Facultad de Ciencias

La Conjetura de Casas-Alvero para un número fijo de raíces (The Casas-Alvero Conjecture for a fixed number of roots)

Trabajo de Fin de Máster
para acceder al

Master en Matemáticas y Computación

Autor: Yemile del Socorro Chávez Martínez

Directores: Laureano Gonzalez Vega

Luis Felipe Tabera Alonso

Junio - 2018

Resumen

Se hace en este trabajo un estudio de la Conjetura Casas-Alvero organizando su análisis con el tratamiento de los polinomios con un número fijo de raíces distintas. Se introducen tanto casos generales en donde esta conjetura se cumple como se descartan casos particulares en grado 20, primer caso donde no se conoce aún si la conjetura es cierta.

En el primer capítulo de este trabajo damos algunos resultados generales encontrados en [**4**], [**8**], [**6**] y [**3**]. En particular, se corrige el enunciado (y la demostración) de uno de los teoremas en [**6**].

En el segundo capítulo se demuestra que para todos los polinomios con coeficientes en un cuerpo de característica 0 con dos y tres raíces distintas, la conjetura es cierta. Para los polinomios con cuatro y cinco raíces distintas se introduce una nueva estrategia que permite, para grado fijo, el comprobar si la conjetura es cierta. Asimismo, y motivado por lo anterior, se introducen nuevas restricciones a los posibles contraejemplos de la conjetura mostrando que estos no pueden existir, por ejemplo, si las últimas derivadas, hasta cierto orden, tienen una misma raíz en común. Finalmente se demuestra que la Conjetura de Casas-Alvero es cierta para todos los polinomios de grado 20 con cuatro, cinco y seis raíces distintas, usando la estrategia antes mencionada y calculando las bases de Gröbner de las últimas k derivadas, donde k es el número de raíces diferentes del polinomio considerado. En resumen, de los 627 casos posibles en grado 20, se ha demostrado que, en 302 de ellos, la Conjetura de Casas-Alvero es cierta.

Viendo la imposibilidad de resolver este problema mediante este método, se utiliza la Geometría Tropical para estudiar un ejemplo concreto de polinomios en donde la conjetura es cierta para las definiciones clásicas, pero con las definiciones tropicales resulta falsa.

En el anexo se muestran los conceptos y resultados que se han usado a lo largo de la memoria: Teoría de la Eliminación, Bases de Gröbner y las Identidades de Newton.

Palabras clave:

Conjetura de Casas-Alvero, Polinomios, Raíces, Bases de Gröbner, Resultantes, Polinomios Tropicales.

Abstract

A study of the Casas-Alvero Conjecture is made in this work, organizing its analysis with the treatment of polynomials with a fixed number of different roots. We

introduce both general cases where this conjecture is true and we discard particular cases in degree 20, first case where it is not known yet if the conjecture is true.

In the first chapter of this paper we give some general results found in [**4**], [**8**], [**6**] and [**3**]. In particular, the statement (and proof) of one of the theorems in [**6**] is corrected.

The second chapter shows that for all polynomials with coefficients in a field of characteristic 0 with two and three different roots, the conjecture is true. For polynomials with four and five different roots, a new strategy is introduced that allows, for a fixed degree, to proof if the conjecture is true. Also, and motivated by the above, new restrictions are introduced to the possible counterexamples of the conjecture showing that these can not exist, for example, if the last derivatives, up to a certain order, have the same root in common. Finally, it is shown that the Casas-Alvero Conjecture is true for all 20 polynomials with four, five and six different roots, using the aforementioned strategy and calculating Gröbner's bases of the last k derivatives, where k is the number of different roots of the polynomial considered. In summary, of the 627 possible cases in grade 20, it has been demonstrated that, in 302 of them, the Casas-Alvero Conjecture is true.

Seeing the impossibility of solving this problem using this method, Tropical Geometry is used to study a concrete example of polynomials where the conjecture is true for classical definitions, but with tropical definitions it is false.

In the annexe the concepts and results that have been used throughout the memory are shown: Elimination Theory, Gröbner Basis and Newton's Identities.

Key words: Casas-Alvero Conjecture, Polynomials, Roots, Gröbner Bases, Resultants, Tropical Polynomials.

Índice general

Capítulo 1

Introducción

El presente trabajo busca hacer un estudio de la conjetura Casas-Alvero, dando algunos casos generales en donde ésta se cumple. Esta conjetura surge en [**2**] como resultado del estudio de curvas planas, dando, si resultara cierta, un criterio de irreducibilidad para las curvas planas definidas cerca del origen por una serie de potencias convergentes en dos variables.

Conjetura. *Sea K un cuerpo de característica 0, $f(x)$ un polinómio en $K[x]$, mónico y de grado $d > 0$. Si para cada $j = 1, ..., d-1$ $f^{(j)}(x)$ denota la derivada j-ésima de $f(x)$ y existe $a_j \in K$ tal que $f(a_j) = f^{(j)}(a_j) = 0$ entonces existe $\alpha \in K$ tal que $f(x) = (x - \alpha)^d$.*

A pesar de que el planteamiento solo utiliza nociones matemáticas elementales, es un problema abierto, incluso bajo las restricciones de que $f \in \mathbb{R}[x]$ y todas sus raíces sean reales. Es fácil ver que si $f(x) = (x - \alpha)^d$ es un polinomio en $K[x]$ de grado d entonces $f(\alpha) = f^{(j)}(\alpha) = 0$ para cada $j = 1, ..., d-1$. Sin embargo, demostrar el recíproco es donde se encuentra la dificultad de este problema.

El propósito general de este trabajo es analizar la Conjetura de Casas-Alvero y la búsqueda de su resolución mediante una orientación diferente a la usual, sabiendo que, en general, se analiza a través del grado de los polinomios y no por el número de raíces diferentes que éstos tienen. En este trabajo nos centramos en demostrar que el conjunto de polinomios que cumplen con las condiciones de la conjetura pero tienen un número específico de raíces diferentes es vacío para los cuerpos de característica 0. Se explora también la conjetura en el caso de la Geometría Tropical para ver si es una vía factible para la resolución de la conjetura.

En el primer capítulo de este trabajo damos algunos resultados generales conocidos. En [**4**] se demuestra, mediante un estudio de casos por grados, que los posibles contraejemplos a la conjetura deberán tener a lo más grado $d > 7$. En [**8**] se demuestra que la conjetura se cumple para los polinomios de grados $2p^e$ y p^e para cualquier primo p, demostrando así, que la conjetura es cierta para un número infinito de grados, siendo los primeros posibles casos de contraejemplo los polinomios de grado $d = 12, 15$ y 20. Más tarde en [**6**] se reescribe la demostración y se agregan casos, donde la conjetura es cierta para los polinomios con grado $d'p^e$ con $d' \in \{1, 2, 3, 4\}$ y p un primo $p > d'$, $e \in \mathbb{Z}_{\geq 0}$, y $p \neq 7$ si $d' = 4$. Para este resultado, se reescribió la demostración en esta memoria para el caso $d' = 4$ siguiendo los comentarios de [**3**]. En este caso corregimos la demostración en [**6**] mostrando que si $d' = 4$ y $p \geq 11$ entonces la conjetura es cierta. Por último, en [**3**], desde un enfoque geométrico, se analizan los posibles polinomios que no cumplen la conjetura y sus raíces, demostrando que para todo polinomio con 4 o menos raíces distintas, la conjetura es cierta. En [**3**] también se demuestra que los polinomios de grado 12 cumplen con la conjetura: esta prueba se hizo mediante un estudio de casos y el computo de estos, por lo que los polinomios de grado 20 son los polinomios de menor grado donde podría haber algún posible contraejemplo a la conjetura.

En el segundo capítulo se busca cambiar el enfoque con el cual se ataca la conjetura en [**4**], [**6**] y [**3**]. Durante el desarrollo de este trabajo se recurren a diversos tipos de análisis, pero siempre utilizando un polinomio genérico con un número fijo de raíces distintas y cada una de éstas con multiplicidad propia. Tras suponer que las últimas derivadas tienen alguna raíz en común con el polinomio se busca concluir que todas las raíces deben ser la misma. Desde este análisis se empieza a presentar la explosión combinatoria que implicaba un aumento de casos a analizar al aumentar el número de raíces distintas del polinomio, por lo que solo se logra resolver los casos de dos y tres raíces distintas con esta metodología para grado arbitrario.

Para los polinomios con cuatro raíces distintas se calcula la resultante de las últimas derivadas, en donde el análisis por multiplicidad de las raíces solo permite eliminar un caso en general, cuando las últimas tres derivadas comparten una misma raíz con el polinomio. Para el caso de polinomios con exactamente cinco raíces distintas se hace uso de las bases de Gröbner, que nos permiten eliminar otro caso general y simplificar el computo de las bases, cuando las últimas cuatro derivadas comparten una misma raíz con el polinomio. Un resultado general, para cualquier polinomio con $k+1$ raíces que comparte una misma raíz con sus últimas k derivadas, o bien, que tiene k raíces distintas distribuidas en las últimas k derivadas, se da al final de este capítulo.

Debido a la complejidad de los cálculos con grado arbitrario se estudia el caso concreto de los polinomios de grado 20, caso en el que se concluye que los polinomios con exactamente cuatro, cinco y seis raíces distintas cumplen con la conjetura. La demostración se hace mediante el cálculo de las bases de Gröbner de todos los posibles casos con estas características. Para los polinomios de grado 20 y 7 raíces distintas se muestra como, desde el punto de vista computacional se debería abordar.

Al encontrarnos con la explosión combinatoria que implica seguir con este análisis, y al eliminar casi la mitad de los casos para los polinomios de grado 20, se busca también atacar el problema con ayuda de la Geometría Tropical, por lo que se dan nociones tropicales tanto de los polinomios, como de las raíces comunes y lo que implica que estos polinomios cumplan con la conjetura. En este caso se da un ejemplo en donde la conjetura clásica es cierta pero bajo la noción tropical resulta falsa. Esto sucede debido a que la definición de polinomio tropical de Casas-Alvero tropical no es lo suficientemente fuerte.

Por último, en el anexo se dan conceptos teóricos claves, los cuales forman parte de la Teoría de la Eliminación (cuando se utiliza resultantes para encontrar raíces comunes en las últimas derivadas), de la Teoría de las Bases de Gröbner (cuando se busca la compatibilidad de diversos sistemas de ecuaciones algebraicas) y las identidades de Newton (para encontrar igualdades entre los coeficientes de las últimas derivadas cuando se conocen las raíces y sus multiplicidades).

Capítulo 2

La conjetura de Casas-Alvero

La conjetura de Casas-Alvero es un problema abierto, propuesto en 2001 ([**2**]), por Eduardo Casas-Alvero, que relaciona las raíces de un polinomio f con las de sus derivadas sucesivas. Si $f(x) \in K[x]$ entonces $f^{(j)}(x)$ denota su derivada j-ésima

Conjetura Casas-Alvero. *Sea $f(x) \in K[x]$ un polinomio mónico de grado $d > 0$ con K un cuerpo de característica 0, tal que para cada $j = 1, ..., d-1$ existe $a_j \in K$ con $f(a_j) = f^{(j)}(a_j) = 0$. Entonces existe $\alpha \in K$ tal que $f(x) = (x-\alpha)^d$.*

La hipótesis de que K es un cuerpo de característica 0 es necesaria ya que, como se verá en el siguiente ejemplo, existen cuerpos de característica positiva donde la conjetura es falsa. Además se puede demostrar que si la conjetura es cierta para $\mathbb{C}$ entonces es cierta para todo cuerpo de característica 0, por lo que, a lo largo de este trabajo, la mayoría de los resultados se darán sobre el cuerpo $\mathbb{C}$.

Ejemplo 1. Sea $f(x) = x(x-3)(x-4)^2 \in \mathbb{Z}_5$. Entonces,

$$\begin{aligned} f(x) =& x^4 - 11x^3 + 40x^2 - 48x \equiv x^4 + 4x^3 + 2x \mod 5 \\ f^{(1)}(x) =& 4x^3 - 33x^2 + 80x - 48 \equiv 4x^3 + 2x^2 + 2 \mod 5 \\ f^{(2)}(x) =& 12x^2 - 66x + 80 \equiv 2x^2 + 4x \mod 5 \\ f^{(3)}(x) =& 24x - 66 \equiv 4x + 4 \mod 5 \end{aligned}$$

Ya que $f^{(1)}(4) \equiv f^{(2)}(0) \equiv f^{(3)}(4) \equiv 0 \mod 5$, f tiene una raíz en común con $f^{(j)}(x)$ para cada $j = 1, 2, 3$. Por ello, $\mathbb{Z}_5$ es un cuerpo de característica 5 donde la conjetura no se cumple.

Definamos los polinomios que no cumplen la conjetura como sigue.

Definición 2. Sea K un cuerpo de característica 0. Se dice que un polinomio $f \in K[x]$ mónico de grado $d > 0$ es un *polinomio de Casas-Alvero* o CA sobre K si f no es una potencia de un polinomio lineal y si para cada $j = 1, ..., d-1$ existe un $a_j \in K$ tal que $f(a_j) = f^{(j)}(a_j) = 0$.

