'(\alpha) \neq 0$$

2. α es raíz de multiplicidad k de f ($k \geq 2$)

$\Leftrightarrow \alpha$ es raíz de f y además es raíz de multiplicidad $(k-1)$ de f'

3. α es raíz de multiplicidad exactamente k de f ($k \geq 1$)

$$\Leftrightarrow f(\alpha) = f'(\alpha) = \dots = f^{(k-1)}(\alpha) = 0 \text{ y } f^{(k)}(\alpha) \neq 0.$$

Demostración

$$1. \Rightarrow \left. \begin{array}{l} f = (x-\alpha)^2 q \end{array} \right\}$$

$$\text{Luego } f' = 2(x-\alpha)q + (x-\alpha)^2 q'$$

$$f' = (x-\alpha)[2q + (x-\alpha)q']$$

Se verifica que

$$f(\alpha) = f'(\alpha) = 0$$

\leftarrow Como α es raíz de f , se puede escribir $f = (x-\alpha)q$,
debemos mostrar que $q(\alpha) = 0$, o sea que $(x-\alpha)^2 \mid f$,

$$\text{Como } f = (x-\alpha)q' + q, \text{ como } f'(\alpha) = 0$$

$$\Rightarrow q(\alpha) = 0$$

$$2. \Rightarrow \left. \begin{array}{l} f = (x-\alpha)^k q \text{ con } q(\alpha) \neq 0, \text{ luego} \end{array} \right\}$$

$$f' = k(x-\alpha)^{k-1}q + (x-\alpha)^k q'$$

$$f' = (x-\alpha)^{k-1} (kq + (x-\alpha)q'),$$

Tomando $h = kq + (x-\alpha)q'$ se verifica que

$$f' = (x-\alpha)^{k-1}h \text{ con } h(\alpha) \neq 0$$

(pues $q(\alpha) \neq 0$ y en un cuerpo de característica 0, $k \neq 0$)

\leftarrow Como α es raíz de f , tiene cierta multiplicidad

$r \geq 1$ como raíz. Se pretende probar que $r = k$

$$\text{Sea } f = (x-\alpha)^r q \text{ con } q(\alpha) \neq 0$$

$$\text{Luego } f' = (x-\alpha)^{r-1} (rq + (x-\alpha)q') \text{ Si}$$

Tomamos $h = rq + (x-\alpha)q'$ resulta que

$$f' = (x-\alpha)^{r-1}h \text{ con } h(\alpha) \neq 0, \text{ por consiguiente}$$

α es raíz de multiplicidad exactamente $r-1$ de f'

pero por hipótesis, esa multiplicidad es $k-1$ por lo tanto:

$$r - 1 = k - 1, \text{ es decir } r = k$$

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

- Si $k = 1$: es una consecuencia inmediata de (1) α es raíz simple de $f \Leftrightarrow \alpha$ es raíz de f y no es raíz de f'
- Si $k > 1$: Por (2), α es raíz de multiplicidad k de $f \Leftrightarrow f(\alpha) = 0$ y α es raíz de multiplicidad $k - 1$ de f' .

Por hipótesis inductiva, α es raíz de multiplicidad

$$k - 1 \text{ de } f' \Leftrightarrow$$

$$f'(\alpha) = (f')'(\alpha) = \dots = (f')^{(k-2)}(\alpha) = 0 \text{ y } (f')^{(k-1)}(\alpha) \neq 0$$

$$f'(\alpha) = f''(\alpha) = \dots = f^{(k-1)}(\alpha) = 0 \text{ y } f_{(\alpha)}^{(k)} \neq 0$$

2.2.5. Cantidad de raíces de un polinomio

Sea $f \in k[x]$ no nulo de grado n . Entonces f tiene a la sumo n raíces en $|K|$ contadas cada uno con su multiplicidad.

Demostración: Haciendo la prueba por inducción sobre el grado n de f :

- Si $n = 0$: f es un polinomio constante no nulo y no tiene ninguna raíz.
- Si $n > 0$: Si f no tiene ninguna raíz en $|K|$, no hay nada que probar.

- Si f tiene por lo menos una raíz α , entonces $f = (x - \alpha)q$ y q es un polinomio de grado $n-1$ que por hipótesis inductiva tiene a la suma $n-1$ raíces en $|K$.

Por lo tanto, f tiene a la suma n raíces en $|K$.

Observación:

Sea $f \in |K[x]$ y sean $\alpha_1, \alpha_2, \dots, \alpha_m \in |K$ raíces distintas de f de multiplicidad k_1, k_2, \dots, k_m respectivamente, entonces:

$$(x - \alpha_1)^{k_1} \cdot (x - \alpha_2)^{k_2} \dots (x - \alpha_m)^{k_m} | f$$

Esta observación es debido a que

$$(x - \alpha_1)^{k_1} | f, (x - \alpha_2)^{k_2} | f, \dots, (x - \alpha_m)^{k_m} | f$$

Y al ser los polinomios de la izquierda coprimos dos a dos (no tiene ningún factor irreducible en común)

Sea en consecuencia su producto también divide a f .

Capítulo 3: RAÍCES DE POLINOMIOS EN $\mathbb{C}[x]$ Y APLICACIONES DEL TFA

3.1 Teorema Fundamental del Álgebra

Sea $f \in \mathbb{C}[x]$ un polinomio no nulo con coeficientes complejos de grado n mayor o igual que 1. Entonces f tiene por lo menos una raíz en \mathbb{C} .

Equivalentemente, f tiene exactamente n raíces contadas con su multiplicidad. Es decir que la factorización de $f \in \mathbb{C}[x]$ es siempre de la forma:

$$f = c(x - \alpha_1)^{k_1}(x - \alpha_2) \dots (x - \alpha_m) \quad c \in \mathbb{C}/\{0\}$$

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

Demostración Algebraica:

Definición: un campo F está algebraicamente cerrado si todo polinomio no constante en $F[x]$ tiene algún cero en F .

Con el siguiente teorema ponemos fin a nuestro primer objetivo fundamental, que es el Teorema Fundamental del Álgebra (TFA), para ello usaremos algunos resultados de funciones de variable compleja.

Teorema (TFA): El campo \mathbb{C} de números complejos es un campo algebraicamente cerrado.

En efecto:

Sea $f(z) = a_0 + a_1z + a_2z^2 + \dots + a_nz^n \in \mathbb{C}[z]$ tal que $a_n \neq 0$.

Suponiendo que $f(z) \in \mathbb{C}[z]$ polinomio que no tenga cero en \mathbb{C} esto es $(f(z) \neq 0; \forall z \in \mathbb{C})$.

Luego: $\lim_{|z| \rightarrow 0} |f(z)| \neq 0 \Rightarrow \left| \frac{1}{f(z)} \right| \rightarrow 0$

Es decir: $\lim_{|z| \rightarrow \infty} |f(z)| = 0$

Entonces $\frac{1}{f(z)}$ da una función entera, esto es $\frac{1}{f}$ es analítica en

todas partes, además $\frac{1}{f}$ es acotada en el plano. Entonces por el

teorema de Liouville, para funciones complejas, $\frac{1}{f}$ es constante

y así f es constante.

Por tanto, un polinomio no constante en $\mathbb{C}[z]$ debe tener un cero en \mathbb{C} , sigue que \mathbb{C} es cerrado algebraicamente.

3.2 Cota de Cauchy

La cota de Cauchy nos permite la ubicación de las raíces en un abierto del plano complejo

Proposición 3.1. Sea

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0 \in \mathbb{C}[x] \quad \text{Con } n \geq 1, a_n \neq 0$$

Sea $M = 1 + \left| \frac{a_{n-1}}{a_n} \right| + \dots + \left| \frac{a_0}{a_n} \right|$, luego toda

raíz $\alpha \in \mathbb{C}[x]$ de f verifica que $|\alpha| < M$

Demostración

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

- Si $|\alpha| \geq 1$, se observa que

$$f(\alpha) = 0 \quad \Leftrightarrow \quad a_n \alpha^n + a_{n-1} \alpha^{n-1} + \dots + a_0 = 0$$

$$\Leftrightarrow a_n \left(\alpha^n + \frac{a_{n-1}}{a_n} \alpha^{n-1} + \dots + \frac{a_0}{a_n} \right) = 0$$

$$\Leftrightarrow \alpha^n + \frac{a_{n-1}}{a_n} \alpha^{n-1} + \dots + \frac{a_0}{a_n} = 0$$

$$\Leftrightarrow \alpha^n = - \left(\frac{a_{n-1}}{a_n} \alpha^{n-1} + \dots + \frac{a_0}{a_n} \right)$$

$$\Leftrightarrow |\alpha|^n = \left| \frac{a_{n-1}}{a_n} \alpha^{n-1} + \dots + \frac{a_0}{a_n} \right| \leq \left| \frac{a_{n-1}}{a_n} \right| |\alpha|^{n-1} + \dots + \left| \frac{a_0}{a_n} \right| \leq$$

$$|\alpha|^{n-1} \left(\left| \frac{a_{n-1}}{a_n} \right| + \dots + \left| \frac{a_0}{a_n} \right| \right)$$

Para $|\alpha| \geq 1$ se tiene que

$$|\alpha|^{n-1} \geq |\alpha|^k, \quad \forall k, \quad 1 \leq k \leq n-1$$

Luego se tiene que

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

$$\therefore |\alpha| < M$$

Ejemplo: Sea $f = (2+i)x^5 + (2-i)x^4 + x^3 + 5i - 4 \in \mathbb{C}[x]$

Por la cota de Cauchy

$$\begin{aligned} M &= 1 + \left| \frac{2-i}{2+i} \right| + \left| \frac{-1}{2+i} \right| + \left| \frac{5i}{2+i} \right| + \left| \frac{-4}{2+i} \right| \\ &= 1 + \frac{|2-i|}{|2+i|} + \frac{|-1|}{|2+i|} + \frac{|5i|}{|2+i|} + \frac{|-4|}{|2+i|} + \\ &= 1 + \frac{\sqrt{5}}{\sqrt{5}} + \frac{1}{\sqrt{5}} + \frac{5}{\sqrt{5}} + \frac{4}{\sqrt{5}} \\ &= 2 + \frac{10}{\sqrt{5}} \cdot \frac{\sqrt{5}}{\sqrt{5}} \\ &= 2 + \frac{10\sqrt{5}}{5} \\ M &= 2 + 2\sqrt{5} \end{aligned}$$