Como se menciona en el Teorema 43 en el Apéndice A, si K es algebraicamente cerrado, f y $f^{(j)}$ tienen ceros en común si, y solo si,

$$Res(f, f^{(j)}) = 0.$$

Considerando un subconjunto $F \subset K[x_1, \ldots, x_d]$ definamos

$$Zer(F, K^k) = \{x \in K^k |\ f(x) = 0\ \forall f \in F\}.$$

Si representamos un polinomio

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

por su vector de coeficientes

$$(a_0, a_1, a_{d-1}),$$

podemos expresar la conjetura como:

Conjetura Casas-Alvero.

$$Zer(\{Res(f, f^{(j)})|\ j = 1, \ldots, d-1\}, K^d) = \{(x-\alpha)^d : \alpha \in K\} = \{(\alpha^d, d\alpha^{d-1}, \ldots, d\alpha)\}$$

Los siguientes resultados sobre los polinomio de Casas-Alvero son importantes para el desarrollo de este trabajo y haremos uso de ellos en distintas ocasiones.

Empezamos con unos resultados, relacionados con la geometría de las raíces de estos polinomios, que pueden encontrarse en [**3**].

Lema 3. Sea f un polinomio de Casas-Alvero sobre K de grado $d > 0$, $\alpha_1, \alpha_2 \in \mathbb{C}^*$ y $\beta \in \mathbb{C}$. Entonces $g(x) = \alpha_1 f(\alpha_2 x + \beta)$ también es un polinomio de Casas-Alvero.

Este resultado lo utilizaremos principalmente para trasladar dos raíces distintas de un polinomio a los enteros 0 y 1.

Teorema 4 (Gauss-Lucas)**.** *Sea $f \in \mathbb{C}[x]$ un polinomio de grado $d > 0$. Entonces las raíces de su derivada f' se encuentran dentro de la envolvente convexa en $\mathbb{C}$ que forman las raíces de f. Si α es raíz de f' entonces α, o es una raíz de f de multiplicidad al menos 2, o se encuentra en el interior de la envolvente convexa de las raíces de f.*

A esta envolvente convexa se le conoce también como la envolvente convexa de *Gauss-Lucas*.

Proposición 5. *Sea $f \in \mathbb{C}[x]$ un polinomio de grado d cuyas raíces se encuentran todas sobre una línea, es decir la envolvente de Gauss-Lucas es un segmento. Entonces, para todo $j = 0, ..., d-2$, se tiene:*

$$f^{(j)}(c) \neq 0,\ f^{(j+1)}(c) = 0 \Rightarrow f^{(j+2)}(c) \neq 0.$$

Por lo tanto, si un polinomio tiene todas sus raíces reales, a partir de cierta derivada, las raíces de las siguientes derivadas serán siempre raíces simples.

Proposición 6. *Sea $f \in \mathbb{C}[x]$ un polinomio de Casas-Alvero. Entonces f tiene al menos dos raíces distintas en el interior de la envolvente convexa de Gauss-Lucas. En particular f tiene al menos cuatro raíces.*

Los casos más exitosos se basan en demostrar la conjetura en un cuerpo de característica p, donde hemos visto que la conjetura es falsa para estos casos en general. Se pueden refinar los resultados (aunque la conjetura siga siendo falsa) usando la derivada de Hasse en vez de la usual.

Definición 7. Sea

$$f = \sum_{i=0}^{d} a_i x^i$$

un polinomio de grado d. Se define la j-ésima *derivada de Hasse* de f, $H_j f$, como

$$H_j f = \sum_{i=j}^{d} \binom{i}{j} a_i x^{i-j}.$$

Para los cuerpos de característica 0, $H_j f = \frac{f^{(j)}}{j!}$, por lo que f tiene una raíz en común con $f^{(j)}$ si y solo si la tiene con $H_j f$.

Definición 8. Sea K cuerpo de característica positiva. Se dice que un polinomio $f \in K[x]$ de grado $d > 0$ es un polinomio Casas-Alvero si f no es potencia de un polinomio lineal y si para cada $j = 1, ..., d-1$ existe un $a_j \in K$ tal que $f(a_j) = H_j f(a_j) = 0$.

El resultado principal es la siguiente proposición, demostrada originalmente en [**8**] y de la que se da una demostración alternativa en [**6**].

Nosotros enunciamos el resultado de manera análoga a [**6**] con algunas modificaciones debido a que usamos definiciones ligeramente diferentes.

Proposición 9 (Reducción $mod - p$)**.** *Sea $d = d'p^e$ con p un primo, $p > d'$ y K un cuerpo de característica p. Si para todo polinomio de $K[x]$ de grado d' se cumple la conjetura de Casas-Alvero (con las derivadas de Hasse) entonces la conjetura se cumple también para los polinomios de grado d en $\mathbb{C}[x]$.*

Usando esta proposición, en [**8**] se demostraron los casos $d = p^e$ y $d = 2p^e$. En [**6**] estos casos se extendieron a los grados de la forma $3p^e$ y $4p^e$ con una cantidad finita de excepciones. En el artículo [**4**] los casos $d \leq 7$ fueron demostrados. De esta manera, en [**6**] se menciona que los primeros grados de polinomios donde la conjetura continua abierta son $d = 12, 24, 28$ y 30. De todas formas reescribimos la demostración en el caso $d' = 4$ siguiendo los comentarios de [**3**] y corrigiendo [**6**], ya que el teorema en esa referencia no cubriría el caso $d = 20$. El siguiente enunciado se encuentra en [**6**], y como se verá a continuación, no es correcto.

Teorema 10. *Sea $d = d'p^e$ con p un primo, $d' \in \{1, 2, 3, 4\}$, $p > d'$, $e \in \mathbb{Z}_{\geq 0}$. Además supongamos que $p \neq 7$, si $d' = 4$. Entonces la Conjetura se cumple para todos los polinomios de grado d.*

Demostración. Solo consideramos el caso donde $d' = 4$ para mostrar que este enunciado para este caso no es correcto.

Por la Proposición 9, para el caso $d' = 4$, debemos calcular los primos p para los cuales la conjetura es falsa en característica p y grado 4.

Sea h un polinomio de grado 4, el cual se supone es de Casas-Alvero, por lo que h tiene una raíz en común α con su derivada $h^{(3)}$, definimos $g(x) = h(x+\alpha)$, entonces g es de Casas-Alvero en $K[x]$ y debe ser de la forma $g = x^4 + ax^2 + bx$. Las resultantes de g con $H_1 g = 4x^3 + 2ax + b$ y con $H_2 g = 6x^2 + a$ son los determinantes de las matrices de Sylvester

$$\begin{vmatrix} 1 & 0 & a & b & 0 & 0 & 0 \\ 0 & 1 & 0 & a & b & 0 & 0 \\ 0 & 0 & 1 & 0 & a & b & 0 \\ 4 & 0 & 2a & b & 0 & 0 & 0 \\ 0 & 4 & 0 & 2a & b & 0 & 0 \\ 0 & 0 & 4 & 0 & 2a & b & 0 \\ 0 & 0 & 0 & 4 & 0 & 2a & b \end{vmatrix} \text{ y } \begin{vmatrix} 1 & 0 & a & b & 0 & 0 & 0 \\ 0 & 1 & 0 & a & b & 0 & 0 \\ 6 & 0 & a & 0 & 0 & 0 & 0 \\ 0 & 6 & 0 & a & 0 & 0 & 0 \\ 0 & 0 & 6 & 0 & a & 0 & 0 \\ 0 & 0 & 0 & 6 & 0 & a & 0 \end{vmatrix}.$$

Entonces, por ser g de Casas-Alvero,

$$-b^2(4a^3 + 27b^2) = 0 \text{ y } a(25a^3 + 216b^2) = 0,$$

respectivamente.

Buscamos ahora los primos para los cuales el anterior sistema de ecuaciones tiene una solución distinta de $a = b = 0$.

Tenemos varios casos, si $a = 0, b \neq 0$, entonces $27b^2 = 0$, es decir que $p = 3$, lo cual no está en las hipótesis de la Proposición 9, ya que $p > d'$.

De igual forma, si $a \neq 0 \neq b$, entonces $4a^3 + 27b^2 = 0 = 25a^3 + 216b^2$. Operando obtenemos que $a^3(4 \cdot 216 - 25 \cdot 27) = a^3 \cdot 189 = a^3(3^3 \cdot 7) = 0$, lo cual tampoco sucede ya que $p \neq 7$.

Es el caso $a \neq 0,\ b = 0$ el que no es considerado en la demostración de [**6**]. En este caso se tiene que $25a^4 = 0$, lo cual se cumplirá trivialmente con $p = 5$ y $p > d'$. Una sencilla comprobación de que la conjetura no se cumple para los polinomios de grado 4 en un cuerpo K de característica 5 es el Ejemplo 1. Entonces, para $p = 5$, no podemos asegurar que los polinomios de grado d la conjetura sea cierta. ♦

Por lo tanto, el enunciado correcto del Teorema 10 es el siguiente.

Teorema 11. *[Pequeños múltiplos de una potencia de primos] Sea $d = d'p^e$ con p un primo, $d' \in \{1, 2, 3, 4\}$, $p > d'$ y $e \in \mathbb{Z}_{\geq 0}$. Además supongamos que $p \geq 11$ si $d' = 4$. Entonces la Conjetura de Casas- Alvero se cumple para todos los polinomios de grado d.*

En [**3**] se descarta el caso de grado 12, el cual llevo cerca de 3 semanas de computo, usando la versión 2.18-2 de Magma, con Ubuntu 11.10 en un procesador 6-core Intel Xeon 2.53 GHz con 96 GB de memoria RAM.

Entonces, 20, 24, 28, 30, 35 y 36 son los primeros grados donde la conjetura continúa abierta. Se analizará el caso de los polinomios de grado 20 en la Sección 3.5 del Capítulo 3.

Capítulo 3

La Conjetura de Casas-Alvero para polinomios con un número fijo de raíces

En este capítulo se demuestran algunos casos particulares de la conjetura de Casas-Alvero. Más concretamente, fijamos el número de raíces distintas que puede tener un polinomio en lugar de fijar el grado de éste.

Sabiendo que un polinomio de Casas-Alvero debería tener al menos cuatro raíces (Proposición 6), en [**3**], se demuestra lo siguiente.

Teorema 12. *Sea f un polinomio de Casas-Alvero sobre $\mathbb{C}$, entonces f tiene al menos 5 raíces distintas*

Buscamos dar una demostración alternativa a la presentada en [**3**], en donde en lugar de analizar resultados geométricos de las raíces de un polinomio de Casas-Alvero, se fija el número de éstas y se hacen cálculos explícitos.

3.1. Polinomios con dos y tres raíces

Teorema 13. *Sea $f \in \mathbb{C}[x]$ de grado d un polinomio con exactamente dos raíces diferentes. Entonces f no es un polinomio de Casas-Alvero.*

Demostración. Sea $f(x)$ un polinomio de grado $d = m + n$ con exactamente dos raíces distintas α y β. f es de la forma

$$f(x) = (x - \alpha)^m (x - \beta)^n$$

con $n, m \in \mathbb{Z}_{>0}$.

Entonces, usando los resultados de la Sección A.3 del Apéndice A

$$f^{(d-1)}(x) = (d-1)!(dx - n\alpha - m\beta).$$

Si f fuera un polinomio de Casas-Alvero entonces f y $f^{(d-1)}$ tendrían una raíz en común. Supongamos, sin pérdida de generalidad, que α es raíz de $f^{(d-1)}$, de donde

$$(d-1)!(d\alpha - n\beta - m\alpha) = (d-1)!n(\alpha - \beta) = 0,$$

lo que implica que $\alpha = \beta$.

♦

Vamos a analizar ahora el caso de un polinomio con tres raíces distintas y grado d. En este caso se requiere analizar las derivadas $f^{(d-1)}$ y $f^{(d-2)}$. A diferencia de los polinomios con dos raíces, este análisis involucra un estudio por casos y un análisis de los grados implicados.

Teorema 14. *Sea $f \in \mathbb{C}[x]$ un polinomio de grado d con exactamente tres raíces distintas. Entonces f no es un polinomio de Casas-Alvero.*

Demostración. Sea $f(x)$ un polinomio con tres raíces distintas y grado d,

$$f(x) = (x-\alpha)^m(x-\beta)^n(x-\gamma)^p,$$

donde $n, m, p \in \mathbb{Z}_{>0}$, $d = m+n+p$ y $\alpha \neq \beta,\ \alpha \neq \gamma$ y $\beta \neq \gamma$. Supongamos que $f(x)$ es un polinomio de Casas-Alvero.

En este caso, podemos suponer, sin pérdida de generalidad, que α es raíz de,

$$f^{(d-1)}(x) = (d-1)!(dx - m\alpha - n\beta - p\gamma).$$

Esto implica

$$\alpha = \frac{m\alpha + n\beta + p\gamma}{m+n+p} \Rightarrow \alpha = \frac{n\beta + p\gamma}{n+p}.$$

Por ser f de Casas-Alvero entonces $f^{(d-2)}(x)$ tiene también una raíz en común con $f(x)$. Debemos distinguir dos casos, según esta raíz sea α o distinta de α.