Luego todos las raíces α de verificar $|\alpha| < 2 + 2\sqrt{5}$

3.3 Fórmula General,

Aplicaciones del TFA

3.3.1. Polinomios de Grado 1

$$f = ax + b \in \mathbb{C}[x], \alpha \neq 0$$

Entonces por el TFA f tiene una raíz

En efecto

$$ax + b = 0$$

$$(ax + b) + (-b) = 0 + (-b)$$

$$ax + (b+(-b)) = 0 + (-b)$$

$$ax + 0 = -b$$

$$ax = -b$$

$$a^{-1}(ax) = a^{-1}(-b)$$

$$(a^{-1}a)x = a^{-1}(-b)$$

$$1.x = a^{-1}(-b)$$

$$\therefore x = a^{-1}(-b) \text{ ó } x = \frac{-b}{a} \quad \dots \text{ F\acute{o}rmula General}$$

Ejemplo: Dado el polinomio $f = 3x - 12 \in \mathbb{R}[x]$

Haciendo el an\`alisis para su ra\`ız

Seg\`un la cota de Cauchy

$$M = 1 + \left| \frac{-12}{3} \right|$$

$$M = 5$$

Su ra\`ız α_1 se Encuentra en $|\alpha| < 5 \Leftrightarrow -5 < \alpha < 5$

Vecindad: $V_{(0.5)}$ aqu\`ı se encuentra la ra\`ız

Por el TFA y la f\`ormula para polinomios de grado 1 su ra\`ız

es:

$$X = \frac{-(-12)}{3}$$

$$X = 4 = \alpha_1$$

Adem\`as el polinomio se grafica en $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$

Ejemplo: Dado el polinomio

$$f = 2ix - 10 \in \mathbb{C}[x]$$

Análisis de su raíz:

Cota de Cauchy

$$M = 1 + \left| \frac{-10}{2i} \right|$$

$$M = 1 + \left| \frac{-5}{i} \right|$$

$$M = 1 + \frac{|-5|}{|i|}$$

$$M = 1 + \frac{5}{i}$$

$$M = 6$$

$$\Rightarrow |\alpha| < 6, \alpha \in \mathbb{C}, \alpha_1 \text{ raíz de } f \Leftrightarrow \alpha \in \overset{0}{B}(0, 6)$$

Por el TFA y la fórmula general

$$x = \frac{-(-10)}{2i} = \frac{10}{2i} \cdot \frac{2i}{2i}$$

$$x = \frac{5i}{i^2}$$

$$x = -5i = \alpha_1$$

Haciendo un análisis gráfico del polinomio

$$f = 2ix - 10 \in \mathbb{C}[x]$$

$x \in \mathbb{C} \wedge f \in \mathbb{C}$, pero el plano complejo es isomorfo al plano

\mathbb{R}^2 , es decir $\mathbb{C} \approx \mathbb{R}^2$.

Por lo tanto para representar un polinomio complejo se necesitaría 4 dimensiones ya que $\mathbb{R}^2 \times \mathbb{R}^2 = \mathbb{R}^4$

Ejemplo: Dado el polinomio

$$f = (2+i)x + (5-2i)$$

Análisis de su raíz:

Cota de Cauchy

$$M = 1 + \left| \frac{5-2i}{2+i} \right|$$

$$M = 1 + \frac{|5-2i|}{|2+i|}$$

$$M = 1 + \frac{\sqrt{29}}{\sqrt{5}}$$

$$M = 1 + \sqrt{\frac{29}{5}}$$

La raíz α_1 se encuentra

$$\text{En } |\alpha| < 1 + \sqrt{\frac{29}{5}}$$

Por Fórmula General

$$x = \frac{(2i-5)}{2+i}$$

$$x = \frac{-8+9i}{5} = \alpha_1$$

3.3.2. Polinomios de Grado 2

$$f = ax^2 + bx + c \in \mathbb{C}[x], \quad a \neq 0$$

Entonces por el TFA tiene 2 raíces

En efecto

$$f = a \left(x^2 + \frac{b}{a}x + \frac{c}{a} \right)$$

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

$$f = a \left[\left(x + \frac{b}{2a} \right)^2 - \frac{\Delta}{4a^2} \right], \text{ se } \beta \in \mathbb{C} \text{ tal que } \beta^2 = \Delta$$

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

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

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

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

Sus raíces son:

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

$$\alpha_2 = \frac{-b-\beta}{2a}$$

\therefore Sea $f = ax^2 + bx + c$, sus raíces se obtienen de la
Fórmula General

$$\alpha_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

Ejemplo: Dado el polinomio

$$f = x^2 + (1 + 3i)x - (8 - 4i)$$

Análisis de sus raíces

Ubicando sus raíces: cota de Cauchy

$$M = 1 + |1 + 3i| + |4i - 8|$$

$$M = 1 + \sqrt{10} + 4\sqrt{5}$$

Sus raíces $|\alpha| < M$

Por Fórmula General:

$$\alpha_{1,2} = \frac{-(1+3i) \pm \sqrt{(1+3i)^2 + 4(8-4i)}}{2}$$

$$\alpha_{1,2} = - \frac{(1+3i) \pm \sqrt{6i-8+32-16i}}{2}$$

$$\alpha_{1,2} = - \frac{-1-3i \pm \sqrt{10i+24}}{2}$$

$$\alpha_{1,2} = - \frac{1-3i \pm (5-i)}{2}$$

$$\alpha_1 = \frac{-1-3i+5-i}{2}$$

$$\alpha_1 = 2-2i$$

$$\alpha_2 = \frac{-1-3i-5-i}{2}$$

$$\alpha_2 = -3-i$$

\therefore sus raíces son $\alpha_1 = 2-2i$ y $\alpha_2 = -3-i$

Ejemplo: Dado el polinomio

$$f = x^2 - (5-i)x + (8-i)$$

Hacemos el análisis de sus raíces:

Cota de Cauchy

$$M = 1 + |5-i| + |8-i|$$

$$M = 1 + \sqrt{26} + \sqrt{65}$$

Sus raíces

$$|\alpha| < M$$

Por Fórmula General:

$$\alpha_{1,2} = \frac{5-i \pm \sqrt{(5-i)^2 - 4(8-i)}}{2}$$

$$\alpha_{1,2} = \frac{5-i \pm \sqrt{-8-6i}}{2}$$

$$\alpha_{1,2} = \frac{5-i \pm (1-3i)}{2}$$

$$\therefore \text{ sus raíces son } \alpha_1 = 3-2i \text{ y } \alpha_2 = 2+i$$

Observación:

Dado $z \in \mathbb{C}$, $\exists w \in \mathbb{C}$ tal que $w^2 = z$

En efecto

- Si $z = 0 \rightarrow w = 0$
- Si $z \neq 0 \rightarrow z = x + yi$

Debemos hallar $w = a + bi$ tal que $w^2 = z$

Por condición

$$(a+bi)^2 = x + yi$$

$$\text{Efectuando: } a^2 - b^2 + 2abi = x + yi$$

Luego se tiene

$$\begin{cases} a^2 - b^2 = x \\ 2ab = y \end{cases}$$

Reemplazando

$$b = \frac{y}{2a}$$

La primera igualdad se convierte

$$4a^2 - 4xa^2 - y^2 = 0$$

Resolviendo para a^2 se tiene

$$a^2 = \frac{x + \sqrt{x^2 + y^2}}{2} \text{ pero } a^2 \geq 0$$

$$\text{Entonces } a^2 = \frac{-x + \sqrt{x^2 + y^2}}{2}$$

Haciendo el mismo razonamiento obtenemos

$$b^2 = \frac{-x + \sqrt{x^2 + y^2}}{2}$$

En la segunda igualdad se cumple

$$2ab = y, \text{ entonces}$$

- Si $y > 0 \rightarrow a \wedge b$ tiene el mismo signo
- Si $y < 0 \rightarrow a \wedge b$ tiene signos diferentes

Para determinar W nos interesan los valores de a y b

$$a = \pm \sqrt{\frac{x + \sqrt{x^2 + y^2}}{2}} \quad b = \pm \sqrt{\frac{-x + \sqrt{x^2 + y^2}}{2}}$$

Luego

$$W = \pm \left(\sqrt{\frac{x + \sqrt{x^2 + y^2}}{2}} * \sqrt{\frac{-x + \sqrt{x^2 + y^2}}{2}} \right)$$

Donde * es el signo de y

Ejemplo: Determinar $\sqrt{-3 + 4i}$

Aplicando lo anterior

$$\sqrt{-3 + 4i} = \pm \left(\sqrt{\frac{-3 + \sqrt{3^2 + 4^2}}{2}} + \sqrt{\frac{3\sqrt{3^2 + 4^2}}{2}} \right)$$

$$\sqrt{-3 + 4i} = \pm (1 + 2i)$$

3.3.3. Polinomios de Grado 3: Fontana - Cardano

$$f = ax^3 + bx^2 + cx + d \in \mathbb{C}[x], a \neq 0$$

Entonces por el TFA tiene 3 raíces

En efecto

$$ax^3 + bx^2 + cx + d = 0 \quad \text{..... (1)}$$

$$x^3 + \frac{b}{a} x^2 + \frac{c}{a} x + \frac{d}{a} = 0$$

$$x^3 + Bx^2 + Cx + D = 0 \quad \text{..... (2)}$$

Haciendo el cambio: $x = y - \frac{B}{3}$ (3)

$$\left(y - \frac{B}{3}\right)^3 + B \left(y - \frac{B}{3}\right)^2 + C \left(y - \frac{B}{3}\right) + D = 0$$

$$y^3 - 3y^2 \left(\frac{B}{3}\right) + 3y \left(\frac{B^2}{9}\right) - \frac{B^3}{27} + By^2 - \frac{2B^2}{3}y + \frac{B^3}{9} + Cy - \frac{BC}{3} + D = 0$$

$$y^3 + \left(\frac{B^2}{3} - \frac{2B^2}{3} + C\right)y + D - \frac{BC}{27} + \frac{B^3}{9} = 0$$

$$y^3 + \left(C - \frac{B^3}{3}\right)y + \left(\frac{2B^2}{27} + D - \frac{BC}{3}\right) = 0$$

$$y^3 + py + q = 0 \quad \text{..... (4)}$$

Ahora tenemos la ecuación cúbica reducida

Sabemos por el TFA que (4) tiene 3 raíces. Sea y_0 una de esas raíces, enseguida introducimos la variable auxiliar "u" y consideremos el polinomio.

$$f = u^2 - y_0 u - \frac{P}{3} \in \mathbb{C}[x]$$

Y sean α y β sus raíces

Por fórmulas de Cardano - Vieta tenemos:

$$\alpha + \beta = y_0 \quad \text{..... (5)}$$

$$\alpha \cdot \beta = -\frac{P}{3} \quad \text{..... (6)}$$

sustituyendo y_0 en (4), se obtiene:

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

de donde

$$\alpha^3 + \beta^3 + (3\alpha\beta + p)(\alpha + \beta) + q = 0 \quad \text{..... (7)}$$

de (6) y (7) se tiene

$$3 \alpha \beta + p = 0$$

$$\rightarrow \alpha^3 + \beta^3 = -q \quad \text{..... (8)}$$

de (6) además se tiene:

$$\alpha^3 \cdot \beta^3 = \frac{-p^3}{27} \quad \text{..... (9)}$$

Teniendo en cuenta, las fórmulas de Cardano - Vieta

α^3 y β^3 , serán solución de la ecuación de segundo grado:

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

Cuyas raíces son:

La primera:

$$\alpha^3 = z_1 = \frac{-q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$$
$$\alpha = \sqrt[3]{z_1} = \sqrt[3]{\frac{-q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} \quad \text{..... (10)}$$

La segunda:

$$\beta^3 = z_2 = \frac{-q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$$
$$\beta = \sqrt[3]{z_2} = \sqrt[3]{\frac{-q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} \quad \text{..... (11)}$$

Como $y_0 = \alpha + \beta$, es raíz de (4), luego

$$y_0 = \alpha + \beta = \sqrt[3]{\frac{-q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{\frac{-q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$$

de (10) y (11) puesto que la raíz cubica tiene 3 valores en el campo de los complejos, luego α y β tiene 3 valores cada uno. Para un valor de α tenemos que tomar solamente un valor de los tres de β el cual satisface la condición (6)

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

$$\alpha_2 = \alpha_1 W \quad \alpha_3 = \alpha_1 W^2 \quad ; \text{donde } W^3 = 1$$

Lo mismo sucede si β_1 es uno de los tres valores de la raíz de β , los otros valores son:

$$\beta_2 = \beta_1 W \quad \beta_3 = \beta_1 W^2$$

Luego

- $\alpha_1 \cdot \beta_1 = \frac{-p}{3}$
- $\alpha_2 \cdot \beta_3 = \alpha_1 W \beta_1 \cdot W^2 = \alpha_1 \beta_1 W^3 = \frac{-p}{3}$
- $\alpha_3 \cdot \beta_2 = \alpha_1 W^2 \beta_1 \cdot W = \alpha_1 \beta_1 W^3 = \frac{-p}{3}$

Así las tres raíces de la ecuación (4)

$$\left\{ \begin{array}{l} y_1 = \alpha_1 + \beta_1 \\ y_2 = \alpha_2 + \beta_3 \\ y_3 = \alpha_3 + \beta_2 \end{array} \right.$$

Observación: Raíces Cúbicas de la Unidad

$$\sqrt[3]{1} = \begin{cases} 1 \\ -\frac{1}{2} + \frac{\sqrt{3}}{2} i = w \\ -\frac{1}{2} - \frac{\sqrt{3}}{2} i = w^2 \end{cases}$$

En efecto: Sea el complejo $Z = 1$

En forma polar:

$$Z = 1 = 1 + 0i = \cos 0^\circ + i \sin 0^\circ$$

Luego la raíz cúbica es

$$Z_k = \sqrt[3]{|Z|} \left[\cos\left(\frac{0+2k\pi}{3}\right) + i \sin\left(\frac{0+2k\pi}{3}\right) \right]$$

Como $|Z| = 1$

$$Z_k = \left[\cos\left(\frac{2k\pi}{3}\right) + i \sin\left(\frac{2k\pi}{3}\right) \right]$$

Donde : $K = 0, 1, 2$

Para $k = 0 \rightarrow Z_0 = \cos 0^\circ + i \sin 0^\circ = 1$

Para $k = 1 \rightarrow Z_1 = \cos \frac{2\pi}{3} + i \sin \frac{2\pi}{3} = -\frac{1}{2} + \frac{\sqrt{3}}{2} i = w$

Para $k = 2 \rightarrow Z_2 = \cos \frac{4\pi}{3} + i \sin \frac{4\pi}{3} = -\frac{1}{2} - \frac{\sqrt{3}}{2} i = w^2$

Observación: Teorema de Cardano - Vieta

Sea: $ax^2 + bx + c = 0$, $\in \mathbb{C}[x]$ con $a \neq 0$

De raíces α_1 y α_2 se cumple

$$\alpha_1 + \alpha_2 = \frac{-b}{a}$$

$$\alpha_1 \cdot \alpha_2 = \frac{c}{a}$$

En efecto: De la fórmula general

$$\alpha_1 = \frac{-b + \sqrt{b^2 - 4ac}}{2a}, \quad \alpha_2 = \frac{-b - \sqrt{b^2 - 4ac}}{2a},$$

$$\text{I. } \alpha_1 + \alpha_2 = \frac{-b + \sqrt{\Delta}}{2a} + \frac{-b - \sqrt{\Delta}}{2a} = \frac{-2b}{2a} = \frac{-b}{a}$$

$$\text{II. } \alpha_1 \cdot \alpha_2 = \left(\frac{-b + \sqrt{\Delta}}{2a} \right) \left(\frac{-b - \sqrt{\Delta}}{2a} \right) = \frac{b^2 - b\sqrt{\Delta} - b\sqrt{\Delta} - \Delta}{4a^2}$$

$$= \frac{b^2 - (b^2 - 4ac)}{4a^2}$$

$$= \frac{4ac}{4a^2}$$

$$\alpha_1 \cdot \alpha_2 = \frac{c}{a}$$

Ejemplo: Dado el polinomio

$f = x^3 + 3\sqrt[3]{3}x - 2$. Determinar sus raíces

$$f = x^3 + 3\sqrt[3]{3}x - 2 = 0$$

Esta ecuación corresponde a la forma reducida

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

Donde $p = 3\sqrt[3]{3}$ $q = -2$

Luego

$y_1 = \alpha + \beta$, es una raíz de la ecuación reducida

Además cumple

$$\alpha^3 + \beta^3 = 2$$

$$\alpha^3 \cdot \beta^3 = -3$$

Donde α^3 y β^3 son raíces de la ecuación

$$z^2 - 2z - 3 = 0$$

$$\rightarrow z = \frac{2 \pm \sqrt{4+12}}{2} = 1 \pm 2$$

$$\alpha^3 = z_1 = 3 \qquad \beta^3 = z_2 = -1$$

$$\alpha = \sqrt[3]{3} \qquad \beta = \sqrt[3]{-1}$$

$$\alpha = \sqrt[3]{3} \qquad \beta = -1$$

Las raíces de la ecuación son:

$$y_1 = \sqrt[3]{3} - 1$$

$$y_2 = \sqrt[3]{3} w - w^2$$

$$y_3 = \sqrt[3]{3} w^2 - w$$

3.3.4. Polinomios de Grado 4: Ferrari

$$f = ax^4 + bx^3 + cx^2 + dx + e \in \mathbb{C}[x], a \neq 0$$

Entonces por el TFA tiene 4 raíces

En efecto:

$$ax^4 + bx^3 + cx^2 + dx + e = 0 \quad \dots\dots(1)$$

$$x^4 + \frac{b}{a}x^3 + \frac{c}{a}x^2 + \frac{d}{a}x + \frac{e}{a} = 0$$

$$x^4 + Ax^3 + Bx^2 + Cx + D = 0 \quad \dots\dots(2)$$

La ecuación con coeficiente complejo se reduce a la solución de alguna ecuación cúbica auxiliar. Esto es logrado por un procedimiento debido a Ferrari, haciendo la sustitución.

$$x = y - \frac{A}{4}$$

$$\left(y - \frac{A}{4}\right)^4 + A\left(y - \frac{A}{4}\right)^3 + B\left(y - \frac{A}{4}\right)^2 + C\left(y - \frac{A}{4}\right) + D = 0$$

$$y^4 + \left(B - \frac{3A^2}{8}\right)y^2 + \left(\frac{2A^3}{16} - \frac{AB}{2} + C\right)y + \left(\frac{A^2B}{16} - \frac{3A^4}{256} - \frac{AC}{4}\right) = 0$$

Se obtiene la ecuación reducida

$$y^4 + py^2 + qy + r = 0 \quad \dots\dots(3)$$

El miembro izquierdo de la ecuación (3) es transformado con la ayuda de un parámetro auxiliar α y completando cuadrados.

$$y^4 + py^2 + \frac{p^2}{4} + qy + r - \frac{p^2}{4} = 0$$

$$\left(y^2 + \frac{p}{2}\right)^2 + 2\alpha\left(y^2 + \frac{p}{2}\right) + \alpha^2 + qy + r - \frac{p^2}{4} - 2\alpha\left(y^2 + \frac{p}{2}\right) - \alpha^2 = 0$$

Obteniéndose

$$(y^2 + \frac{p}{2} + \alpha)^2 - \left[2\alpha y^2 - qy + \left(\alpha^2 + p\alpha - r + \frac{p^2}{4} \right) \right] = 0$$

$$(y^2 + \frac{p}{2} + \alpha)^2 - \left[2\alpha \left(y^2 - \frac{q}{2\alpha}y + \frac{q^2}{16\alpha^2} - \frac{q^2}{16\alpha^2} \right) + \left(\alpha^2 + p\alpha - r + \frac{p^2}{4} \right) \right] = 0$$

$$(y^2 + \frac{p}{2} + \alpha)^2 - \left[2\alpha \left(y - \frac{q}{4\alpha} \right)^2 - \frac{q^2}{8\alpha} + \left(\alpha^2 + p\alpha - r + \frac{p^2}{4} \right) \right] = 0$$

$$\left[(y^2 + \frac{p}{2} + \alpha)^2 - 2\alpha \left(y - \frac{q}{4\alpha} \right)^2 \right] + \left[\frac{q^2}{8\alpha} - \left(\alpha^2 + p\alpha - r + \frac{p^2}{4} \right) \right] = 0 \quad \dots (4)$$

Así se debe tener la ecuación

$$q^2 - 8\alpha \left(\alpha^2 + p\alpha - r + \frac{p^2}{4} \right) = 0 \dots \dots \dots (5)$$

La ecuación cúbica en la variable α con coeficientes complejos. Como sabemos, esta ecuación tiene tres raíces complejas.

Sea α_0 una de las raíces, expresado en radicales y con coeficientes de la ecuación (3). Luego la ecuación (4) tiene raíz α_0 .