Como

$$\begin{aligned}\frac{f^{(d-2)}(x)}{(d-2)!} =& \frac{d(d-1)x^2}{2} - (d-1)(m\alpha + n\beta + p\gamma)x \\ &+ \frac{(m-1)m\alpha^2 + (n-1)n\beta^2 + (p-1)p\gamma^2 + 2(mn\alpha\beta + mp\alpha\gamma + mp\beta\gamma)}{2},\end{aligned}$$

si $f^{(d-1)}(\alpha) = 0$ entonces

$$\frac{-np(\beta-\gamma)^2(d-2)!}{2n+2p} = 0,$$

es decir, $\beta = \gamma$. Obsérvese que $d - 2 > 0$.

Si α no fuese raíz de $f^{(d-2)}(x)$, sin pérdida de generalidad, supongamos que lo es β. Sustituyendo

$$\alpha = \frac{n\beta + p\gamma}{n+p}$$

en $f^{(d-2)}(\beta)$ obtenemos:

$$\frac{p(\beta-\gamma)^2(m^2p + 2mnp + 2mp^2 + n^2p + 2np^2 + p^3 - mp - n^2 - 2np - p^2)}{2(n+p)^2} = 0.$$

Como

$$\begin{aligned} n^2p &\geq n^2 \\ 2np^2 &\geq 2np \\ 2nmp &> mp \\ p^3 &\geq p^2 \\ m^2p &> 0 \\ 2mp^2 &> 0 \end{aligned}$$

entonces

$$m^2p + 2mnp + 2mp^2 + n^2p + 2np^2 + p^3 - mp - n^2 - 2np - p^2 \neq 0,$$

lo que implica que $\beta = \gamma$.

Por lo tanto, todo polinomio con tres raíces distintas no es un polinomio de Casas-Alvero. ♦

3.2. Polinomios con cuatro raíces

Continuando el análisis de polinomios con un número fijo de raíces, para el caso de 4 raíces diferentes, haremos uso de las resultantes, que nos darán una condición para que las últimas tres derivadas tengan alguna raíz común con el polinomio considerado.

Teorema 15. *Sea $f \in \mathbb{C}[x]$ un polinomio de grado d con exactamente cuatro raíces distintas. Si*

$$f(\alpha) = f^{(d-1)}(\alpha) = f^{(d-2)}(\alpha) = f^{(d-3)}(\alpha) = 0$$

entonces f no es un polinomio de Casas-Alvero.

Demostración. Consideremos

$$f(x) = (x-\alpha)^m (x-\beta)^n (x-\gamma)^p (x-\delta)^q,$$

con $n, m, p, q \in \mathbb{Z}_{>0}$. En este caso el grado de f es $d = m + n + p + q$.

Como en casos anteriores, al ser $f^{(d-1)}(\alpha) = 0$, entonces

$$\alpha = \frac{m\alpha + n\beta + q\delta + p\gamma}{m+n+p+q} \Rightarrow \alpha = \frac{n\beta + p\gamma + q\delta}{n+p+q} \tag{1}$$

Al sustituir x por α y luego α por la expresión en (1) en $f^{(d-2)}(x)$ y $f^{(d-3)}(x)$, obtenemos dos polinomios en las variables β, γ y δ y en los parámetros m, n, p y q. Si calculamos la resultante de $f^{(d-2)}(\alpha)$ y $f^{(d-3)}(\alpha)$ respecto a β se obtiene

$$\frac{-4m^2p^2q^2(p+q)(m+q)(m+p)(\gamma-\delta)^6}{(m+p+q)^4} = 0$$

ya que tienen una raíz común β. Se concluye entonces que $\gamma = \delta$. ♦

Se deberían considerar ahora los casos:

$$f^{(d-1)}(\alpha) = f^{(d-2)}(\beta) = f^{(d-3)}(\alpha) = 0,$$
$$f^{(d-1)}(\alpha) = f^{(d-2)}(\alpha) = f^{(d-3)}(\beta) = 0,$$
$$f^{(d-1)}(\alpha) = f^{(d-2)}(\beta) = f^{(d-3)}(\beta) = 0,$$
$$f^{(d-1)}(\alpha) = f^{(d-2)}(\beta) = f^{(d-3)}(\gamma) = 0.$$

Si tratamos de hacer esto mismo para

$$f^{(d-1)}(\alpha) = f^{(d-2)}(\beta) = f^{(d-3)}(\alpha) = 0$$

obtendríamos una expresión de la forma

$$\frac{4p^2q^2(p+q)(\gamma-\delta)^6 S(m,n,p,q)}{(n+p+q)^6},$$

donde S es un polinomio en los parámetros m, n, p y q, de grado 9 y con 438 términos. Para este polinomio, deberíamos ver que no tiene raíces enteras positivas. No es este un caso tan sencillo como el anterior.

El resto de casos son similares por lo que esta aproximación no nos deja ir más lejos.

Gracias a la Proposición 6 se tiene que la envolvente convexa de f es un segmento, entonces la Proposición 5 nos dice que los únicos casos posibles para cuatro raíces son:

$$\begin{aligned} f^{(d-1)}(\alpha) = f^{(d-2)}(\beta) = f^{(d-3)}(\alpha) = 0, \\ f^{(d-1)}(\alpha) = f^{(d-2)}(\beta) = f^{(d-3)}(\gamma) = 0. \end{aligned} \tag{2}$$

Se fijará ahora el grado del polinomio a 20 (primer caso aún abierto) y en lugar de calcular la resultante de las últimas derivadas se calculará la base de Gröbner del ideal generado por éstas.

3.3. Polinomios con cinco raíces

Por los resultados vistos en el Capítulo 2, si f es un polinomio de Casas-Alvero con 5 raíces diferentes y grado d,

$$f = (x-\alpha)^m (x-\beta)^n (x-\gamma)^p (x-\delta)^q (x-\epsilon)^r$$

entonces, por la Proposición 6, existen dos casos: todas las raíces se encuentran en un segmento o tres de ellas forman un triángulo y las otras dos se encuentran en el interior de la envolvente convexa.

En cualquiera de los dos casos tendríamos que si m_f es la multiplicidad maximal de las raíces de f, $m_f \leq d-4$, entonces sabemos que, en la envolvente convexa de

Gauss-Lucas de $f^{(d-4)}$, ya no estarán las raíces que eran vértices de la envolvente convexa de f.

En el primer caso, por el Lema 3, podemos trasladar cualquier pareja de raíces al 0 y al 1, trasladando así el resto de las raíces también a la recta real, es decir, podemos considerar que f tiene todas sus raíces reales, y si α, β y γ son las raíces que se encuentran en el interior de la envolvente convexa de f y δ y ϵ son sus vértices, por la Proposición 5, tendríamos que los únicos casos posibles para las raíces de $f^{(j)}$, $d-4 \leq j \leq d-1$ son:

- $f^{(d-4)}(\alpha) = f^{(d-3)}(\beta) = f^{(d-2)}(\alpha) = f^{(d-1)}(\beta) = 0$.
- $f^{(d-4)}(\alpha) = f^{(d-3)}(\beta) = f^{(d-2)}(\alpha) = f^{(d-1)}(\gamma) = 0$
- $f^{(d-4)}(\alpha) = f^{(d-3)}(\beta) = f^{(d-2)}(\gamma) = f^{(d-1)}(\alpha) = 0$
- $f^{(d-4)}(\alpha) = f^{(d-3)}(\beta) = f^{(d-2)}(\gamma) = f^{(d-1)}(\beta) = 0$

En el segundo caso, si α y β son las raíces que se encuentran en el interior de la envolvente convexa de f y γ, δ y ϵ, los vértices, tendríamos que los únicos casos posibles para $f^{(j)}$, $d-4 \leq j \leq d-1$, son:

- Solo una raíz que aparecerá en las últimas 4 derivadas.
  - $f^{(d-4)}(\alpha) = f^{(d-3)}(\alpha) = f^{(d-2)}(\alpha) = f^{(d-1)}(\alpha) = 0$.
- Dos raíces, una que se presentará 3 veces y otra solamente una.
  - $f^{(d-4)}(\alpha) = f^{(d-3)}(\alpha) = f^{(d-2)}(\alpha) = f^{(d-1)}(\beta) = 0$.
  - $f^{(d-4)}(\alpha) = f^{(d-3)}(\alpha) = f^{(d-2)}(\beta) = f^{(d-1)}(\alpha) = 0$.
  - $f^{(d-4)}(\alpha) = f^{(d-3)}(\beta) = f^{(d-2)}(\alpha) = f^{(d-1)}(\alpha) = 0$.
  - $f^{(d-4)}(\beta) = f^{(d-3)}(\alpha) = f^{(d-2)}(\alpha) = f^{(d-1)}(\alpha) = 0$.
- Dos raíces, ambas presentes exactamente dos veces.
  - $f^{(d-4)}(\alpha) = f^{(d-3)}(\alpha) = f^{(d-2)}(\beta) = f^{(d-1)}(\beta) = 0$.
  - $f^{(d-4)}(\alpha) = f^{(d-3)}(\beta) = f^{(d-2)}(\beta) = f^{(d-1)}(\alpha) = 0$.
  - $f^{(d-4)}(\alpha) = f^{(d-3)}(\beta) = f^{(d-2)}(\alpha) = f^{(d-1)}(\beta) = 0$.

De todos estos casos, podemos probar el siguiente teorema.

Teorema 16. *Sea $f \in \mathbb{C}[x]$ un polinomio de grado d con exactamente cinco raíces distintas. Si*

$$f(\alpha) = f^{(d-1)}(\alpha) = f^{(d-2)}(\alpha) = f^{(d-3)}(\alpha) = f^{(d-4)}(\alpha) = 0,$$

entonces f no es un polinomio de Casas-Alvero.

Demostración. Sea $f = (x-\alpha)^m(x-\beta)^n(x-\gamma)^p(x-\delta)^q(x-\epsilon)^r$. Se calcula la base de Gröbner del ideal generado por

$$f^{(d-1)}(\alpha), f^{(d-2)}(\alpha), f^{(d-3)}(\alpha), f^{(d-4)}(\alpha),$$

respecto del orden $lex(m, n, p, q, r, \alpha, \beta, \gamma, \delta, \epsilon)$. Esta tiene 27 elementos y uno de ellos es precisamente

$$-r(\delta - \epsilon)(\beta - \epsilon)(\alpha - \epsilon)(\gamma - \epsilon).$$

♦

No fue posible calcular las Bases de Gröbner del resto de los casos las debido a su complejidad y al tiempo de computo que éstas precisan.

De igual forma que con los polinomios con cuatro raíces distintas se fijará el grado a 20 (primer caso aún abierto) y se continuará calculando las bases de Gröbner para cada uno de estos casos.

3.4. Resultados generales sobre la distribución de raíces en las últimas derivadas

Generalizamos algunos casos extremos de distribución de las raíces en las últimas k derivadas para los polinomios con exactamente $k+1$ raíces distintas. En particular generalizamos los Teoremas 15 y 16 a grado y número de raíces arbitrario, y cuando tenemos k y $k-1$ raíces distintas distribuidas en las últimas k derivadas. .

Teorema 17. *Sea $f \in \mathbb{C}[x]$ un polinomio de grado d con exactamente $k+1$ raíces distintas. Entonces, no puede ocurrir que*

$$f(\alpha) = f^{(d-1)}(\alpha) = f^{(d-2)}(\alpha) = \cdots = f^{(d-k)}(\alpha) = 0.$$

Demostración. Sea

$$f(x) = \prod_{i=1}^{k+1}(x - \alpha_i)^{p_i} = x^d + c_{d-1}x^{d-1} + \cdots + c_1 x + c_0,$$

$c_i = (-1)^{d-i}\sigma_{d-i}(\alpha_1, \ldots, \alpha_{k+1})$ donde σ_{d-i} es la función simétrica elemental de grado $d-i$ (véase la sección A.3).

Razonemos por reducción al absurdo. Suponemos, sin pérdida de generalidad, que $\alpha_{k+1} = 0$ y que es una raíz en común con las últimas derivadas,

$$f(0) = f^{(d-1)}(0) = f^{(d-2)}(0) = \cdots = f^{(d-k)}(0) = 0.$$

Entonces considerando la derivada de Hasse tenemos

$$H_{d-k}f = \binom{d}{d-k}x^k + \binom{d-1}{d-k}c_{d-1}x^{k-1} + \cdots + c_{d-k} = \binom{d}{d-k}x^k.$$

Por lo que $c_i = 0$ para $d-k \leq i \leq d-1$. Entonces $\sigma_i = 0$ para $1 \leq i \leq k$. Esto implica que las sumas de las potencias de las raíces (Sección A.3) son $\pi_i = 0$ para

$1 \leq i \leq k$, es decir,

$$\begin{array}{rcccl} \pi_1 & = & p_1\alpha_1 + \cdots + p_k\alpha_k + p_{k+1}\alpha_{k+1} & = & 0, \\ \pi_2 & = & p_1\alpha_1^2 + \cdots + p_k\alpha_k^2 + p_{k+1}\alpha_{k+1}^2 & = & 0, \\ & & \cdots & & \\ \pi_k & = & p_1\alpha_1^k + \cdots + p_k\alpha_k^k + p_{k+1}\alpha_{k+1}^k & = & 0. \end{array}$$

Como $\alpha_{k+1} = 0$ entonces:

$$\begin{pmatrix} \alpha_1 & \cdots & \alpha_k \\ \alpha_1^2 & \cdots & \alpha_k^2 \\ & \cdots & \\ \alpha_1^k & \cdots & \alpha_k^k \end{pmatrix} \cdot \begin{pmatrix} p_1 \\ \vdots \\ p_k \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Por lo que el de terminante de la matriz de la izquierda es

$$(\prod_{i=1}^{k} \alpha_i) \cdot \left(\prod_{i<j} (\alpha_i - \alpha_j) \right),$$

por lo que existen $i \neq j$ con $\alpha_i = \alpha_j$ o existe i con $\alpha_i = 0 = \alpha_{k+1}$, en contradicción con las hipótesis. ♦

Usando el siguiente lema, el otro caso extremo en donde k raíces se encuentran distribuidas en las últimas k derivadas.