Así:

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

que da origen a las ecuaciones cuadráticas:

$$\left. \begin{aligned} y^2 - \sqrt{2\alpha_0}y + \left(\frac{p}{2} + \alpha_0 + \frac{q}{2\sqrt{2\alpha_0}}\right) &= 0 \\ y^2 + \sqrt{2\alpha_0}y + \left(\frac{p}{2} + \alpha_0 + \frac{q}{2\sqrt{2\alpha_0}}\right) &= 0 \end{aligned} \right\} \quad (6)$$

Luego las raíces de (6) servirán como raíces de (4)

Ejemplo: Dado el polinomio

$$f = x^4 - 2x^3 - 5x^2 + 10x - 3$$

Encontrar sus raíces, primero hacemos el cambio de variable:

$$x = y - \frac{-2}{4} \rightarrow x = y + \frac{1}{2}$$

Así:

$$\left(y + \frac{1}{2}\right)^4 - 2\left(y + \frac{1}{2}\right)^3 - 5\left(y + \frac{1}{2}\right)^2 + 10\left(y + \frac{1}{2}\right) - 3 = 0$$

$$\left(y + \frac{1}{2}\right)^4 = C_0^4 y^4 + C_1^4 \left(\frac{1}{2}\right) y^3 + C_2^4 \left(\frac{1}{2}\right)^2 y^2 + C_3^4 \left(\frac{1}{2}\right)^3 y + C_4^4 \left(\frac{1}{2}\right)^4$$

$$= y^4 + 2y^3 + \frac{3}{2}y^2 + \frac{1}{2}y + \frac{1}{16}$$

$$\left(y + \frac{1}{2}\right)^3 = y^3 + \frac{3}{2}y^2 + \frac{3}{4}y + \frac{1}{8}$$

$$\Rightarrow -2\left(y + \frac{1}{2}\right)^3 = -2y^3 - 3y^2 - \frac{3}{2}y - \frac{1}{4}$$

$$\left(y + \frac{1}{2}\right)^2 = y^2 + y + \frac{1}{4}$$

$$\Rightarrow -5\left(y + \frac{1}{2}\right)^2 = -5y^2 - 5y - \frac{5}{4}$$

$$10\left(y + \frac{1}{2}\right) - 3 = 10y + 2$$

La ecuación de grado 4 reducida es:

$$y^4 - \frac{13}{2}y^2 + 4y + \frac{9}{16} = 0$$

donde:

$$p = -13/2 \quad q = 4 \quad r = 9/16$$

Por deducción para polinomios de grado 4

$$q^2 - 8\alpha\left(\alpha^2 + p\alpha - r + \frac{p^2}{4}\right) = 0, \text{ Ecuación cúbica resolvente}$$

reemplazando los valores conocidos p , q y r , además reduciendo se tiene.

$$2\alpha^3 - 13\alpha^2 + 20\alpha - 4 = 0$$

Donde se verifica que $\alpha_1 = 2$ es una raíz de la ecuación cúbica resolvente. Luego $\alpha_1 = 2$ da origen a dos ecuaciones cuadráticas.

$$\left. \begin{aligned} y^2 - \sqrt{2(2)}y + \left(\frac{-13}{4} + 2 + \frac{4}{2\sqrt{2(2)}}\right) &= 0 \\ y^2 - \sqrt{2(2)}y + \left(\frac{-13}{4} + 2 + \frac{4}{2\sqrt{2(2)}}\right) &= 0 \end{aligned} \right\}$$

Reduciendo:

$$\left. \begin{aligned} y^2 - 2y - \frac{1}{4} &= 0 \\ y^2 - 2y - \frac{5}{4} &= 0 \end{aligned} \right\}$$

Resolviendo:

$$y_1 = \frac{2 + \sqrt{5}}{2}; y_2 = \frac{2 - \sqrt{5}}{2}; y_3 = \frac{-2 + \sqrt{13}}{2}; y_4 = \frac{-2 - \sqrt{13}}{2}$$

Volviendo para encontrar los valores de x: $x = y + \frac{1}{2}$

$$x_1 = \frac{3 + \sqrt{5}}{2}; x_2 = \frac{3 - \sqrt{5}}{2}; x_3 = \frac{-1 + \sqrt{13}}{2}; x_4 = \frac{-1 - \sqrt{13}}{2}$$

que son las 4 raíces del polinomio.

$$f = x^4 - 2x^3 - 5x^2 + 10x - 3$$

3.3.4.1. Ecuación Cúbica Resolvente

Enfoquémonos en la ecuación cúbica resolvente para f de grado 4.

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

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

$$q^2 - 8\alpha^3 - 8p\alpha^2 - 8\alpha \left(\frac{p^2 - 4r}{4} \right) = 0$$

$$q^2 - 8\alpha^3 - 8p\alpha^2 - 2\alpha(p^2 - 4r) = 0$$

dándole forma a esta ecuación cubica

$$Z = -2\alpha \rightarrow \begin{cases} Z^3 = -8\alpha^3 \\ Z^2 = 4\alpha^2 \end{cases}$$

reemplazando:

$$q^2 + z^3 - 2pz^2 + (p^2 - 4r)z = 0$$

Por lo tanto obtenemos la Ecuación cúbica resolvente

$$z^3 - 2pz^2 + (p^2 - 4r)z + q^2 = 0$$

Observación: $f = x^4 + px^2 + qx + r$

Las raíces son del tipo $\alpha = \frac{1}{2}(\pm\sqrt{-z_1} \pm \sqrt{-z_2} \pm \sqrt{-z_3})$ donde z_1, z_2, z_3 son las tres raíces del polinomio resolvente.

$$z^3 - 2pz^2 + (p^2 - 4r)z + q^2$$

La condición aquí para elegir las 4 raíces complejas en las 8 posibles es:

$$(\pm\sqrt{-z_1})(\pm\sqrt{-z_2})(\pm\sqrt{-z_3}) = -q$$

3.4 Polinomio Soluble Por Radicales

Llegamos ahora con una extensa disposición de resultados de la teoría de Grupos y Campos dispuestos a mostrar nuestro objetivo final.

Que no todos los ceros de todo polinomio $f_{(x)}$ de grado 5 puede expresarse en términos de radicales (es decir que involucre los coeficientes de $f_{(x)}$ y las operaciones algebraicas como $+$, $-$, \times , \div , $\sqrt[k]{}$). Hasta el momento hemos obtenido las raíces complejas de polinomios $f_{(x)} \in \mathbb{C}[x]$ de $\partial f \leq 4$.

Nuestro objetivo final involucra a muchos matemáticos importantes en la historia, pero principalmente a dos de ellos contemporáneos, matemáticos muy jóvenes que influyeron en el desarrollo del Álgebra Moderna. Ellos son Niels Henrik Abel (1802 - 1829) y Evaristo Galois (1811 - 1832).

Abel (1820).

No hay una fórmula que describa las raíces de un polinomio general f de grados ≥ 5 a partir de sus coeficientes y las operaciones elementales $+$, $-$, \times , \div , $\sqrt[k]{}$

Galois (1830)

Caracterizó cuales eran los polinomios de grado ≥ 5 para los cuales existe tal fórmula, aunque no es fácilmente deducible de los coeficientes del polinomio, sino que tiene que ver con cierto grupo asociado con dicho polinomio.

A partir de ahora daremos a conocer definiciones y teoremas y lo asociamos con resultados del capítulo I y II para ver de manera precisa que significa estos resultados y probarlos.

3.4.1. Grupo $G(E/F)$

Definición: si σ es un isomorfismo de un campo E en algún campo, entonces un elemento a de E queda fijo bajo σ si $a\sigma = a$. Una colección S de isomorfismo de E deja fijo un subcampo F de E si cada $a \in F$ queda fijo bajo toda $\sigma \in S$. Si $\{\sigma\}$ deja fijo F , entonces σ deja fijo F .

Teorema: sea E un campo y sea F un subcampo de E . entonces, el conjunto $G(E/F)$ de todos los automorfismos de E que deja fijo F forma un subgrupo de todos los automorfismos de E .

Demostración:

Para $\sigma, \tau \in G(E/F)$ y $a \in F$, tenemos

$$a(\sigma\tau) = (a\sigma)\tau = a\tau = a$$

de aquí que $\sigma\tau \in G(E/F)$

El automorfismo identidad $i : E \rightarrow E$, definida por

$ai = a, \forall a \in E$ es obviamente un automorfismo de E , además como $a \in F$ y por hipótesis $a\sigma = a \forall a \in F$, entonces $a = a\sigma^{-1}$, de esto último $\sigma \in G(E/F)$ implica que

$\sigma^{-1} \in G(E/F)$. por lo tanto $G(E/F)$ es un subgrupo del grupo de todos los automorfismos de E .

Como $a\sigma = a, \forall \sigma \in G(E/F)$ se sigue que el campo $E_{G(E/F)}$ (campo de todos los elementos de E que quedan fijos bajo $G(E/F)$) contiene F , es decir $F \leq E_{G(E/F)}$.

Definición: el grupo $G(E/F)$ es el grupo de automorfismos de E que dejan fijo F , o brevemente, $G(E/F)$ es el grupo de E sobre F .

Ejemplo: consideremos $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ sobre \mathbb{Q} . luego los automorfismos

i : automorfismo identidad

$$\sigma_1 = \Psi_{\sqrt{2}, -\sqrt{2}}$$

$$\sigma_2 = \Psi_{\sqrt{3}, -\sqrt{3}}$$

$$\sigma_3 = \Psi_{\sqrt{2}, -\sqrt{2}} \Psi_{\sqrt{3}, -\sqrt{3}}$$

donde:

$$\sigma_1 = \Psi_{\sqrt{2}, -\sqrt{2}}: (\mathbb{Q}(\sqrt{3}))(\sqrt{2}) \rightarrow (\mathbb{Q}(\sqrt{3}))(\sqrt{2})$$

Definido por:

$$(a + b\sqrt{2}) \Psi_{\sqrt{2}, -\sqrt{2}} = a - b\sqrt{2}$$

$$\sigma_2 = \Psi_{\sqrt{3}, -\sqrt{3}}: (\mathbb{Q}(\sqrt{2}))(\sqrt{3}) \rightarrow (\mathbb{Q}(\sqrt{2}))(\sqrt{3})$$

Definido por:

$$(a + b\sqrt{3}) \Psi_{\sqrt{3}, -\sqrt{3}} = a - b\sqrt{3}$$

$$\sigma_3 = \Psi_{\sqrt{2}, -\sqrt{2}} \Psi_{\sqrt{3}, -\sqrt{3}}: \mathbb{Q}(\sqrt{2}, \sqrt{3}) \rightarrow \mathbb{Q}(\sqrt{2}, \sqrt{3})$$

Definido por:

$$(a + b\sqrt{2}\sqrt{3}) \Psi_{\sqrt{2}, -\sqrt{2}} \Psi_{\sqrt{3}, -\sqrt{3}} = a - b\sqrt{2}\sqrt{3}$$

En forma equivalente:

$$(a + b\sqrt{6}) \Psi_{\sqrt{2}, -\sqrt{2}} \Psi_{\sqrt{3}, -\sqrt{3}} = a - b\sqrt{6}$$

\mathbb{Q} es el campo fijo de $G = \{i, \sigma_1, \sigma_2, \sigma_3\}$. Luego como en el capítulo I construimos la tabla de grupo para G .

	i	σ_1	σ_2	σ_3
i	i	σ_1	σ_2	σ_3
σ_1	σ_1	i	σ_3	σ_2
σ_2	σ_2	σ_3	i	σ_1
σ_3	σ_3	σ_2	σ_1	i

Para ver cómo hemos construido la tabla tenemos dos ejemplos.