Lema 18 ([**3**])**.** Sea $f \in \mathbb{C}[x]$ y α una raíz de f que sea vértice de la envolvente convexa de las raíces de f. Entonces si m es la multiplicidad de α en f, $f^{(k)}(\alpha) \neq 0$ para toda $k \geq m$.

Demostración. Sabemos, por ser m la multiplicidad de α, que α no es raíz de $f^{(m)}$. Sean C y C_m las envolventes convexas de las raíces de f y $f^{(m)}$ respectivamente. Sabemos por 4 que $C_m \subseteq C$, como α es vértice de C y no es raíz de $f^{(m)}$ entonces $\alpha \notin C_m$. Como las raíces de $f^{(k)}$ se encuentran en C_m para todo $k \geq m$, entonces α no puede ser raíz de $f^{(k)}$. ♦

Teorema 19. *Sea $f \in \mathbb{C}[x]$ un polinomio con exactamente $k+1$ raíces distintas, $\alpha_1, \alpha_2, \ldots, \alpha_{k+1}$ y de grado d. Entonces no puede ocurrir que*

$$f^{(d-1)}(\alpha_1) = f^{(d-2)}(\alpha_2) = \cdots = f^{(d-k)}(\alpha_k) = 0.$$

Demostración. Consideremos la envolvente convexa de las raíces de f. Entonces existen por lo menos α_i y α_j vértices de ésta. Sabemos que la máxima multiplicidad posible de una raíz de f es $d-k$, por el lema anterior, α_i y α_j no son raíces de $f^{(d-1)}, f^{(d-2)}, \ldots, f^{(d-k)}$. ♦

Por último, veamos que si el conjunto de raíces en común que tienen las últimas k derivadas con f es exactamente $k-1$, las raíces en éstas derivadas deberán ser simples.

Lema 20. Sea $f \in \mathbb{C}[x]$ un polinomio con exactamente $k+1$ raíces distintas de grado d. Sea

$$\mathcal{F} = \{\alpha |\ f(\alpha) = f^{(j)}(\alpha) = 0 \text{ para algún } d-k \leq j \leq d-1\}.$$

Si $|\mathcal{F}| = k-1$, entonces la componente convexa de f es un segmento.

Demostración. Supongamos que la envolvente convexa de f, C, no es un segmento. Entonces C tiene por lo menos tres vértices, sin pérdida de generalidad supongamos que α_1, α_2 y α_3 son tales. Consideremos m el máximo de las multiplicidades de α_1, α_2 y α_3 en f, sabemos que m es a lo más $d-k$. Como se vio en el Lema 18, $\alpha_1, \alpha_2, \alpha_3 \notin C_j$ con $d-k \leq j \leq d-1$ donde C_j es la componente convexa de $f^{(j)}$. Entonces

$$\alpha_1, \alpha_2, \alpha_3 \notin \mathcal{F}.$$

Por ello, $k-2 = |\mathcal{F}| \leq k-3$. Lo cual es una contradicción. ♦

Teorema 21. *Sea $f \in \mathbb{C}[x]$ un polinomio con exactamente $k+1$ raíces distintas de grado d. Si $|\mathcal{F}| = k-1$ entonces no puede ocurrir que*

$$f(\alpha) = f^{(j)}(\alpha) = f^{(j+1)}(\alpha) = 0$$

con $d-k \leq j \leq d-1$.

Demostración. Por el lema anterior, sabemos que la envolvente convexa de f es un segmento de linea. Entonces por la Proposición 5, si $f(\alpha) = f^{(j)}(\alpha) = 0$ entonces $f^{j+1}(\alpha) \neq 0$. ♦

3.5. Polinomios de grado 20

Estudiamos en esta sección el caso de grado 20, que es grado más bajo para el cual la conjetura permanece abierta.

Sea f un polinomio de grado 20. Entonces f es producto de 20 polinomios lineales y tendrá a lo sumo 20 raíces distintas. Considerando las diferentes particiones de multiplicidades que las raíces de f puedan tener debemos considerar 627 casos posibles para descartar la existencia de los polinomios de Casas-Alvero de este grado. De todos éstos, separándolos por el número de raíces distintas tendremos la Tabla 1

Es fácil ver que cuando f tiene todas sus raíces de multiplicidad 1 entonces f no puede ser de Casas-Alvero, ya que en particular f' no tendría ninguna raíz en común con f. Por lo tanto, de los 627 casos posibles tenemos ya resueltos 45: los que se corresponden con 1, 2, 3 y 20 raíces distintas.

Número de raíces	Casos	Número de raíces	Casos
1	1	11	30
2	10	12	22
3	33	13	15
4	64	14	11
5	84	15	7
6	90	16	5
7	82	17	3
8	70	18	2
9	54	19	1
10	42	20	1

TABLA 1. Distribución de multiplicidades para un polinomio de grado 20

Para el caso de 4, 5 y 6 raíces distintas se procede de la siguiente manera: se consideran todas las diferentes multiplicidades del producto de 20 polinomios lineales con 4, 5 y 6 raíces distintas respectivamente, de igual manera que en las Secciones 3.1, 3.2 y 3.3. Consideraremos solamente las $k-1$ últimas derivadas, donde k es el número de raíces distintas del polinomio, es decir, $k = 4, 5$ y 6.

Teorema 22. *Sea $f \in \mathbb{C}[x]$ un polinomio de grado 20 con exactamente cuatro, cinco o seis raíces diferentes. Entonces f no es un polinomio de Casas-Alvero*

A modo de demostración utilizaremos los siguientes ejemplos para ilustrar el método utilizado.

En todos los casos, se considera cada una de las posibles distribución de las raíces de f en sus últimas derivadas. Ya que en cada caso se fijan las raíces de estas derivadas, entonces se deben considerar también todas las posibles permutaciones de los arreglos de multiplicidades de sus raíces.

Es decir, para 4 raíces, en cada uno de los arreglos en (2, página 12) se evalúan las 64 posibles multiplicidades de las 4 raíces, junto con sus respectivas permutaciones, que nos darán la multiplicidad de cada raíz en f: 1 938casos en total. Teniendo cada uno de estos casos específicos se calcula la Base de Gröbner para los ideales generados por estas tres últimas derivadas evaluadas cada una en su respectiva raíz. Esta base resulta $\{1\}$ en todos los casos, es decir, ninguno de ellos es un polinomio de Casas-Alvero.

Ejemplo 23. Consideramos $f \in \mathbb{C}[x]$, de grado 20, con cuatro raíces distintas:

$$f(x) = (x-\alpha)^m (x-\beta)^n (x-\gamma)^p (x-\delta)^q.$$

Sea $(1,1,2,16)$ una de las particiones de 20 en 4 elementos. Entonces existen 12 permutaciones distintas de esta partición:

$$\begin{gathered}(1,1,2,16),(1,1,16,2),(1,2,1,16),(1,2,16,1)\\(1,16,1,2),(1,16,2,1),(2,1,1,16),(2,1,16,1),\\(2,16,1,1),(16,1,1,2),(16,1,2,1),(16,2,1,1).\end{gathered}$$

Si tomamos $(16,1,1,2)$ entonces $m=16,\ n=1,\ p=1$ y $q=2$. Si suponemos que

$$f^{(d-1)}(\alpha)=f^{(d-2)}(\beta)=f^{(d-3)}(\beta)=0,$$

por el Lema 3 podemos suponer que $\alpha=0$ y $\beta=1$ y podemos decir que

$$f^{(d-1)}(0)=f^{(d-2)}(1)=f^{(d-3)}(1)=0.$$

En este caso:

$$\begin{aligned}f(x)=&x^{16}(x-1)^1(x-\gamma)^1(x-\delta)^2,\\ \frac{f^{(19)}(x)}{19!}=&20x-2\delta-\gamma-1\\ \frac{f^{(18)}(x)}{18!}=&190x^2+(-19\gamma-19-38\delta)x+2\delta+\gamma+\delta^2+2\gamma\delta\\ \frac{f^{(17)}(x)}{17!}=&1140x^3+(-171\gamma-171-342\delta)x^2\\ &+(36\delta+18\gamma+18\delta^2+36\delta\gamma)x\\ &-\delta^2-2\gamma\delta-\gamma\delta^2\end{aligned}$$

La base de Gröbner del ideal generado por $f^{(17)}(x), f^{(18)}(x)$ y $f^{(19)}(x)$ respecto del orden $lex(\gamma,\delta)$ es $\{1\}$ y por ello se descarta la permutación $(16,1,1,2)$ para esa distribución de las raíces en las derivadas.

El computo de todas estas bases de Gröbner requirió 5.511 segundos.

Para 5 raíces, como vimos en la Sección 3.3, solo tenemos 10 posibles maneras en las que las raíces de f podrían ser también raíces de sus últimas 4 derivadas.

Para cada uno de estos arreglos de raíces se evalúan las 84 posibles multiplicidades de las 5 raíces, junto con sus respectivas permutaciones, que nos darán la multiplicidad de cada raíz en f: en total 38 760 casos. Una vez más, en cada uno de estos casos se calcula la Base de Gröbner del ideal generado por estas derivadas evaluadas en su respectiva raíz. La base resulta ser $\{1\}$ en todos los casos. El computo requirió 168.670 segundos.

Los siguientes ejemplos se muestran para hacer notar que, aunque los polinomios tengan un grado fijo (20 en este caso), al aumentar el número de raíces distintas, se produce una explosión combinatoria en el número de casos a considerar y el cálculo de cada caso se vuelve más costoso.

Ejemplo 24. Una de las particiones de 20 en 5 elementos es $(1, 2, 4, 4, 9)$. Esto supone $m = 1, n = 2, p = 4, q = 4$ y $r = 9$, es decir,

$$\begin{aligned}
f(x) =&(x-\alpha)(x-\beta)^2(x-\gamma)^4(x-\delta)^4(x-\epsilon)^9,\\
\frac{f^{(19)}(x)}{19!} =&-20x+2\beta+4\gamma+9\epsilon+\alpha+4\delta,\\
\frac{f^{(18)}(x)}{18!} =&190x^2-19(\alpha+2\beta+4\delta+9\epsilon+4\gamma)x+36\epsilon^2+9(\alpha+2\beta+4\delta+4\gamma)\epsilon\\
&+(2\beta+4\delta+4\gamma)\alpha+6\delta^2+4(2\beta+4\gamma)\delta+6\gamma^2+8\beta\gamma+\beta^2,\\
\frac{f^{(17)}(x)}{17!} =&1140x^3-171(\alpha+\beta+\delta+16\epsilon+\gamma)x^2\\
&+18(\alpha\beta+\alpha\delta+16\alpha\epsilon+\alpha\gamma+\beta\delta+16\beta\epsilon+\beta\gamma+16\delta\epsilon+\delta\gamma+120\epsilon^2+16\epsilon\gamma)x\\
&-560\epsilon^3-120(\alpha+\beta+\delta+\gamma)\epsilon^2-8((\beta+\delta+\gamma)2\alpha+(\beta+\gamma)2\delta+2\beta\gamma)\epsilon\\
&-\frac{((\beta+\gamma)2\delta+2\beta\gamma)\alpha}{2}-\beta\delta\gamma,
\end{aligned}$$

$$\begin{aligned}
\frac{f^{(16)}(x)}{16!} =&4845x^4-969(\alpha+\beta+\delta+16\epsilon+\gamma)x^3\\
&+\frac{306(\alpha\beta+\alpha\delta+\alpha\gamma+\beta\delta+\beta\gamma+\delta\gamma+120\epsilon^2+16(\delta\epsilon+\beta\epsilon+\epsilon\gamma+\alpha\epsilon))x^2}{2}\\
&-\frac{102}{6}(\alpha\beta\delta+16\alpha\beta\epsilon+\alpha\beta\gamma+16\alpha\delta\epsilon+\alpha\delta\gamma+120\alpha\epsilon^2+16\alpha\epsilon\gamma\\
&+16\beta\delta\epsilon+\beta\delta\gamma+120\beta\epsilon^2+16\beta\epsilon\gamma+120\delta\epsilon^2+16\delta\epsilon\gamma+560\epsilon^3+\epsilon^2\gamma)x\\
&+1820\epsilon^4+560(\alpha+\beta+\delta+\gamma)\epsilon^3+60((\beta+\delta+\gamma)2\alpha+(\beta+\gamma)2\delta+2\beta\gamma)\epsilon^2\\
&+\frac{(((\beta+\gamma)2\delta+2\beta\gamma)24\alpha+48\beta\delta\gamma)\epsilon}{3}+\beta\delta\gamma\alpha
\end{aligned}$$

Luego, si

$$f^{(19)}(\alpha) = f^{(18)}(\beta) = f^{(17)}(\alpha) = f^{(16)}(\beta) = 0,$$

por el lema 3, asumiendo que

$$f^{(19)}(0) = f^{(18)}(1) = f^{(17)}(0) = f^{(16)}(1) = 0,$$

es decir $\alpha = 0$ y $\beta = 1$, se calcula la base de Gröbner respecto del orden $lex(\gamma, \delta, \epsilon)$, la cual resulta ser $\{1\}$, descartando la permutación considerada.