- $$\begin{aligned}
\sigma_1 \sigma_1 &= \Psi_{\sqrt{2}, -2} \Psi_{\sqrt{2}, -2} \\
&= (a + b\sqrt{2}) \Psi_{\sqrt{2}, -\sqrt{2}} \Psi_{\sqrt{2}, -\sqrt{2}} \\
&= ((a + b\sqrt{2}) \Psi_{\sqrt{2}, \sqrt{-2}}) \Psi_{\sqrt{2}, -\sqrt{2}} \\
&= (a - b\sqrt{2}) \Psi_{\sqrt{2}, -\sqrt{2}} \\
&= (a - -b\sqrt{2}) \\
&= a + b\sqrt{2}
\end{aligned}$$

$$\sigma_1 \sigma_1 = i$$

- $$\begin{aligned}
\sigma_1 \sigma_3 &= \Psi (\psi_{\sqrt{2}, -\sqrt{2}} \Psi_{\sqrt{3}, -\sqrt{3}}) \quad \text{"asociando"} \\
&= (\Psi_{\sqrt{2}, -\sqrt{2}} \psi_{\sqrt{2}, -\sqrt{2}}) (\psi_{\sqrt{3}, -\sqrt{3}}) \\
&= i \Psi_{\sqrt{3}, -\sqrt{3}} \\
&= \Psi_{\sqrt{3}, -\sqrt{3}}
\end{aligned}$$

$$\sigma_1 \sigma_3 = \sigma_2$$

$\therefore G\left(Q(\sqrt{2}, \sqrt{3})/Q\right)$ es un grupo y además

tiene orden 4 $[Q(\sqrt{2}, \sqrt{3}) : Q] = 4$

3.4.2. Extensión por Radicales

Definición: Si K es una extensión finita de un campo F , $G(K/F)$ es el grupo de Galois de K sobre F .

Definición: Una extensión K de un campo F es una extensión de F por radicales si existen elementos $\alpha_1, \dots, \alpha_r \in K$ y enteros positivos n_1, \dots, n_r tales que $K = F(\alpha_1, \dots, \alpha_r)$, $\alpha_1^{n_1} \in F$ y $\alpha_i^{n_i} \in F(\alpha_1, \dots, \alpha_{i-1})$ para $1 < i \leq r$

3.4.3. Polinomio soluble por Radicales

Definición: Un polinomio $f_{(x)} \in F[x]$ es soluble por radicales sobre F si el campo de descomposición E de $f_{(x)}$ sobre F está contenido en una extensión por radicales. Para nuestro caso $\mathbb{C}, \mathbb{R}, \mathbb{Q}$ campos de característica 0. Un polinomio $f_{(x)} \in \mathbb{R}[x]$ es soluble por radicales sobre \mathbb{R} si podemos obtener todo cero de $f_{(x)}$ usando una sucesión finita de operaciones de $+$, $-$, \times , \div , $\sqrt[k]{}$, utilizando elementos de \mathbb{R} .

Entonces decir que la quintica (o $f(x)$ de grado ≥ 5) es insoluble, significa que existe algún polinomio de grado ≥ 5 con coeficientes reales, que no es soluble por radicales. Luego decir que la quintica no es soluble, no quiere decir que ninguna quintica sea soluble por radicales.

3.4.4. Condiciones para que un polinomio de grado mayor o igual a 5 sea soluble o insoluble por Radicales

Estamos aquí concluyendo este capítulo después de haber recorrido un largo camino, llegando, deteniéndonos y pasando por el maravilloso mundo de tres grandes estructuras algebraicas: grupos, anillos y campos. Es algo mágico por las herramientas (definiciones, teoremas, resultados y aplicaciones) que tienen estas estructuras. Y a la vez te genera algo de nostalgia porque son tan profundas y amplias.

3.4.4.1. Primera Condición

Un polinomio $f(x) \in \mathbb{R}[X]$ es soluble por radicales sobre \mathbb{R} . Si su campo de descomposición \mathbb{K} sobre \mathbb{R} tiene un grupo de descomposición soluble.

Recordemos que en el capítulo I hemos definido lo que es un grupo soluble, es aquel que tiene una serie de composición con coeficientes abelianos.

Teorema: Sea $a \in \mathbb{C}$. Si \mathbb{K} es el campo de descomposición de $x^n - a$ sobre \mathbb{C} , entonces $G(\mathbb{K}/\mathbb{C})$ es un grupo soluble.

Demostración:

Se ve que \mathbb{C} contiene todas las raíces n -ésimas del unitario, estas raíces n -ésimas del unitario forman un subgrupo cíclico de $\langle \mathbb{C}^*, \cdot \rangle$. Sea w un generador del subgrupo. Entonces las raíces n -ésimas del unitario son:

$$1, w, w^2, \dots, w^{n-1}$$

Si $\beta \in \bar{\mathbb{C}}$ es un cero de $(x^n - a) \in F[x]$, entonces todos los ceros de $x^n - a$ son:

$$\beta, w\beta, w^2\beta, \dots, w^{n-1}\beta.$$

Como $\mathbb{K} = \mathbb{C}(\beta)$, un automorfismo σ en $G(\mathbb{K}/\mathbb{C})$ determinado por $\beta\sigma = w^i\beta$ y si $T \in G(\mathbb{K}/\mathbb{C})$ de aquí $T = w^i\beta$ entonces:

$$\begin{aligned}\beta(\sigma T) &= (w^i\beta)T = w^iw^i\beta \\ &= w^i(w^i\beta) \\ &= \beta(T\sigma)\end{aligned}$$

Así que: $\sigma T = T\sigma$ y $G(\mathbb{K}/\mathbb{C})$ es abeliano y, por tanto, soluble.

Ejemplo: El polinomio $x^5 - 1$ es soluble por radicales sobre \mathbb{Q} . El campo de descomposición K de $x^5 - 1$ esta generado sobre \mathbb{Q} por una raíz quinta primitiva W del unitario. Entonces, $W^5 = 1$ y $K = \mathbb{Q}(W)$

Ejemplo: $x^5 - 2$ es soluble por radicales sobre \mathbb{Q} , su campo de descomposición sobre \mathbb{Q} está generado por $\sqrt[5]{2}$ y W , donde $\sqrt[5]{2}$ es el cero real $x^5 - 2$.

Observación: El teorema anterior, se generaliza:

Si F es un campo de característica 0 (\mathbb{C} , \mathbb{R} y \mathbb{Q}) y sea $a \in F$. Si K es el campo de descomposición de $x^n - a$ sobre F , Entonces $G(K/F)$ es un grupo soluble.

3.4.4.2. Segunda Condición

Si \mathbb{K} es una extensión normal por radicales de un campo F de característica 0 (\mathbb{C} , \mathbb{R} y \mathbb{Q}), entonces $G(K/F)$ es soluble.

Demostración:

Sean $\alpha_1, \dots, \alpha_r \in K$ y n_1, \dots, n_r tales que $K = F(\alpha_1, \dots, \alpha_r)$, $\alpha_1^{n_1} \in F$ y $\alpha_i^{n_i} \in F(\alpha_1, \dots, \alpha_{i-1})$ para $1 < i \leq r$, esta se dio en una definición anterior.

Sea $K_0 = F$ y sea K_i el campo de descomposición de $x^{n_i} - \alpha_i^{n_i}$ sobre K_{i-1} . Entonces $\mathbb{K} \leq \mathbb{K}_r$ por el teorema anterior $G(K_i/K_{i-1})$ es soluble además como $G(K_i/K_{i-1}) \simeq G(K_r/K_{i-1}) / G(K_r/K_i)$ la serie normal $\{i\} \leq G(K_r/K_{r-1}) \leq G(K_r/K_{r-2}) \leq \dots \leq G(K_r/K_0) = G(K_r/F)$ tiene grupos cocientes solubles, esta serie tiene un refinamiento que es una serie de composición con cocientes abelianos, de modo que $G(K_r/F)$ es soluble. La

última parte lo estudiamos en el capítulo I en grupos solubles.

3.4.4.3. Tercera Condición

Existe un subcampo F de los números reales y un polinomio $f(x) \in F[x]$ de grado 5 con un campo de descomposición E sobre F tal que $G(E/F) \simeq S_5$.

En efecto:

Recordando que una serie de composición de S_5 es

$$\{1\} < A_5 < S_5$$

Como A_5 no es abeliano, entonces $G(E/F)$ no es soluble, entonces $f(x)$ no es soluble por radicales sobre F .

Por lo tanto un polinomio de grado n no necesariamente es soluble por radicales para $n \geq 5$.

Capítulo 4: APLICACIONES DE RESULTADOS EN $\mathbb{Q}[x]$ Y $\mathbb{R}[x]$

4.1 Polinomios con coeficientes en \mathbb{Q}

Por la teoría descrita anteriormente, se puede tener los siguientes resultados para $f \in \mathbb{Q}[x]$

1. Sea $f \in \mathbb{Q}[x]$ de $\partial f = n \geq 1$, tiene a lo sumo n raíces en \mathbb{Q} contados con su multiplicidad.
2. Sea $f \in \mathbb{Q}[x]$ de $\partial f \geq 1$, si f tiene una raíz, entonces f es reducible.
3. Si $f \in \mathbb{Q}[x]$ es reducible no implica que f tiene raíces en \mathbb{Q} . Así se tiene por ejemplo $f = x^2 - 2$ es reducible y sin raíces racionales.
4. Sea $f \in \mathbb{Q}[x]$ de grado 2 ó 3 es reducible si y solo si tiene una raíz en \mathbb{Q}

4.1.1. Cálculo de raíces en \mathbb{Q}

Se puede encontrar todas las raíces racionales de un polinomio $f \in \mathbb{Q}[x]$ por medio de un algoritmo.

$$\text{Sea } f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Q}[x].$$

Entonces existe $C \in \mathbb{Z}/\{0\}$ tal que $g = Cf \in \mathbb{Z}[x]$, donde

C : mcm de los denominadores de los coeficientes de f y además las raíces de f claramente coinciden con las de g .