Se procede de igual forma para 6 raíces, solo que en este caso, gracias a los resultados de la Sección 3.4 se consideran 50 formas en las que las últimas 5 derivadas tendrán raíces en común con f: con dos raíces (una presente 4 veces y otra solo una vez) 5 y (una presente tres y otra dos veces) 10, con tres raíces (una tres veces y las otras dos solo una vez) 10 y (dos presentes dos veces y la tercera solo una vez) 15, y cuatro raíces (una presente dos veces y las otras tres solamente una vez) 10. El caso en donde cinco raíces distintas están distribuidas en las últimas 5 derivadas no se toma en cuenta gracias al Teorema 19.

Se calculan las bases de Gröbner con las últimas 5 derivadas en cada uno de los 50 casos anteriores y en los 90 casos de multiplicidad de cada raíz con sus respectivas permutaciones: 581 400casos. Una vez más, todas las bases de Gröbner resultan ser igual a $\{1\}$, requiriendo un total de 10 125.138 segundos.

Ejemplo 25. Consideremos un polinomio de 6 raíces

$$f(x) = (x-r_1)^{p_1}(x-r_2)^{p_2}(x-r_3)^{p_3}(x-r_4)^{p_4}(x-r_5)^{p_5}(x-r_6)^{p_6}$$

y ahora consideremos una de las particiones de 20 en 6 elementos: $(1,1,2,3,3,10)$. Entonces $p_1 = 1,\ p_2 = 1,\ p_3 = 2,\ p_4 = 3,\ p_5 = 3$ y $p_6 = 10$, con

$$\begin{aligned}
f(x) =&(x-r_1)(x-r_2)(x-r_3)^2(x-r_4)^3(x-r_5)^3(x-r_6)^{10}\\
\frac{f^{(19)}(x)}{19!} =&20x - r_2 - 2r_3 - 3r_4 - 3r_5 - 10r_6 - r_1\\
\frac{f^{(18)}(x)}{18!} =&(x-r_3)^2 + 3(x-r_4)^2 + 3(x-r_5)^2 + 45(x-r_6)^2 + (x-r_1)(x-r_2)\\
&+30(x-r_4)(x-r_6) + 9(x-r_4)(x-r_5)\\
&+3(x-r_2)(x-r_5) + 3(x-r_2)(x-r_4) + 3(x-r_1)(x-r_5)\\
&+3(x-r_1)(x-r_4) + 6(x-r_3)(x-r_4) + 10(x-r_1)(x-r_6)\\
&+2(x-r_2)(x-r_3) + 2(x-r_1)(x-r_3) + 30(x-r_5)(x-r_6)\\
&+20(x-r_3)(x-r_6) + 6(x-r_3)(x-r_5) + 10(x-r_2)(x-r_6)
\end{aligned}$$

$f^{(17)}(x)$ es un polinomio de grado 3 y 43 términos

$$\begin{aligned}
\frac{f^{(17)}(x)}{17!} =& (x-r_4)^3 + (x-r_5)^3 + 120(x-r_6)^3 + 30(x-r_4)^2(x-r_6)\\
&+30(x-r_5)^2(x-r_6) + 10(x-r_3)^2(x-r_6) + 9(x-r_4)^2(x-r_5)\\
&+45(x-r_1)(x-r_6)^2 + 45(x-r_2)(x-r_6)^2 + 9(x-r_4)(x-r_5)^2\\
&\quad\vdots\\
&+30(x-r_2)(x-r_4)(x-r_6) + 3(x-r_1)(x-r_2)(x-r_5)\\
&+3(x-r_1)(x-r_2)(x-r_4) + 6(x-r_2)(x-r_3)(x-r_5)\\
&+6(x-r_1)(x-r_3)(x-r_5) + 2(x-r_1)(x-r_2)(x-r_3)
\end{aligned}$$

$f^{(16)}(x)$ es un polinomio de grado 4 y 77 términos

$$\begin{aligned}
\frac{f^{(16)}(x)}{16!} =& 210(x-r_6)^4 + 135(x-r_4)^2(x-r_6)^2 + 10(x-r_4)^3(x-r_6)\\
&+135(x-r_5)^2(x-r_6)^2 + 10(x-r_5)^3(x-r_6) + 45(x-r_3)^2(x-r_6)^2\\
&+9(x-r_4)^2(x-r_5)^2 + 3(x-r_4)^3(x-r_5) + 3(x-r_3)^2(x-r_4)^2\\
&+3(x-r_3)^2(x-r_5)^2 + (x-r_2)(x-r_5)^3 + (x-r_1)(x-r_5)^3\\
&\quad\vdots
\end{aligned}$$

$$\begin{aligned}
&+(180(x-r_3)(x-r_4)(x-r_5)(x-r_6) + 60(x-r_2)(x-r_3)(x-r_4)(x-r_6)\\
&+60(x-r_2)(x-r_3)(x-r_5)(x-r_6) + 60(x-r_1)(x-r_3)(x-r_5)(x-r_6)\\
&\quad\vdots\\
&+30(x-r_1)(x-r_4)^2(x-r_6) + 30(x-r_2)(x-r_5)^2(x-r_6)
\end{aligned}$$

$f^{(15)}(x)$ es un polinomio de grado 5 y 115 términos

$$
\begin{aligned}
\frac{f^{(15)}(x)}{15!} =& 252(x-r_6)^5 + 360(x-r_4)^2(x-r_6)^3 + 45(x-r_4)^3(x-r_6)^2 \\
&+360(x-r_5)^2(x-r_6)^3 + 45(x-r_5)^3(x-r_6)^2 + 120(x-r_3)^2(x-r_6)^3 \\
&+3(x-r_4)^2(x-r_5)^3 + 3(x-r_4)^3(x-r_5)^2 + (x-r_3)^2(x-r_4)^3 \\
&\ \vdots \\
&+18(x-r_1)(x-r_3)(x-r_4)(x-r_5)^2 + 9(x-r_1)(x-r_3)^2(x-r_4)(x-r_5) \\
&\ \vdots \\
&+(10(x-r_2)(x-r_4)^3(x-r_6) + 6(x-r_3)(x-r_4)^3(x-r_5) \\
&+3(x-r_2)(x-r_4)^3(x-r_5) + 45(x-r_1)(x-r_3)^2(x-r_6)^2 \\
&+2(x-r_1)(x-r_3)(x-r_4)^3 + (3(x-r_1)(x-r_3)^2(x-r_5)^2 \\
&+405(x-r_4)(x-r_5)^2(x-r_6)^2
\end{aligned}
$$

Considerando

$$f^{(19)}(r_1) = f^{(18)}(r_2) = f^{(17)}(r_1) = f^{(16)}(r_2) = f^{(15)}(r_1) = 0,$$

trasladando estas raíces una vez más al 0 y 1, se tiene

$$f^{(19)}(0) = f^{(18)}(1) = f^{(17)}(0) = f^{(16)}(1) = f^{(15)}(0) = 0.$$

De nuevo la base de Gröbner es $\{1\}$ respecto del orden $lex(r_3, r_4, r_5, r_6)$.

Viendo el problema combinatorio que supone continuar con esta metodología para los polinomios con 7,...,19 raíces se busca seguir eliminando casos, lo que nos lleva a la siguiente proposición.

Proposición 26. *Si f es un polinomio de Casas-Alvero con todas sus raíces de multiplicidad al menos 2 entonces f' también es un polinomio de Casas-Alvero*

Demostración. Sea

$$f(x) = \prod_{i=1}^{j} (x-\alpha_i)^{p_i}$$

al que $p_i \geq 2,\ 1 \leq i \leq j$ y de grado d. Entonces

$$f'(x) = \prod_{i=1}^{j} (x-\alpha_i)^{p_i-1} \prod_{l=1}^{k} (x-\beta_l)^{p_l}$$

$p_i \geq 1$ y $1 \leq i \leq j$. Es decir, en f' todas las raíces de f también son sus raíces (junto con otras nuevas).

Además, para cada $n = 1, ..., d-1$ existe un $a \in K$ tal que $f(a) = f^{(n)}(a) = 0$, por ser f CA , pero $f^{(n)} = (f')^{(n-1)}$, por lo que para cada $n = 1, ..., d-2$ existe un $a \in K$ tal que $f'(a) = (f')^{(n)}(a) = 0$, por lo que f' también es de Casas-Alvero. ⧫

Corolario 27. Si f es un polinomio de Casas-Alvero de grado 20 entonces debe tener al menos una raíz simple en su factorización.

Demostración. Si f es de Casas-Alvero de grado 20 con

$$f(x) = \prod_{i=1}^{j} (x - \alpha_i)^{p_i}$$

y tal que $p_i \geq 2$ y $1 \leq i \leq j$, entonces f' sería de Casas-Alvero. Pero el grado de f' es 19, lo cual sabemos que no es posible por el Teorema 11. ⧫

Por ello eliminamos también todas las particiones de 20 en donde no haya al menos una raíz simple. Es decir, 11 casos de las 82 particiones de 20 para 7 raíces, para 8 raíces se eliminan 5 casos de 70, para 9 raíces se eliminan 2 casos de 54 y para 10 raíces se elimina 1 caso de 42. A partir de 11 raíces se tendrá siempre una raíz simple. Por lo que los casos restantes para grado 20 se muestran en la Tabla 2.

Número de raíces	Casos	No. de raíces	Casos
7	71	14	11
8	65	15	7
9	52	16	5
10	41	17	3
11	30	18	2
12	22	19	1
13	15		

Tabla 2. 325 casos restantes

La Tabla 3 muestra los tiempos y número de bases calculadas para cada uno de los polinomios de 4, 5 y 6 raíces de grado 20. El cálculo se realizó en el programa Maple 2017 en un computador con sistema operativo MacOs 10.13.4 con 2.3 GHz Intel Core i5 y 8 GB de memoria RAM.

Analizando el caso de los polinomios de grado 20 con exactamente 7 raíces distintas, como ya sabemos, solo se tienen 71 posibles multiplicidades de las 7 raíces del polinomio. Por otro lado, se tienen 203 posibles distribuciones de las raíces en las últimas 6 derivadas.

Haciendo uso del Corolario 27 y los Teoremas 17, 19 y 21, se descartan 6 casos éstas 203 distribuciones, por lo que para cada una de las 71 posibles multiplicidades

Número de raíces	Bases de Gröbner	Casos	Tiempo (s)	Tiempo (h)
4	1 938	64	5.511	0.00153
5	38 760	84	168.670	0.04685
6	581 400	90	10 125.138	2.81254

Tabla 3. Tiempos y número de bases calculadas

y sus permutaciones se deben calcular las bases de Gröbner en cada una de las 197 posibles distribuciones de las raíces en las últimas 6 derivadas: un total de 5 162 976 bases de Gröbner. Calculando algunos casos concretos de distribuciones de raíces en todas las posibles multiplicidades se estima que el tiempo cálculo de todas estas bases de Gröbner es de 62 horas aproximadamente.

De no ser por los resultados anteriores, el número de bases de Gröbner que se deberían calcular es de 5 507 796, y suponiendo que cada una se calcula en el mismo tiempo promedio que en el otro caso, todas éstas llevarían 67 horas aproximadamente.

Capítulo 4

La versión tropical de la Conjetura de Casas-Alvero: el caso p-ádico

En este capítulo exploramos si la geometría tropical p-ádica nos arroja algún resultado útil para atacar la resolución de la Conjetura de Casas-Alvero.

Partimos de el cuerpo de números p-ádicos, $\mathbb{Q}_p$, con la valoración p-ádica. Esta valoración se puede extender a la clausura algebraica $K = \overline{\mathbb{Q}}_p$ de $\mathbb{Q}_p$

$$v : K^* \to \mathbb{Q}.$$

Un polinomio de grado d,

$$\sum_{i=0}^{d} a_i x^i,$$

donde ningún coeficiente es 0, lo podemos identificar con la tupla $(a_0, a_1, \ldots, a_d) \in (K^*)^{d+1}$. Si aplicamos la valoración v coordenada a coordenada, obtendremos un punto $(v(a_0), v(a_1), \ldots, v(a_d))$ en $\mathbb{Q}^{d+1}$.

Vamos a calcular la imagen por v de todos los polinomios de la forma $b(x-a)^3$ donde $a, b \neq 0$ con la valoración 3-ádica.

Proposición 28. *Sea $A = \{b(x-a)^3 \in K[x] | a, b \neq 0\}$ ($K = \overline{\mathbb{Q}}_3$). Entonces, $v(A) \subset \mathbb{Q}^4$ es un plano.*

Demostración. Sea $b(x-a)^3 \in A$. Entonces

$$b(x-a)^3 = b(x^3 + 3x^2a + 3xa^2 + a^3)$$

se corresponde a la tupla $(ba^3, 3ba^2, 3ba, b)$. Si $s = v(a)$ y $t = v(b)$ entonces al aplicar v obtenemos $(3s+t, 2s+t+1, s+t+1, t)$, la parametrización de un plano. ♦

Queremos ver si estudiando las hipótesis de la Conjetura de Casas-Alvero, desde el lado de la valoración, obtenemos el mismo plano. Si esto fuera así, se podría aprovechar la geometría tropical para demostrar la conjetura.

Veremos que no es el caso. Para ello tenemos que dar la definición tropical de un polinomio de Casas-Alvero.

Definición 29. Un *polinomio tropical* en n variables es una expresión:

$$f(x) = \min_{i \in A}\{a_i + i_1 x_1 + \ldots + i_n x_n\}$$

donde $a_i \in \mathbb{Q}$ y $A \subseteq \mathbb{N}^n$ es el soporte de f.

Nótese que si $a_i = 0$ esto no elimina el monomio i del polinomio.

Definición 30. Sea

$$f(x) = \min_{i \in A}\{a_i + i_1 x_1 + \ldots + i_n x_n\}$$

un polinomio tropical. $w \in \mathbb{R}^n$ es una *raíz* de $f(x)$ si existen $j, k \in A$ tales que:

$$f(w) = a_j + j_1 w_1 + \ldots + j_n w_n = a_k + k_1 w_1 + \ldots + k_n w_n.$$

Esto es, el mínimo se alcanza dos veces.

Veremos a continuación qué significa que un polinomio tropical f tenga una raíz en común con una de sus derivadas $f^{(j)}$.

Teorema 31. [**7**] *Sea*

$$g = \sum_{i \in A} a_i x^i \in K[x_1, \ldots, x_n].$$

Llamamos

$$T(g) = \min_{i \in A}\{v(a_i) + i_1 x_1 + \ldots + i_n x_n\}$$

la tropicalización de g. Entonces

$$v(Zer(g, (K^*)^n)) \subseteq \mathbb{Q}^n$$

es exactamente el conjunto de las raíces del polinomio tropical $T(g)$.

Para estudiar las condiciones de Casas-Alvero en polinomios tropicales, no basta con afirmar que f y $f^{(j)}$ tienen una raíz en común.

Queremos estudiar los polinomios $T(g)$ donde g es un polinomio de grado d que tiene una raíz en común con su derivada j-ésima. En el caso clásico, estos son los ceros de $Res(g, g^{(j)})$. Por ello, lo que queremos estudiar es la valoración de este conjunto.

Definición 32. Sea $d > 0$ y $1 \leq j \leq d-1$. Denotamos por

$$\mathrm{TRes}(d, j) = v(Zer(Res(g, g^{(j)}), (K^*)^{d+1})) \subseteq \mathbb{Q}^{d+1}.$$

Nótese que si f es un polinomio tropical de grado d entonces sus coeficientes están en $\mathrm{TRes}(d, j)$ si y solo si f es la tropicalización de un polinomio g que tiene una raíz en común con $g^{(j)}$.

Definición 33. Un polinomio tropical f de grado d es un *polinomio tropical de Casas-Alvero* si, para todo $j = 1, \ldots, d-1$, $f \in \mathrm{TRes}(d, j)$.

Una definición más natural de polinomio tropical de Casas-Alvero sería el hecho de que f fuera la valoración de un polinomio clásico de Casas-Alvero, pero al no conocer los polinomios de Casas-Alvero, esta definición no es útil. Nótese que no son equivalentes ya que, en nuestra definición, para cada j el polinomio g_j que nos muestra que $f \in \mathrm{TRes}(d, j)$ depende de j.

Ahora veremos una caracterización de $\mathrm{TRes}(d, j)$ sin calcular la resultante. Aplicamos los resultados en [**5**] para este problema.

Definición 34. Sea M una matriz $r \times s$ con coeficientes en K. Un *circuito* de M es una combinación de filas de M no nula cuyo soporte (coordenadas no nulas) es minimal.

Observemos que si c_1 y c_2 son circuitos con el mismo soporte entonces c_1 es múltiplo de c_2. Entonces, por cada soporte minimal, existe esencialmente un único circuito. Por tanto, existe un número finito de circuitos.

Los circuitos nos permiten calcular la valoración del núcleo de una matriz.

Teorema 35. [**5**] *Sea M una matriz $r \times s$ con coeficientes en K. Sea $W = \ker(M) \cap (K^*)^s$. Sean $c_1, \ldots, c_t$ los circuitos de M. Cada circuito $c_j = (a_1, \ldots, a_s)$ determina un polinomio tropical de la forma*

$$C_j = \min_{a_i \neq 0} \{v(a_i) + x_i\}.$$

Entonces $v(W) \subseteq \mathbb{Q}^s$ es exactamente el conjunto de raíces tropicales comunes de $C_1, \ldots, C_t$.

Fijemos un primo p y un grado d. Estudiemos primero el conjunto de polinomios $g(x)$ de grado d que verifican $g(1) = (x^j g^{(j)})(1) = 0$. Estos polinomios forman un espacio vectorial y son el núcleo de la matriz,

$$\begin{pmatrix} 1 & 1 & .... & 1 & 1 & 1 & ... & 1 \\ 0 & 0 & ... & j! & \frac{(j+1)!}{1!} & \frac{(j+2)!}{2!} & ... & \frac{d!}{(d-j)!} \end{pmatrix}.$$

Usando el Teorema 35 podemos calcular la valoración del núcleo de esta matriz. Para ello tenemos que calcular los circuitos.

Las columnas de la matriz están indexadas del 0 a d. Ahora, para cada columna $j, ..., d$ hacemos una operación por filas para obtener un cero en la columna j. Esto nos proporciona un circuito que se corresponde con el polinomio $\frac{i!}{(i-j)!} g - x^j g^{(j)}$. De esta manera, calculamos todos los circuitos de la matriz y definimos la matriz M como sigue

$$M = \begin{pmatrix} 1 & 1 & .... & 1 & 1 & 1 & ... & 1 \\ 0 & 0 & ... & j! & \frac{(j+1)!}{1!} & \frac{(j+2)!}{2!} & ... & \frac{d!}{(d-j)!} \\ j! & j! & ... & 0 & j! - \frac{(j+1)!}{1!} & j! - \frac{(j+2)!}{2!} & ... & j! - \frac{d!}{(d-j)!} \\ \vdots & & & & & & & \\ \frac{d!}{(d-j)!} & \frac{d!}{(d-j)!} & ... & \frac{d!}{(d-j)!} - j! & \frac{d!}{(d-j)!} - \frac{(j+1)!}{1!} & \frac{d!}{(d-j)!} - \frac{(j+2)!}{2!} & ... & 0 \end{pmatrix}.$$

Si

$$g = \sum_{i=0}^{d} a_i x^i$$

entonces:

$$M \cdot \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_d \end{pmatrix} = \begin{pmatrix} g(1) \\ (x^j g^{(j)})(1) \\ (j! g - x^j g^{(j)})(1) \\ \vdots \\ \left(\frac{d!}{(d-j)!} g - x^j g^{(j)}\right)(1) \end{pmatrix}.$$

La valoración de la matriz M será:

$$M_p = \begin{pmatrix} 0 & 0 & .... & 0 & ... & 0 \\ \infty & \infty & ... & v_p(j!) & ... & v_p(\frac{d!}{(d-j)!}) \\ v_p(j!) & v_p(j!) & ... & \infty & ... & v_p(j! - \frac{d!}{(d-j)!}) \\ \vdots & & & & \ddots & \vdots \\ v_p(\frac{d!}{(d-j)!}) & v_p(\frac{d!}{(d-j)!}) & ... & v_p(\frac{d!}{(d-j)!} - j!) & ... & \infty \end{pmatrix}.$$

El Teorema 35 nos asegura lo siguiente

Corolario 36. Con la notación anterior, el núcleo de M_p (las raíces tropicales del sistema lineal dado por las filas de M_p) son todos los polinomios tropicales de $\mathrm{TRes}(n, j)$ que tienen al 0 como raíz en común con su derivada.

Teorema 37. *Sean d un grado, p un primo y $1 \leq j \leq d-1$ fijos. Sea*

$$f = \min_{i=0,\ldots,d} \{a_i + ix\}$$

un polinomio tropical. Si definimos

$$f^{(j)} = \min_{i=j,\ldots,d} \left\{ v\left(\frac{i!}{(i-j)!}\right) + a_i + ix \right\}$$

$$f_k = \min_{i \neq k} \left\{ v\left(\frac{k!}{(k-j)!} - \frac{i!}{(i-j)!}\right) + a_i + ix \right\}$$

para $k = j, \dots, d$ *(con* $\frac{i!}{(i-j)!} = 0$ *cuando* $i < j$*) entonces* f *está en* $\mathrm{TRes}(d, j)$ *si* $f, f^{(j)}, f_j, \dots, f_d$ *tienen una raíz en común.*

Demostración. Primeramente observemos que si $g \in K[x]$, $f = T(g)$, entonces, para todo $a \in K^*$, $T(g(ax)) = f(v(a) + x)$. Además se tiene que

$$(f(\alpha + x))^{(i)} = f^{(i)}(\alpha + x)$$

y

$$(f(\alpha + x))_i = f_i(\alpha + x)$$

con $j \leq i \leq d$.

Si $f \in \mathrm{TRes}(d, j)$ entonces $f = T(g)$ con $g(a) = g^{(j)}(a) = 0$. Por lo tanto $f, f^{(j)}$y los f_i con $j \leq i \leq d$ tienen a $v(a)$ como raíz común.

Sea $H = \{f, f^{(j)}, f_j, \dots, f_d\}$. Los polinomios en H tienen una raíz en común α si y solo si el conjunto de polinomios $\{f(\alpha + x), f^{(j)}(\alpha + x), f_j(\alpha + x), \dots, f_d(\alpha + x)\}$ tienen a 0 como raíz en común si y solo si los coeficientes de $f(\alpha + x)$ están en el núcleo de la matriz tropical M_p y, por tanto, podemos encontrar g en el núcleo de M cuyo valoración sea $f(\alpha + x)$. Esto significa que $g(1) = g^{(j)}(1) = 0$. Consideremos a tal que $v(a) = \alpha$ y sea $h = g(a^{-1}x)$. Entonces $h(a) = h^{(j)}(a) = 0$ y

$$T(h) = T(g)(v(a^{-1}) + x) = T(g)(-\alpha + x) = f.$$

Y por tanto $f \in \mathrm{TRes}(d, j)$. ♦

Usamos este teorema para determinar los polinomios tropicales de grado 3 de Casas-Alvero para $p = 3$.

Teorema 38. *La Conjetura de Casas-Alvero tropical es falsa para* $K = \mathbb{Q}_3$.

Demostración. Sea f nuestro polinomio genérico de grado 3:

$$f = \mathrm{mín}\{a_0, a_1 + x, a_2 + 2x, 3x\}.$$

Veamos ahora las condiciones necesarias para que f esté en $\mathrm{TRes}(3, 1)$. Considerando los circuitos correspondientes a los polinomios $\frac{i!}{(i-1)!}g - xg^{(1)}$ donde g son los polinomios de grado 3 tales que $g(1) = (xg^{(1)})(1) = 0$. Entonces la matriz M será

$$M = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 \\ 1 & 0 & -1 & -2 \\ 2 & 1 & 0 & -1 \\ 3 & 2 & 1 & 0 \end{pmatrix}.$$

A partir de ésta matriz definiremos M_p con $p = 3$ y la valoración p-ádica de las entradas diferentes de 0:

$$M_3 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ \infty & 0 & 0 & 1 \\ 0 & \infty & 0 & 0 \\ 0 & 0 & \infty & 0 \\ 1 & 0 & 0 & \infty \end{pmatrix}.$$

Por lo que $f \in \mathrm{TRes}(3, 1)$ solo si los siguientes polinomios tropicales tienen una misma raíz en común

$$\begin{aligned} f &= \text{mín}\{a_0, a_1 + x, a_2 + 2x, 3x\} \\ f^{(1)} &= \text{mín}\{a_1 + x, a_2 + 2x, 1 + 3x\} \\ f_1 &= \text{mín}\{a_0, a_2 + 2x, 3x\} \\ f_2 &= \text{mín}\{a_0, a_1 + x, 3x\} \\ f_3 &= \text{mín}\{a_0 + 1, a_1 + x, a_2 + 2x\}. \end{aligned}$$

Si suponemos que f tiene tres raíces distintas es fácil ver que no podría tener una raíz en común con $f^{(1)}, f_1, f_2$ y f_3. Por ello f tiene, a lo más, dos raíces distintas.

Sea ω la raíz común de todos los polinomios y supongamos que f tiene dos raíces distintas. Entonces f tiene que tener el mismo grafo que f_1 ó f_2.