Por consiguiente para encontrarlas raíces racionales de $f \in \mathbb{Q}[x]$, nos basta con encontrar las raíces racionales de $g \in \mathbb{Z}[x]$.

4.1.2. Lema uno de Gauss y aplicación

Sea $f(x) = a_n x^n + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$ con $a_n, a_0 \neq 0$. Entonces, si $\frac{\alpha}{\beta} \in \mathbb{Q}$ es una raíz racional de f , con α y $\beta \in \mathbb{Z}$ primos entre sí, entonces $\alpha | a_0$ y $\beta | a_n$.

Demostración:
Por hipótesis

$$f\left(\frac{\alpha}{\beta}\right) = 0$$

$$a_n \left(\frac{\alpha}{\beta}\right)^n + a_{n-1} \left(\frac{\alpha}{\beta}\right)^{n-1} + a_1 \left(\frac{\alpha}{\beta}\right) + a_0 = 0$$

$$\frac{a_n \alpha^n}{\beta^n} + \frac{a_{n-1} \alpha^{n-1}}{\beta^{n-1}} + \dots + \frac{a_1 \alpha}{\beta} + a_0 = 0$$

$$\frac{a_n \alpha^n + a_{n-1} \alpha^{n-1} \beta + \dots + a_1 \alpha \beta^{n-1} + a_0 \beta^n}{\beta^n} = 0$$

$$a_n \alpha^n + a_{n-1} \alpha^{n-1} \beta + \dots + a_1 \alpha \beta^{n-1} + a_0 \beta^n = 0 \quad \dots (*)$$

$$a_n \alpha^n + a_{n-1} \alpha^{n-1} \beta + \dots + a_1 \alpha \beta^{n-1} = -a_0 \beta^n$$

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

de lo último $\alpha | -a_0 \beta^n$, pero al ser α y β PESI, entonces $\alpha | a_0$.

de la misma manera que el caso anterior se tiene como $\beta | -a_n \alpha^n$, resulta $\beta | a_n$.

APLICACIÓN DEL LEMA DE GAUSS (algoritmo para calcular las raíces racionales de un polinomio en $\mathbb{Z}[x]$)

En las condiciones del Lema de Gauss implica que si construye el conjunto finito A de los divisores positivos y negativos de a_0 y el conjunto finito de β de los de a_n , las raíces del polinomio f se encuentran en el conjunto de todos las fracciones $\frac{\alpha}{\beta}$, eligiendo α en A y $\beta \in \beta$.

Verificando para cada fracción $\frac{\alpha}{\beta}$ cumpla $f\left(\frac{\alpha}{\beta}\right) = 0$, así se obtienen todas las raíces racionales de f .

Debemos tener un poco de cuidado con este algoritmo porque no aclara la multiplicidad de cada raíz.

Ejemplo:

Hallamos las raíces racionales de :

$$f(x) = x^8 + \frac{3}{8}x^7 + \frac{1}{3}x^6 - \frac{14}{3}x^5 - \frac{14}{3}x^4 - \frac{4}{3}x^3 \in Q[x]$$

obteniendo el polinomio $g \in \mathbb{Z}[x]$

$$\begin{aligned} g(x) &= 3x^8 + 8x^7 + x^6 - 14x^5 - 14x^4 - 4x^3 = 3f(x) \\ &= x^3(3x^5 + 8x^4 + x^3 - 14x^2 - 14x - 4) \end{aligned}$$

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

$$h(x) = 3x^5 + 8x^4 + x^3.$$

Aquí $a_0 = -4$ y $a_n = 3$

$A = \{\pm 1, \pm 2, \pm 4\}$ y $B = \{\pm 1, \pm 3\}$, luego las raíces racionales se buscan en el conjunto:

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

Evaluando obtenemos $h(-1) = 0$ y $h\left(\frac{-2}{3}\right) = 0$.

Así, las raíces racionales distintas de $h(x)$ son -1 y $\frac{-2}{3}$, para conocer la multiplicidad de cada raíz encontrada, utilizaremos el método de la derivada.

$$h'(x) = 15x^4 + 32x^3 + 3x^2 - 28x - 14 \text{ y se tome}$$

$$h'(-1) = 0$$

Volviendo a derivar

$$h''(x) = 60x^3 + 96x^2 + 6x - 28$$

$$h''(-1) \neq 0$$

Se concluye que -1 es raíz doble de h .

Evaluando de la misma manera

$$h'\left(\frac{-2}{3}\right) \neq 0. \text{ Se tiene que } \frac{-2}{3} \text{ es raíz simple.}$$

Finalmente la factorización de $h(x)$ en $\mathbb{Q}[x]$ es:

$$h(x) = 3x^5 + 8x^4 + x^3 - 14x^2 - 14x - 4$$

$$\begin{array}{r|rrrrrr}
 & & 3 & 8 & 1 & -14 & -14 & -4 \\
 -1 & \downarrow & & & & & & \\
 \hline
 & & 3 & 5 & -4 & -10 & -4 & 0 \\
 -1 & \downarrow & & & & & & \\
 \hline
 & & 3 & 2 & -6 & -4 & 0 & \\
 -\frac{2}{3} & \downarrow & & & & & & \\
 \hline
 & & 3 & 0 & -6 & 0 & &
 \end{array}$$

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

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

Dado:

$$g(x) = 3 f(x)$$

$$\frac{1}{3} g(x) = f(x)$$

Luego la factorización de $f(x) \in \mathbb{Q}[x]$

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

\therefore 0 es raíz de multiplicidad 3
 -1 es raíz de multiplicidad 2
 $\frac{-2}{3}$ es raíz simple

$f(x)$ tiene 6 raíces racionales de sus 8 raíces

Observación: El Lema de Gauss nos provee un algoritmo para calcular las raíces racionales de un polinomio en $\mathbb{Q}[x]$, pero se ve claramente que éste es bastante laborioso, pues hay que evaluar el polinomio de entrada en un gran número de fracciones $\frac{a}{b}$, como en el ejemplo dado se tiene que hacer 12 evaluaciones en el polinomio $f(x)$, es decir la cantidad de fracciones está relacionada con la cantidad de divisores de a_0 y a_n .

4.1.3. Irreducibilidad en $\mathbb{Q}[x]$

El objetivo ahora es dar un criterio que permite probar la irreducibilidad de ciertos polinomios en $\mathbb{Q}[x]$ y mostrar que existen polinomios irreducibles de cualquier grado. Para ello necesitamos relacionar factorizaciones en $\mathbb{Q}[x]$ con factorizaciones en $\mathbb{Z}[x]$, puesto que $f \in \mathbb{Q}[x]$ es reducible si y solo si Cf es reducible para todo $c \in \mathbb{Q}/\{0\}$

Definición: Sea $f(x) = a_n x^n + \dots + a_0 \in \mathbb{Z}[x]$ un polinomio no nulo. Se define el "contenido de f " como el máximo común divisor de los coeficientes de f , es decir el contenido de f es el número entero.

$$\text{Cont}(f) = \text{mcd}(a_n, \dots, a_0)$$

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

Observación: Por la definición anterior, resulta que si

$f \in \mathbb{Z}[x]$ y $c \in \mathbb{Z}/\{0\}$, entonces

$\text{cont}(cf) = c \text{ cont}(f)$ y además

$f = \text{cont}(f)\bar{f}$ donde $\bar{f} \in \mathbb{Z}[x]$

es un polinomio primitivo.

4.1.4. Lema dos de Gauss

Sean $f, g \in \mathbb{Z}[x]$, entonces

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

Demostración:

1. Sea f y g primitivos tal que

$$f(x) = a_n x^n + \dots + a_0 \text{ y } g = b_n x^n + \dots + b_0$$

investiguemos si existe algún primo p que pueda dividir a $\text{cont}(fg)$.

Al ser f y g primitivos, $p \nmid \text{cont}(f)$ y

$p \nmid \text{cont}(g)$ entonces, existe a_i y b_j no

divisibles por el primo p . sean

$i_0 = \min \{i / p \nmid a_i\}$ y $j_0 = \min \{j / p \nmid b_j\}$, el

coeficiente $c_{i_0+j_0}$ del producto fg :

$$c_{i_0+j_0} = a_{i_0+j_0}b_0 + \dots + a_{i_0+1}b_{j_0-1} + a_{i_0}b_{j_0} + a_{i_0+1}b_{j_0+1} + \dots + a_0b_{i_0+j_0}$$

Por la definición de i_0 y j_0 , se observa que

$p \mid a_0, \dots, p \mid a_{i_0-1}$ y $p \mid b_0, \dots, p \mid b_{j_0-1}$ es decir p divide a todos los términos de la derecha de la igualdad, salvo eventualmente $a_{i_0}b_{j_0}$. Además

$p \nmid a_{i_0}$ y $p \nmid b_{j_0}$, por lo tanto, dado que p es

primo, $p \nmid a_{i_0}b_{j_0}$. En definitiva $p \nmid c_{i_0+j_0}$, o sea

$p \nmid \text{cont}(fg)$, en consecuencia $\text{cont}(fg) = 1$.

Por lo tanto fg es primitivo.

2. Como $f = \text{cont}(f) \cdot \bar{f}$ y

$$g = \text{cont}(g) \cdot \bar{g}$$

Donde $\bar{f}, \bar{g} \in \mathbb{Z}[x]$ son primitivos tenemos que

$$fg = \text{cont}(f) \text{cont}(g) \bar{f} \cdot \bar{g}$$

$$\Rightarrow \text{cont}(fg) = \text{cont}(\text{cont}(f) \text{cont}(g) \bar{f} \cdot \bar{g})$$

$$= \text{cont}(f) \text{cont}(g) \text{cont}(\bar{f} \cdot \bar{g})$$

$$\therefore \text{de (1) } \text{con}(f \cdot g) = \text{cont}(f) \cdot \text{con}(g)$$

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

1. $f = \tilde{g} \cdot \tilde{h}$
2. $\partial \tilde{g} = \partial g$ y $\partial \tilde{h} = \partial h$

Demostración: supongamos que f es primitivo, sean

$b, c \in \mathbb{Z} \setminus \{0\}$ tales que bg y $ch \in \mathbb{Z}[x]$, entonces :

$$\begin{aligned} b \cdot c \cdot f &= bc \cdot gh = (bg) \cdot (ch) \\ \Rightarrow \text{cont}(bc) &= \text{cont}(bcf) = \text{cont}((bg)(ch)) \\ &= \text{Cont}(bg) \cdot \text{cont}(ch) \end{aligned}$$

Por los datos anteriores

$$\begin{aligned} \text{Cont}(bg) &\neq b \cdot \text{cont}(g) \quad \text{y} \\ \text{Cont}(ch) &\neq c \cdot \text{cont}(h) \end{aligned}$$

Puesto $g, h \in \mathbb{Q}[x]$ Luego: $bg = \text{cont}(bg) \cdot \overline{bg}$ y $ch = \text{cont}(ch) \cdot \overline{ch}$

Con $\overline{bg}, \overline{ch} \in \mathbb{Z}[x]$ primitivos, se tiene que $f = \overline{bg} \cdot \overline{ch}$ y por lo tanto alcanza con definir:

$$\tilde{g} = \overline{bg} \quad \text{y} \quad \tilde{h} = \overline{ch}$$

Entonces: $f = \tilde{g} \tilde{h}$ y $\partial \tilde{g} = \partial g$, $\partial \tilde{h} = \partial h$

4.1.5. Criterio de Eisenstein

Sea $f \in \mathbb{Z}[x]$, $f = a_n x^n + \dots + a_0$ tal que existe un primo p que verifica $p \nmid a_n$, $p \mid a_i$ para $0 \leq i \leq n-1$ y $p^2 \nmid a_0$, entonces f es irreducible en $\mathbb{Q}[x]$.