Si el grafo de f es igual al de f_1, f_2 tendría una raíz ω de éstas dos. No hay otra opción más que

$$a_2 + 2\omega = a_1 + \omega = a_0 \leq 3\omega.$$

Por tanto

$$a_2 + 2\omega \leq 3\omega \Rightarrow a_2 \leq \omega$$

y

$$a_1 + \omega = a_0 \Rightarrow \omega = a_0 - a_1.$$

Entonces

$$a_2 \leq a_0 - a_1 \Rightarrow a_2 - a_1 \leq a_0$$

Además

$$a_0 = a_2 + 2(a_0 - a_1) \Rightarrow a_0 = 2a_1 - a_2.$$

Por lo que se debería cumplir lo siguiente

$$\begin{cases} a_0 = 2a_1 - a_2 \\ a_0 \geq a_2 - a_1 \end{cases}. \tag{3}$$

En el segundo caso

$$a_2 + 2\omega = a_1 + \omega = 3\omega \leq a_0,$$

es decir, $\omega = a_2 = a_1 - a_2$ y por ello $2a_2 = a_1$. Entonces

$$a_1 + a_2 \leq a_0.$$

Por lo que el siguiente sistema se debería cumplir

$$\begin{cases} 2a_2 & = a_1 \\ a_0 & \geq a_2 + a_1 \end{cases}. \tag{4}$$

En cualquiera de los dos casos ω sería también raíz tanto de $f^{(1)}$ como de f_3.

Suponiendo que f tiene una única raíz ω, sabemos que $3\omega = a_0$ y que $a_1 + \omega$ y $a_2 + 2\omega$ son mayores iguales que a_0, por lo que ω siempre es una raíz en común de f_1 y f_2. Como ω tiene que ser también raíz de $f^{(1)}$ entonces tenemos tres casos en donde el mínimo se alcanzaría,

- $a_1 + \omega = 3\omega + 1 \leq a_2 + 2\omega$
- $a_2 + 2\omega = 3\omega + 1 \leq a_1 + \omega$
- $a_1 + \omega = a_2 + 2\omega \leq 3\omega + 1$.

1. Cuando $a_1 + \omega = 3\omega + 1 \leq a_2 + 2\omega$ con $3\omega = a_0$. Entonces

$$\begin{cases} 3a_1 = & 2a_0 + 1 \\ 3a_1 \leq & a_2 + a_0 \end{cases}. \tag{5}$$

2. Si $a_2 + 2\omega = 3\omega + 1 \leq a_1 + \omega$ y $3\omega = a_0$ entonces $\omega = a_2 - 1 = \frac{a_0}{3}$. Por ello se debería cumplir lo siguiente

$$\begin{cases} a_0 = & 3(a_2 - 1) \\ a_0 \leq & a_1 + a_2 - 2 \end{cases}. \tag{6}$$

3. Si $a_1 + \omega = a_2 + 2\omega \leq 3\omega + 1$ con $3\omega = a_0$ y $a_0 \leq a_1 + \omega$ entonces

$$\begin{cases} 3a_1 = & 3a_2 + a_0 \\ 3a_1 \leq & 2a_0 + 3 \\ 2a_0 \leq & 3a_1 \end{cases}. \tag{7}$$

En éste y los otros dos casos donde ω es raíz de $f^{(1)}$, ω también será raíz de f_3.

Por lo tanto, para que $f \in \text{TRes}(3,1)$ se debe cumplir uno de los sistemas de ecuaciones y desigualdades correspondiente a alguno de los cinco casos que ya hemos mencionado.

Ahora veamos las condiciones necesarias para que f esté en $\text{TRes}(3,2)$. Considerando ahora los circuitos correspondientes a los polinomios $\frac{i!}{(i-2)!}g - x^2 g^{(2)}$ donde g

es un polinomio de grado 3 tal que $g(1) = (x^2 g^{(2)})(1) = 0$, tendremos la matriz

$$M = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 2 & 6 \\ 2 & 2 & 0 & -4 \\ 6 & 6 & 4 & 0 \end{pmatrix}.$$

Entonces,

$$M_3 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ \infty & \infty & 0 & 1 \\ 0 & 0 & \infty & 0 \\ 1 & 1 & 0 & \infty \end{pmatrix}.$$

Por lo que f tendrá una raíz en común con su segunda derivada solo si los siguientes polinomios tropicales tienen una misma raíz en común:

$$\begin{aligned} f &= \text{mín}\{a_0, a_1 + x, a_2 + 2x, 3x\}, \\ f^{(2)} &= \text{mín}\{a_2 + 2x, 1 + 3x\}, \\ \overline{f_2} &= \text{mín}\{a_0, a_1 + x, 3x\}, \\ \overline{f_3} &= \text{mín}\{a_0 + 1, a_1 + 1 + x, a_2 + 2x\}. \end{aligned}$$

Ya que $f^{(2)}$ tiene una única raíz ω, con $3\omega + 1 = a_2 + 2\omega$, entonces $\omega = a_2 - 1$. Por ello ω tendría que ser raíz de todos los polinomios anteriores.

En $\overline{f_2}$ tenemos tres opciones en donde se alcanzaría el mínimo:

- $a_1 + \omega = a_0 \leq 3\omega \Rightarrow a_1 + \omega + 1 = a_0 + 1 \leq 3\omega + 1 = a_2 + 2\omega$
- $a_1 + \omega = 3\omega \leq a_0 \Rightarrow a_1 + \omega + 1 = 3\omega + 1 = a_2 + 2\omega \leq a_0 + 1$
- $a_0 = 3\omega \leq a_1 + \omega \Rightarrow a_0 + 1 = 3\omega + 1 = a_2 + 2\omega \leq a_1 + \omega + 1$

En el primer caso nos queda:

$$\begin{cases} a_0 = & a_1 + a_2 - 1 \\ a_0 \leq & 3(a_2 - 1) \end{cases}. \tag{8}$$

En el segundo caso:

$$\begin{cases} a_1 + a_2 - 1 & = 3(a_2 - 1) \\ 3(a_2 - 1) & \leq a_0 \end{cases}. \tag{9}$$

De $a_0 + 1 = 3\omega + 1 = a_2 + 2\omega \leq a_1 + \omega + 1$ podemos ver que $\omega = a_2 - 1 = \frac{a_0}{3}$ y

$$a_0 + 1 \leq a_1 + a_2 - 1 + 1,$$

por lo que se debería cumplir lo siguiente:

$$\begin{cases} a_0 = & 3(a_2 - 1) \\ a_0 \leq & a_1 + a_2 - 1 \end{cases} . \tag{10}$$

En cualquiera de los tres casos ω también será raíz de $\overline{f_3}$ y f.

Así que $f \in \mathrm{TRes}(3,2)$ si se cumple alguno de los sistemas de ecuaciones y desigualdades correspondientes a los tres casos anteriores.

Entonces $\mathrm{TRes}(3,1) \cap \mathrm{TRes}(3,2)$ consiste en los polinomios que cumplen uno de los sistemas (3), (4), (5), (6) y (7) y uno de los sistemas (8), (9) y (10). Si resolvemos todas las posibles combinaciones tendremos cuatro sistemas con solución.

- (3) y (10)$\begin{cases} \dfrac{3}{8} \leq a_0,\ a_1 = \dfrac{1}{2} + \dfrac{2a_0}{3},\ a_2 = \dfrac{a_0}{3} + 1 \end{cases}$
- (5)y (10)$\begin{cases} a_0 \leq 0,\ a_1 = \dfrac{2a_0}{3} + \dfrac{1}{3},\ a_2 = \dfrac{a_0}{3} + 1 \end{cases}$
- (6) y (10)$\begin{cases} a_0 = a_0,\ 1 + \dfrac{2a_0}{3} \leq a_1,\ a_2 = \dfrac{a_0}{3} + 1 \end{cases}$
- (7) y (10)$\begin{cases} a_0 = a_0,\ a_1 = 1 + \dfrac{2a_0}{3},\ a_2 = \dfrac{a_0}{3} + 1 \end{cases}$

El caso (7)-(10) es la frontera del caso (6)-(10). Además, este caso (7)-(10) es exactamente la tropicalización del conjunto de Casas-Alvero descrito en la Proposición 28 con polinomios mónicos. Los otros tres casos nos proporcionan tres tipos de contraejemplos a la conjetura. ♦

Ejemplo 39. Sea $f(x) = \text{mín}\{0, 2+x, 1+2x, 3x\}$. Es facil ver que f, al igual que f_1 y f_2, tiene una única raíz en $\omega = 0$, cumpliendo el sistema (4). Por ello ω también es raíz de $f^{(1)}$, al igual que de f_3. Por lo tanto $f \in \mathrm{TRes}(3,1)$.

De igual forma se puede ver que f cumple con el sistema (10), es decir $f \in \mathrm{TRes}(3,2)$.

Como ya vimos en la Proposición 28, la tupla

$$(3s + t, 2s + t + 1, s + t + 1, t)$$

con la que se correspondería f es precisamente (a_0, a_1, a_2, a_3), es decir,

$$a_0 = 3s + t,\ a_1 = 2s + t + 1,\ a_2 = s + t + 1,\ a_3 = t.$$

Pero en este caso $t = s = 0$ y tendríamos que $a_1 = a_2 = 1$, lo cual es falso.

Esto quiere decir que existen dos polinomios clásicos, g_1 y g_2, cuya valoración en ambos casos es precisamente f, donde g_1 tiene una raíz en común con su primera derivada y g_2 con su segunda derivada, pero no viceversa.

Por ejemplo

$$g_1 = (x-1)^2(x-4) = x^3 - 6x^2 + 9x - 4$$

y

$$g_2 = (x-1)(x^2-2x+7) = x^3 - 3x^2 + 9x - 7.$$

Apéndice A

Conceptos y resultados utilizados

En este capítulo, recopilamos algunos de los conceptos y resultados que hemos usado a lo largo de este trabajo. La primera sección es parte de la Teoría de la Eliminación, donde vemos algunos resultados básicos sobre las resultantes. La segunda es un breve resumen de la teoría de las Bases de Gröbner que usamos para comprobar si diversos sistemas son compatibles o no. Por último, se dan fórmulas generales para las derivadas de los polinomios con un número fijo de raíces distintas usando las identidades de Newton.

A.1. Resultantes

Definición 40. Sean P y Q dos polinomios diferentes de cero en $D[x]$ con D un dominio y K su cuerpo de fracciones. Sean $p = \deg(P),\ q = \deg(Q)$. Escribamos

$$\begin{aligned} P =& a_p x^p + a_{p-1}x^{p-1} + ... + a_0 \\ Q =& b_q x^q + b_{q-1}x^{q-1} + ... + b_0 \end{aligned}$$

La *matriz de Sylvester* de p y Q, denotada por $Syl(P, Q)$, es la matriz

$$\begin{pmatrix} a_p & \dots & \dots & \dots & \dots & a_0 & 0 & \dots & 0 \\ 0 & \ddots & & & & & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & & & & & \ddots & 0 \\ 0 & \dots & 0 & a_p & \dots & \dots & \dots & \dots & a_0 \\ b_q & \dots & \dots & \dots & b_0 & 0 & \dots & \dots & 0 \\ 0 & \ddots & & & & \ddots & \ddots & & \vdots \\ \vdots & \ddots & \ddots & & & & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & & & & \ddots & 0 \\ 0 & \dots & \dots & 0 & b_q & \dots & \dots & \dots & b_0 \end{pmatrix}$$

Esta matriz tiene $p + q$ columnas y $p + q$ filas. Además, cada fila, contiene las coordenadas de

$$x^{q-1}P, ..., P, x^{p-1}Q, ..., Q$$

como vectores del espacio vectorial de los polinomios de grado a lo sumo $p+q-1$ en la base $\{x^{p+q-1}, ..., x, 1\}$.

Definición 41. La *Resultante* de P y Q, denotada por $Res(P,Q)$, es el determinante de la matriz de Sylvester de P y Q.

Si consideremos la transformación lineal

$$\begin{array}{rccc} R: & K[x]_{q-1} \times K[x]_{p-1} & \longrightarrow & K[x]_{p+q-1} \\ & (U,V) & \mapsto & UP+VQ \end{array}$$

es fácil ver que la matriz $Syl(P,Q)$ es la matriz asociada a la transformación lineal R donde en el espacio $K[x]_{q-1} \times K[x]_{p-1}$ consideramos la base

$$(x^{q-1}, ..., x, 1; x^{p-1}, ..., x, 1)$$

y en $K[x]_{p+q-1}$ la base

$$(x^{p+q-1}, ..., x, 1).$$

De aquí se deduce el siguiente lema.

Lema 42. Sea D un dominio. Entonces $Res(P,Q) = 0$ si y solo si existen dos polinomios diferentes de cero $U, V \in K[x]$ con $\deg(U) < q$, $\deg(V) < p$, y tales que $UP + VQ = 0$.

Demostración. $UP + VQ = 0$ si y solo si $(U,V) \in ker(Syl(P,Q))$ y el núcleo es no nulo si y solo si $Res(P,Q) = 0$. ♦

A partir de este lema se tiene el siguiente teorema.

Teorema 43. *Sea D un dominio. Sean $P, Q \in D[x]$ polinomios no nulos. Son equivalentes:*

- $Res(P,Q) = 0$.
- *P y Q tienen un factor común en $K[x]$.*
- *P y Q tienen una raíz en común en $\overline{K}$.*

Donde $\overline{K}$ es la cerradura algebraica de K.