Demostración: supongamos que f es reducible en $\mathbb{Q}[x]$, es decir que existen $g, h \in \mathbb{Q}[x]$ tal que $f = gh$ y $1 \leq \partial g < \partial f$. por el teorema anterior podemos suponer que $g, h \in \mathbb{Z}[x]$.

Supongamos que:

$$g = b_d x^d + \dots + b_0 \quad \text{y}$$

$$h = c_e x^e + \dots + c_0$$

donde $1 \leq d, e < n$

dado que $f = gh$, las hipótesis implican que $p \mid c_0 b_0$

pero $p^2 \nmid b_0 c_0$, entonces suponiendo que $p \mid b_0$ y $p \nmid c_0$

además suponiendo que $p \mid b_0, p \mid b_1, \dots, p \mid b_i$ y

veamos que entonces $p \mid b_i$ para $1 \leq i \leq \partial g - 1$ de la igualdad $f = g$ implican que

$$a_{i+1} = b_0 c_{i+1} + \dots + b_i c_1 + b_{i+1} c_0$$

Por hipótesis inductiva, p divide a todos los primeros factores de la derecha de la igualdad, y por otro lado dado que $i + 1 \leq \partial g < \partial f$, se tiene por la hipótesis del teorema que $p \nmid a_{i+1}$. Por lo tanto $p \mid b_{i+1} c_0$. Pero $p \nmid c_0$, en consecuencia $p \mid b_{i+1}$. Así, $p \mid \text{cont}(g)$ y por lo tanto $p \mid \text{cont}(g) \text{ cont}(h) = \text{cont}(gh) = \text{cont}(f)$. lo que contradice el hecho que $p \nmid a_n$, puesto que f es reducible.

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

Consecuencia: existen polinomios irreducibles de cualquier grado en $\mathbb{Q}[x]$. Por ejemplo el polinomio $x^n - 2$ es irreducible en $\mathbb{Q}[x] \quad \forall n \in \mathbb{N}$.

4.2 Polinomios con coeficientes en \mathbb{R}

Si $f \in \mathbb{R}[x]$ se tiene:

1. Sea $f \in \mathbb{R}[x]$ y $\partial f \geq 1$ tiene a lo sumo n raíces contados con multiplicidad.
2. Sea $f \in \mathbb{R}[x]$ de grado ≥ 2 . Si f tiene una raíz, entonces f es reducible.
3. Si $f \in \mathbb{R}[x]$ es reducible no implica que f tenga raíces en \mathbb{R} . Por ejemplo el polinomio x^2+1 es reducible y sin raíces reales
4. $f \in \mathbb{R}[x]$ de grado 2 ó 3 es reducible si y solo si tiene una raíz en \mathbb{R} . Además en $\mathbb{R}[x]$ no existen polinomios irreducibles de cualquier grado.

4.2.1. Raíces de un polinomio de grado impar

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

Demostración: sea $f = a_n x^n + \dots + a_0 \in \mathbb{R}[x]$, con n impar

Si $a_n > 0$, entonces

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

Y si $a_n < 0$, entonces

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

En ambos casos los signos son opuestos, y por lo tanto, por el teorema de Bolzano debe existir $\alpha \in \mathbb{R}$ tal que

$$f(\alpha) = 0.$$

Analicemos ahora y seamos más explícitos y precisar mejor cuantas raíces reales puede tener f

4.2.2. Raíces complejas y conjugadas

Teorema: sea $f \in \mathbb{R}[x]$ y sea $z \in \mathbb{C} \setminus \mathbb{R}$ un número complejo no real. Entonces

1. $f(z) = 0 \leftrightarrow f(\bar{z}) = 0$
2. z es raíz de multiplicidad k de $f \Leftrightarrow \bar{z}$ es raíz de multiplicidad k de f .
3. z raíz de multiplicidad k de $f \Leftrightarrow f(z) = f'(z) = \dots = f^{(k-1)}(z) = 0$ y $f^{(k)}(z) \neq 0$.

Pero $f', \dots, f^{(k-1)}, f^{(k)}$.También son polinomios en $\mathbb{R}[x]$ y por lo tanto, por (1):

$$\begin{aligned} f(z) = \dots = f^{(k-1)}(z) = 0 \text{ y } f^{(k)}(z) &\neq 0 \\ \Leftrightarrow f(\bar{z}) = \dots = f^{(k-1)}(\bar{z}) = 0 \text{ y } f^{(k)}(\bar{z}) &\neq 0 \\ \Leftrightarrow \bar{z} \text{ raíz de multiplicidad } k \text{ de } f \end{aligned}$$

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

Observación: sean z, \bar{z} números complejos conjugados, entonces el polinomio $(x - z)(x - \bar{z})$ es un polinomio real puesto que

$$(x - z)(x - \bar{z}) = x^2 - 2\operatorname{Re}(z)x + |z|^2 \in \mathbb{R}[x].$$

Observación: los siguientes enunciados son evidentes y conocidos.

1. Los polinomios irreducibles en $\mathbb{R}[x]$ son exactamente los de grado 1 y aquéllos de grado 2 con discriminante negativo.

2. La factorización en irreducible de un polinomio $f \in \mathbb{R}[x]$ es de la forma:

$$f = c (x - \alpha_1)^{k_1} \dots (x - \alpha_r)^{k_r} (x^2 - \beta_1 x + \gamma_1)^{j_1} \dots (x^2 - \beta_5 x + \gamma_5^1)^{j_5}$$

Con $1 \leq i \leq r$, $1 \leq \ell \leq 5$ y $B_\ell^2 - 4 \varphi_\ell < 0$.

4.2.3. Cantidad de raíces reales de un polinomio real

Sabemos que $f \in \mathbb{R}[x]$ de grado $n \geq 1$ tiene exactamente n raíces complejas (contadas con multiplicidad). Además sabemos que si $\partial f \geq 5$, no existe una fórmula general para describir las raíces.

Entonces nos preguntamos ¿Cuántas de estas raíces serán reales? No existe para raíces reales un criterio como el Lema de Gauss para raíces racionales.

Pero sin embargo existe un algoritmo que permite contar con exactitud la cantidad de raíces reales del polinomio f en un intervalo, esto es el Teorema de Sturm (1836).

Además existe un criterio que permite acotar la cantidad de raíces reales de $f \in \mathbb{R}[x]$, es el criterio de Descartes (1596 - 1650).

Empecemos el último tramo de este proyecto.

Notación: sea $f = a_n x^n + \dots + a_0 \in \mathbb{R}[x]$

- $Z_+(f)$: cantidad de raíces reales estrictamente positivos de f (contadas con multiplicidad)
- $Z_-(f)$: cantidad de raíces reales estrictamente negativos de f (contadas con multiplicidad)
- $V(f) : V(a_n, \dots, a_0)$: número de cambios de signo en la sucesión ordenado a_n, \dots, a_0 , saltando los ceros.

Ejemplo:

a) si $f = 3x^6 + 2x^5 - x^3 + x^2 - 7$

Entonces:

$$V(f) = x(3, 2, 0, -1, 1, 0, -7) = 3$$

b) si $g = 3x^4 + x^2 + 2$

Entonces:

$$V(g) = (3, 0, 1, 0, 2) = 0$$

c) si $h = x^3 - x^2 + x - 1$

Entonces:

$$V(h) = (1, -1, 1, -1) = 3$$

4.2.4. Regla de signos de Descartes

Sea $f = a_n x^n + \dots + a_0 \in \mathbb{R}[x]$, entonces:

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

Observación: Descartes anuncio esta regla, pero fue probado con total generalidad por Gauss.

Demostración:

El inciso (1), se basa en el "teorema de Rolle".

Sea $f: \mathbb{R} \rightarrow \mathbb{R}$ continua y derivable y $\alpha < \beta \in \mathbb{R}$ tales que $f(\alpha) = f(\beta) = 0$, entonces existe

$$\varphi, \alpha < \varphi < \beta \text{ tal que } f'(\varphi) = 0$$

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

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

El inciso (4) se obtiene agregando la siguiente observación (que se puede probar por inducción en ∂f) siempre vale $V(f) + V(f(-x)) \leq n$. Luego si f tiene n raíces reales, que podemos suponer no nulas, la única posibilidad es que se cumplan las igualdades en (1) y (2).

Aplicaciones:

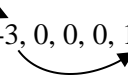
1. $f = x^n - 1$, tiene a lo sumo 1 raíz real positiva puesto que

$$V(f) = (1, 0, \dots, -1) = 1, \text{ pero como}$$


$V(f) - Z_+(f)$ es par, luego tiene exactamente una raíz positiva y tiene raíz real negativa en función de si n es par o impar.

En conclusión si $f \in \mathbb{R}[x]$ tal que $V(f) = 1$, entonces, al ser $V(f) - Z_+(f)$ siempre par, tiene que $Z_+(f) = 1$.

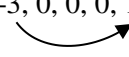
2. Sea $f = x^5 - 3x^4 + 1$

$$\text{Entonces: } V(f) = (1, -3, 0, 0, 0, 1) = 2$$


Como: $V(f) - Z_+(f)$ es par $\rightarrow Z_+(f) = 0$ ó $Z_+(f) = 2$

Pero como $f(0) = 1$ y $f(1) = -1$ por el teorema del valor de intermedio, f tiene una raíz en el intervalo $\langle 0, 1 \rangle$, entonces $Z_+(f) = 2$.

Además: $f(-x) = -x^5 - 3x^4 + 1$

$$V(f(-x)) = (-1, -3, 0, 0, 0, 1) = 1 \text{ y}$$


Como: $V(f(-x)) - Z_-(f)$ es par

Entonces: $Z_-(f) = 1$

Además se observa que f tiene entonces 2 raíces complejas no reales conjugadas.

4.2.5. Sucesión de Sturm

Pasaremos ahora al teorema de Sturm, que permite determinar exactamente el número de raíces reales de un polinomio real f en un intervalo $\langle a, b \rangle$. Para ello necesitaremos asociar al polinomio f en un polinomio

$\bar{f} = \frac{f}{\text{mcd}(f; f')}$ (\bar{f} : polinomio libre de cuadrados asociados a f), con las mismas raíces complejas que f , pero todas de multiplicidad 1.

Proposición: sea $f \in \mathbb{R}[x]$, $\partial f \geq 1$. Entonces $\bar{f} \in \mathbb{R}[x]$ tiene las mismas raíces complejas que f , pero todas de multiplicidad 1.

Demostración: sea: $f = c(x - \alpha_1)^{k_1} \dots (x - \alpha_m)^{k_m} \in \mathbb{C}[x]$
sabemos que si α_i es raíz de multiplicidad k_i de f , entonces es raíz de multiplicidad k_{i-1} de f' y por lo tanto
 $f' = (x - \alpha_1)^{k_{i-1}} \dots (x - \alpha_m)^{k_{m-1}} g(x)$, con $g(\alpha_i) \neq 0$.
Luego $\text{mcd}(f, f') = (x - \alpha_1)^{k_1-1} \dots (x - \alpha_m)^{k_m-1} \in \mathbb{R}[x]$
y $\bar{f} = \frac{f}{\text{mcd}(f; f')} = c(x - \alpha_1) \dots (x - \alpha_m) \in \mathbb{R}[x]$.

Definición: (sucesión de Sturm)

Sea $f \in \mathbb{R}[x]$ un polinomio sin raíces múltiples en \mathbb{C} .

Sean $a, b, \in \mathbb{R}$, $a < b$ tales que $f(a) \neq 0$ y $f(b) \neq 0$.

Se define la siguiente sucesión de polinomios:

1. $f_0 = f$
2. $f_1 = f'$
3. $\forall i \geq 1 \quad f_{i-1} = q_i f_i + r_i \quad \text{con } \partial r_i < \partial f_i \quad \text{y se define } f_{i+1} = -r_i$
4. Se termina cuando llega a f_s : constante.

Observación:

Dado que esta sucesión coincide salvo eventualmente signos con la sucesión de restos que se obtiene aplicando el algoritmo de Euclides para calcular el máximo común divisor a f y f' , la hipótesis que f no tenga raíces múltiples en \mathbb{C} garantiza que se llega siempre a f_s igual a una constante no nula.

4.2.6. Aplicación del teorema de Sturm

Notación:

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

Teorema (Sturm): sea $f \in \mathbb{R}[x]$ un polinomio sin raíces múltiples. Sea $a, b \in \mathbb{R}, a < b$ tales que $f(a) \neq 0$ y $f(b) \neq 0$. Entonces $Z_{\langle a, b \rangle}(f) = V(a) - V(b)$.

Realicemos el siguiente ejemplo:

Ejemplo: sea $f(x) = x^3 - 4x^2 + 4x - 7$
 $V(f) = (1, -4, 4, -7) = 3$
 $V(f) - z_+(f) = \text{par}$
 $\Rightarrow Z_+(f) = 1 \text{ ó } Z_+(f) = 3$

Además:

$$f(-x) = x^3 - 4x^2 + 4x - 7$$
$$V(f(-x)) = (-1, -4, -4, -7) = 0$$

Por otro lado: $f'(x) = 3x^2 + 8x + 4$

$$f'(x) = (3x - 2)(x - 2)$$

Se tiene que f' tiene exactamente 2 raíces reales positivas, pero esto no nos permite decidir si f tiene 1 ó 3 raíces reales.

Hallamos la sucesión de Sturm de f , aún sin saber si f no tiene raíces múltiples

$$f_0(x) = x^3 - 4x^2 + 4x - 7$$

$$f_1(x) = f'(x) = 3x^2 + 8x + 4$$

$$f_2(x) = \frac{8}{9}x + \frac{47}{9} ; \quad f_0(x) = \left(\frac{1}{3}x - \frac{4}{9}\right) f_1(x) - \frac{8}{9}x - \frac{47}{9}$$

$$f_3(x) = \frac{-9891}{64} ; \quad f_1(x) = \left(\frac{27}{8}x - \frac{1845}{64}\right) f_2(x) + \frac{9891}{64}$$

Como llegamos a que f_3 es una constante no nulo, se deduce de inmediato que f no tiene raíces múltiples en \mathbb{C} .

APLICANDO EL TEOREMA DE STURM:

1) sea por ejemplo $a = 0$ y $b = 1$, entonces:

$$V(a) = V(0) = V(f_0(0), f_1(0), f_2(0), f_3(0))$$

$$= V(-7, 4, \frac{47}{9}, \frac{-9891}{64}) = 2$$

$$V(b) = V(1) = V(-6, -1, \frac{55}{9}, \frac{-9891}{64}) = 2$$

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

2) sea $a = 3$ y $b = 4$, entonces :

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

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

Por lo tanto: $Z_{(3,4)}(f) = V(3) - V(4) = 1$, luego f tiene 1 raíz real en $\langle 3,4 \rangle$

3) también queremos averiguar la cantidad de raíces reales de f , como sabemos $M = 1 + 4 + 4 + 7 = 16$ es una cota superior para los módulos de las raíces de f , podríamos calcular $V(-16) - V(16)$ o $V(-N) - V(N)$; $\forall N \geq 16$, hemos usado la cota de Cauchy.

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

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

pues el coeficiente principal de f_i es positivo.
de la misma manera:

$$\begin{aligned} f_i(-N) > 0 &\Leftrightarrow \lim_{x \rightarrow +\infty} f_i(x) = +\infty \\ &\Leftrightarrow (-1)^{\deg f_i} \text{cp}(f_i) > 0 \end{aligned}$$

Así observamos que:

$$V(-N) = V(-\infty) = V(-\infty, +\infty, -\infty, \frac{-9891}{64}) = 2$$

$$V(N) = V(+\infty) = V(+\infty, +\infty, +\infty, \frac{-9891}{64}) = 1$$

De donde concluimos que:

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

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

Observación: sea $f \in \mathbb{R}[x]$ un polinomio sin raíces múltiples y sea f_0, f_1, \dots, f_s la sucesión de Sturm, entonces $Z(f) = V(-\infty) - V(+\infty)$ donde:

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

Ejemplo: sea el polinomio cuadrático

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

En efecto:

$$f \text{ tiene raíces simples} \Leftrightarrow \text{mcd}(f, f') = 1$$

donde :

$$f'(x) = 2x + b \text{ o sea,}$$

$$\text{mcd}(f, f') = 1 \Leftrightarrow f\left(\frac{-b}{2}\right) \neq 0 \Leftrightarrow \frac{b^2}{4} - \frac{b^2}{2} + c \neq 0$$

$$\Leftrightarrow b^2 - 4c \neq 0$$

Es decir, si $b^2 - 4c \neq 0$, f tiene raíces simples y podemos aplicar directamente el teorema de Sturm.

Mientras que si $b^2 - 4c = 0$

$\text{mcd}(f, f') = x + \frac{b}{2}$ y tenemos que trabajar con el cociente

$$\bar{f}(x) = x + \frac{b}{2}$$

1) caso $b^2 - 4c \neq 0$

$$f_0(x) = x^2 - bx + c$$

$$f_1(x) = 2x + b$$

$$f_2(x) = -c + \frac{b^2}{4} = \frac{b^2 - 4c}{4}$$

Luego:

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

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

Por lo tanto: si $b^2 - 4c > 0$

$$Z(f) = Z_{(-\infty, +\infty)}(f) = V(-\infty) - V(+\infty) = 2 - 0 = 2$$

Además: si $b^2 - 4c < 0$

$$Z(f) = Z_{(-\infty, +\infty)}(f) = V(-\infty) - V(+\infty) = 1 - 1 = 0$$

Es decir, para este caso no existe raíces reales

2) caso $b^2 - 4c = 0$

$$\bar{f}_0(x) = x + \frac{b}{2}$$

$$\bar{f}_1(x) = 1$$

Luego:

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

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

Entonces:

$$Z(\bar{f}) = 1 ; \text{ es decir } f \text{ tiene una raíz doble.}$$

CONCLUSIONES Y SUGERENCIAS

Conclusiones:

El estudio de polinomios como hemos visto constituye una teoría rigurosa, profunda y formal. Consecuentemente por sus diversas funciones el estudio de los polinomios es esencial, importante y trascendente ya que sus aplicaciones en diversas áreas como: Matemática, Ingeniería, Biología, Economía, Física entre otras son múltiples. Del presente trabajo de investigación se desprenden conclusiones relevantes.

- No tan solo se conoce el Teorema Fundamental del Álgebra, sino que se demuestra.
- Una de las interrogantes antes de desarrollar el presente trabajo fue ¿Por qué no existe una fórmula general para las ecuaciones de grado 5 a mas?, la respuesta a esta pregunta esta en el Teorema de Abel.
- Otra de las interrogantes fue ¿Todas las ecuaciones de grado 5 no se pueden resolver mediante radicales?, la respuesta es que si existen ecuaciones de grado 5 a mas que pueden resolverse mediante radicales, esto es por el Teorema de Galois.
- En la búsqueda de determinar la cantidad de raíces reales era posible, si lo es por la herramienta del Teorema de Sturm.

Sugerencias:

- De todos los resultados necesarios es preciso indicar que existe una fórmula general para las ecuaciones de grado 5, esta fórmula es usando Funciones Elípticas, el cual sería un gran trabajo futuro.
- Como lo hemos mencionado existen muchas demostraciones para el Teorema Fundamental del Álgebra, nosotros solo utilizamos una de las tantas demostraciones. Quedando así un trabajo que investigar.
- Teniendo en cuenta los resultados obtenidos en el estudio de polinomios, es recomendable hacer una investigación con polinomios reales, darle una visión grafica y utilizar métodos numéricos.

BIBLIOGRAFÍA

- [1] B.L. Van der Waerden. Modern Algebra, Frederick Ungar. Publishing co. NY (1953)
- [2] E. Gentile. Notas de Álgebra, Eudeba.
- [3] Herstein, I.N. Álgebra Moderna, Ginn 1964
- [4] Fraleigh, John B.A. First Course in Abstract Álgebra, Addison - Wesley 2002
- [5] Mutañian, Claude. Álgebra II, Compañía Editorial Continental, México, 1980
- [6] S. Lang. Álgebra, Addison - Wesley 1965