Demostración. Es claro que P y Q tienen una raíz en común en $\overline{K}$ si y solo si tienen un factor común en $K[x]$. Por el lema anterior, $Res(P,Q) = 0$ si y solo si existen $U, V \in K[x]$ no nulos con $\deg(U) < q$, $\deg(V) < p$ y tales que $UP = -VQ$. Entonces P divide a VQ y por ser $\deg(V) < p$ y P y Q tienen que tener algún factor común.

Sea $F = \gcd(P,Q)$: si P y Q tienen un factor común entonces $\deg(F) > 1$, $P = FV$ y $Q = -FU$. De donde se tiene que $PU + QV = 0$. ♦

Ejemplo 44. Sean $P = x^2 - 3x + 1$ y $Q = 2x^3 - x^2 + 1$. Entonces

$$Syl(P,Q) = \begin{pmatrix} 1 & -3 & 1 & 0 & 0 \\ 0 & 1 & -3 & 1 & 0 \\ 0 & 0 & 1 & -3 & 1 \\ 2 & -1 & 0 & 1 & 0 \\ 0 & 2 & -1 & 0 & 1 \end{pmatrix}$$

y $Res(P,Q) = 29$. P y Q no tienen raíces comunes.

A.2. Bases de Gröbner

Definición 45. Un orden total, $>$, sobre el conjunto $\mathcal{M}_k$ de monomios en k variables, es un *orden monomial* si se cumplen las siguientes propiedades:

I. $X^\alpha > 1$ para todo $\alpha \in \mathbb{N}^k,\ \alpha \neq (0,...,0)$,
II. $X^\alpha > X^\beta \Rightarrow X^{\alpha+\gamma} > X^{\beta+\gamma}$, para todo $\alpha,\ \beta,\ \gamma \in \mathbb{N}^k$,
III. $>$ es un buen orden en $\mathcal{M}_k$.

Al monomio X^α más grande de $P \in K[x_1,...,x_k]$ con respecto al orden $>$ se denominará *monomio principal* de P.

Ejemplo 46. Sea $\mathcal{M}_k$ el conjunto de monomios en k variables, para $\alpha \in \mathbb{N}^k$, con $\alpha = (\alpha_1,\ldots,\alpha_k)$ y $X^\alpha = x_1^{\alpha_1}\cdots x_k^{\alpha_k} \in \mathcal{M}_k$. El *orden lexicográfico*, $>_{lex}$, con $x_1 >_{lex} x_2 >_{lex} \ldots >_{lex} x_k$, denotado por $lex(x_1,...,x_k)$, es el orden monomial tal que para todo $\alpha,\beta \in \mathbb{N}^k$, con $\alpha = (\alpha_1,\ldots,\alpha_k), \beta = (\beta_1,\ldots,\beta_k)$ se tiene

$$(\alpha_1,\ldots,\alpha_k) >_{lex} (\beta_1,\ldots,\beta_k) \Leftrightarrow (\alpha_1 > \beta_1) \vee (\alpha_1 = \beta_1 \wedge (\alpha_2,\ldots,\alpha_k) >_{lex} (\beta_2,\ldots,\beta_k))$$

Definición 47. Una *Base de Gröbner* de un ideal $I \subset K[x_1,...,x_k]$ respecto del orden monomial $>$ sobre $\mathcal{M}_k$ es un conjunto finito $\mathcal{G} \subset I$ tal que el monomio principal de cualquier elemento de I es un múltiplo de un monomio principal de algún elemento en $\mathcal{G}$.

Los siguientes resultados son demostrados en [**1**] y muestran propiedades importantes de estas bases.

Proposición 48. *Si $\mathcal{G}$ es una Base de Gröbner de I respecto del orden monomial $>$ sobre $\mathcal{M}_k$ entonces $P \in I$ si y sólo si P es reducible a 0 módulo $\mathcal{G}$*

Proposición 49. *Toda Base de Gröbner de I respecto del orden monomial $>$ sobre $\mathcal{M}_k$ es un conjunto de generadores de I.*

Proposición 50. *Para todo ideal de $K[x_1,...,x_k]$ existe una Base de Gröbner respecto de cualquier orden monomial $>$ sobre $\mathcal{M}_k$.*

El siguiente teorema da una propiedad importante de los conjuntos de polinomios que no comparten ceros en común.

Teorema 51 (Teorema de los ceros de Hilbert: versión débil). *Sea K un cuerpo algebraicamente cerrado y sea $\mathcal{P} = \{P_1, ..., P_s\}$ un subconjunto finito de $K[x_1, ..., x_k]$. Entonces, $Zer(\mathcal{P}, K^k) = \emptyset$ si y sólo si existen $A_1, ..., A_s \in K[x_1, ..., x_k]$ tales que*

$$A_1P_1 + ... + A_sP_s = 1.$$

Equivalentemente, si $I \subset K[x_1, \dots, x_k]$ es un ideal entonces

$$Zer(I, K^k) = \emptyset \Leftrightarrow I = (1)$$

De los resultados anteriores, dado un ideal $I \subset K[x_1, \dots, x_k]$, $I = (1)$ si y solo si para cualquier base de Gröbner G respecto de cualquier orden monomial, $1 \in G$.

A.3. Derivadas n-ésimas del producto de polinomios lineales

Sea

$$f(x) = \prod_{i=1}^{k} (x - \alpha_i)^{p_i}$$

con $\alpha_i \neq \alpha_j$ para todo $i \neq j$ con

$$\deg(p) = d = \sum_{i=1}^{k} p_i.$$

Queremos dar una expresión general de la $(d-i)$-ésima derivada de un polinomio para un i fijo. Para esto podemos usar la Regla General de Leibniz, la cual afirma que si h y g son funciones diferenciables n-veces entonces la n-ésima derivada del producto $f = hg$ está dada por

$$f^{(n)}(x) = (hg)^{(n)}(x) = \sum_{k=0}^{n} \binom{n}{k} h^{(n-k)}(x) g^{(k)}(x).$$

Se obtuvieron así expresiones generales para las siguientes derivadas de un polinomio f de grado d.

$$\frac{f^{(d-1)}(x)}{(d-1)!} = dx - \sum_{i=1}^{k} \alpha_i p_i$$

$$\frac{f^{(d-2)}(x)}{(d-2)!} = \frac{(d-1)d}{2} x^2 - (d-1) \left(\sum_{i=1}^{k} \alpha_i p_i \right) x + \frac{1}{2} \left(\sum_{i=1}^{k} p_i(p_i - 1)\alpha_i^2 + 2 \sum_{i \neq j} \alpha_i p_i \alpha_j p_j \right)$$

$$
\begin{aligned}
\frac{f^{(d-3)}(x)}{(d-3)!} =& \frac{(d-2)(d-1)d}{3!}x^3 - \frac{(d-2)(d-1)}{2!}\left(\sum_{i=1}^{k}\alpha_i p_i\right)x^2 \\
&+\frac{d-2}{2}\left(\sum_{i=1}^{k} p_i(p_i-1)\alpha_i^2 + 2\sum_{i\neq j} p_i\alpha_i p_j\alpha_j\right)x \\
&-\frac{1}{3!}\left(\sum_{i=1}^{k} p_i(p_i-1)(p_i-2)\alpha_i^3 + 3\sum_{i\neq j} p_i(p_i-1)\alpha_i^2 p_j\alpha_j + 3!\sum_{i\neq j\neq l} p_i\alpha_i p_j\alpha_j p_l\alpha_l\right) \\
\frac{f^{(d-4)}(x)}{(d-4)!} =& \frac{(d-3)(d-2)(d-1)d}{4!}x^4 - \frac{(d-3)(d-2)(d-1)}{3!}\left(\sum_{i=1}^{k}\alpha_i p_i\right)x^3 \\
&+\frac{(d-3)(d-2)}{2^2}\left(\sum_{i=1}^{k} p_i(p_i-1)\alpha_i^2 + 2\sum_{i\neq j} p_i\alpha_i p_j\alpha_j\right)x^2 \\
&-\frac{(d-3)}{3!}\left(\sum_{i=1}^{k} p_i(p_i-1)(p_i-2)\alpha_i^3 + 3\sum_{i\neq j} p_i(p_i-1)\alpha_i^2 p_j\alpha_j\right. \\
&\left.+3!\sum_{i\neq j\neq l} p_i\alpha_i p_j\alpha_j p_l\alpha_l\right)x \\
&+\frac{1}{4!}\left(\sum_{i=1}^{k} p_i(p_i-1)(p_i-2)(p_i-3)\alpha_i^4 + 4\sum_{i\neq j} p_i(p_i-1)(p_i-2)\alpha_i^3 p_j\alpha_j\right. \\
&+3!\sum_{i\neq j} p_i(p_i-1)\alpha_i^2 p_j(p_j-1)\alpha_j^2 + 12\sum_{i\neq j\neq l} p_i(p_i)\alpha_i^2 p_j\alpha_j p_l\alpha_l \\
&\left.+4!\sum_{i\neq j\neq l\neq m} \alpha_i p_j\alpha_j p_l\alpha_l p_m\alpha_m\right)
\end{aligned}
$$

Estas expresiones pueden ser deducidas también a partir de las identidades de Newton([**9**]). Sea

$$f(x) = \prod_{i=1}^{d}(x-\alpha_i),$$

con α_i sus raíces (no necesariamente diferentes). Sean $\sigma_k(\alpha_1, \alpha_2, ..., \alpha_d)$ los polinomios simétricos elementales definidos por

$$
\begin{aligned}
\sigma_0(\alpha_1, \alpha_2, ..., \alpha_d) =& 1 \\
\sigma_1(\alpha_1, \alpha_2, ..., \alpha_d) =& \alpha_1 + \alpha_2 + ... + \alpha_d
\end{aligned}
$$

$$\begin{aligned}
\sigma_2(\alpha_1, \alpha_2, ..., \alpha_d) =& \sum_{1 \leq i < j \leq d} \alpha_i \alpha_j \\
\sigma_3(\alpha_1, \alpha_2, ..., \alpha_d) =& \sum_{1 \leq i < j < k \leq d} \alpha_i \alpha_j \alpha_k \\
&\vdots \\
\sigma_d(\alpha_1, \alpha_2, ..., \alpha_d) =& \alpha_1 \alpha_2 ... \alpha_d \\
\sigma_k(\alpha_1, \alpha_2, ..., \alpha_d) =& 0, \text{ para } \ k > n,
\end{aligned}$$

y las sumas de potencias de las raíces , denominadas sumas de Newton

$$\pi_k(\alpha_1, \alpha_2, ..., \alpha_d) = \sum_{i=1}^{d} \alpha_i^k.$$

Entonces

$$k\sigma_k(\alpha_1, \ldots, x_d) = \sum_{i=1}^{k} (-1)^{i-1} \sigma_{k-i}(\alpha_1, \ldots, \alpha_d) \pi_i(\alpha_1, \ldots, \alpha_d),$$

con $1 \leq k \leq d$.

O bien,

$$\pi_k = (-1)^{k-1} k \sigma_k + \sum_{i=1}^{k-1} (-1)^{k-1+i} \sigma_{k-i} \pi_i,$$

para $1 \leq k \leq d$.

Ya que

$$f(x) = \sum_{k=0}^{d} (-1)^{d-k} \sigma_{d-k} x^k,$$

entonces los coeficientes de f se pueden describir en términos de las sumas de potencias de las raíces.

Bibliografía

[1] Saugata Basu, Richard Pollack, and Marie-Françoise Roy. *Algorithms in real algebraic geometry*, volume 10 of *Algorithms and Computation in Mathematics*. Springer-Verlag, Berlin, second edition, 2006.

[2] Eduardo Casas-Alvero. Higher order polar germs. *J. Algebra*, 240(1):326–337, 2001.

[3] Wouter Castryck, Robert Laterveer, and Myriam Ounaï es. Constraints on counterexamples to the Casas-Alvero conjecture and a verification in degree 12. *Math. Comp.*, 83(290):3017–3037, 2014.

[4] Gema M. Diaz-Toca and Laureano Gonzalez-Vega. On analyzing a conjecture about univariate polynomials and their roots by using Maple. In *Maple conference 2006. Proceedings of the conference, Waterloo, Ontario, Canada, July 23–26, 2006.*, pages 81–98. Waterloo: Maplesoft, 2006.

[5] Alicia Dickenstein, María Isabel Herrero, and Luis Felipe Tabera. Arithmetics and combinatorics of tropical Severi varieties of univariate polynomials. *Israel J. Math.*, 221(2):741–777, 2017.

[6] Jan Draisma and Johan P. de Jong. On the Casas-Alvero conjecture. *Eur. Math. Soc. Newsl.*, (80):29–33, 2011.

[7] Manfred Einsiedler, Mikhail Kapranov, and Douglas Lind. Non-Archimedean amoebas and tropical varieties. *J. Reine Angew. Math.*, 601:139–157, 2006.

[8] Hans-Christian Graf von Bothmer, Oliver Labs, Josef Schicho, and Christiaan van de Woestijne. The Casas-Alvero conjecture for infinitely many degrees. *J. Algebra*, 316(1):224–230, 2007.

[9] I. G. Macdonald. *Symmetric functions and Hall polynomials*. Oxford Mathematical Monographs. The Clarendon Press, Oxford University Press, New York, second edition, 1995. With contributions by A. Zelevinsky, Oxford Science Publications.

Índice alfabético