



UNIVERSIDAD DE BUENOS AIRES
Facultad de Ciencias Exactas y Naturales
Departamento de Matemática

Tesis de Licenciatura

Sobre la conjetura de Casas-Alvero

Juan Pablo Vicedo

Director: Daniel Perrucci

Diciembre de 2015

Índice general

Introducción	3
1. La conjetura en grados bajos	5
1.1. Preliminares básicos	5
1.2. Polinomios de grado 2 y grado 3	6
1.3. Formulación equivalente para grado ≥ 3	7
1.4. Polinomios de grado 4	15
1.5. Polinomios de grado 5	17
2. Resultados varios relacionados con la conjetura	21
2.1. El Principio de Transfer aplicado a la conjetura	21
2.2. “Casi contraejemplos” a la conjetura	25
2.3. Sobre el conjunto de raíces de un polinomio de Casas-Alvero	30
3. La conjetura en infinitos grados	41
3.1. Valuaciones	41
3.2. La conjetura en característica p	47
3.3. Resultado principal	56
Bibliografía	61

Introducción

La conjetura de Casas-Alvero fue formulada en el año 2001 por el matemático español Eduardo Casas-Alvero, mientras preparaba un trabajo relacionado con propiedades de curvas planas complejas ([1]). A la fecha la conjetura permanece abierta, y es reconocida por la simpleza de su planteo. Una de las formulaciones habituales de esta conjetura es la siguiente:

Conjetura de Casas-Alvero: Sea \mathbb{K} un cuerpo de característica 0, y sea $P(X) \in \mathbb{K}[X]$ un polinomio de grado $n \in \mathbb{N}$ tal que

$$\text{gr}(\text{mcd}(P, P^{(k)})) \geq 1 \quad \forall k \in \{1, 2, \dots, n-1\}.$$

Entonces P tiene una única raíz de multiplicidad n . Más precisamente, existen $\lambda \in \mathbb{K} \setminus \{0\}$ y $\alpha \in \overline{\mathbb{K}}$ tales que

$$P(X) = \lambda(X - \alpha)^n.$$

Notemos que, en caso de existir λ y α como se plantea en la conjetura, vale que $\alpha \in \mathbb{K}$ ya que el coeficiente de P de grado $n-1$ será igual a $-n\lambda\alpha \in \mathbb{K}$. Por otra parte, es claro que la conjetura vale trivialmente para $n=1$.

Esta conjetura también puede formularse del siguiente modo:

Formulación equivalente: Sea \mathbb{K} un cuerpo de característica 0, $P(X) \in \mathbb{K}[X]$ un polinomio de grado $n \in \mathbb{N}$ tal que existen $\alpha_1, \alpha_2, \dots, \alpha_{n-1} \in \overline{\mathbb{K}}$ que verifican:

$$P(\alpha_k) = P^{(k)}(\alpha_k) = 0 \quad \forall k \in \{1, 2, \dots, n-1\}.$$

Entonces $\alpha_1 = \alpha_2 = \dots = \alpha_{n-1}$ (y por lo tanto, P tiene una única raíz de multiplicidad n).

En resumidas cuentas, el primer registro de avance en relación a la conjetura se encuentra en [6], donde se prueba mediante técnicas de álgebra computacional la misma hasta grado

igual a 5, y se deja expresado que similarmente los autores han verificado la conjetura hasta grado igual a 7. Por otro lado, el mayor avance desde el punto de vista teórico fue logrado originalmente en [8], probando la conjetura para infinitos grados, utilizando la teoría de esquemas.

El objetivo de esta tesis es presentar un panorama general de lo que se sabe actualmente en torno a la conjetura de Casas-Alvero. En el Capítulo 1, se presenta una demostración de la conjetura para grados bajos, así como también una nueva formulación equivalente para grado mayor o igual a 3. En el Capítulo 2, se estudian diversos resultados relacionados con la conjetura, como por ejemplo la independencia del cuerpo de coeficientes en cuestión para su veracidad. Finalmente, en el Capítulo 3, se incluye una demostración de la conjetura para infinitos grados. Los resultados del último capítulo provienen originalmente de [8], pero el desarrollo en esta tesis seguirá el hilo de la demostración de estos mismos realizada en [7], que reemplaza como herramienta principal la teoría de esquemas por la teoría de valuaciones.

Capítulo 1

La conjetura en grados bajos

Como el nombre del capítulo lo indica, el objetivo del mismo es demostrar la conjetura para grados bajos; más específicamente, para los casos de grado 2, 3, 4 y 5. Sin embargo, presentaremos también una reformulación equivalente de la conjetura para polinomios de grado mayor o igual a 3. Ésta será utilizada para probar la conjetura en polinomios de grado 4 y 5, y también en el capítulo siguiente para dar una demostración de la independencia de la conjetura respecto del cuerpo de coeficientes en cuestión.

Comenzaremos con algunos aspectos preliminares que serán de utilidad a lo largo de toda la tesis.

1.1. Preliminares básicos

Sea \mathbb{K} un cuerpo de característica 0 y sea $P \in \mathbb{K}[X]$ un polinomio de grado $n \in \mathbb{N}$. Diremos que P es un polinomio *de Casas-Alvero*, o simplemente un polinomio *C-A* si P es un polinomio que satisface la hipótesis de la conjetura; es decir, si existen $\alpha_1, \alpha_2, \dots, \alpha_{n-1} \in \overline{\mathbb{K}}$ que verifican:

$$P(\alpha_k) = P^{(k)}(\alpha_k) = 0 \quad \forall k \in \{1, 2, \dots, n-1\}.$$

Para empezar, notemos que se puede suponer que el cuerpo \mathbb{K} es algebraicamente cerrado, ya que dado $P \in \mathbb{K}[X] \subset \overline{\mathbb{K}}[X]$ polinomio *C-A*, entonces existen $\lambda \in \overline{\mathbb{K}} \setminus \{0\}$ y $\alpha \in \overline{\mathbb{K}}$ tales que $P = \lambda(X - \alpha)^n$. Luego, como λ es el coeficiente principal de P , vale que $\lambda \in \mathbb{K}$.

Por otro lado, para todo $\lambda \in \mathbb{K} \setminus \{0\}$, $k \in \mathbb{N}$ tenemos que

- $(\lambda P)^{(k)} = \lambda P^{(k)}$,
- $\text{mcd}(\lambda P, \lambda P^{(k)}) = \text{mcd}(P, P^{(k)})$.

Entonces podemos suponer, de ser necesario, que P es mónico sin pérdida de generalidad.

A su vez, vale que para todo $\mu \in \mathbb{K} \setminus \{0\}$, $\alpha \in \mathbb{K}$ y $k \in \mathbb{N}$:

- $(P(\mu X + \alpha))^{(k)} = \mu^k P^{(k)}(\mu X + \alpha)$,
- $\text{mcd}(P(\mu X + \alpha), \mu^k P^{(k)}(\mu X + \alpha)) = \frac{1}{\mu^\ell} \text{mcd}(P, P^{(k)})(\mu X + \alpha)$, con $\ell = \text{gr}(\text{mcd}(P, P^{(k)}))$.

En consecuencia, suponiendo que \mathbb{K} es algebraicamente cerrado, podemos entonces efectuar transformaciones afines a las raíces para fijar el valor de una de ellas, o también de dos de ellas cuando se suponga que existe más de una.

1.2. Polinomios de grado 2 y grado 3

A lo largo de todo este capítulo supondremos sin pérdida de generalidad, por lo visto en la Sección 1.1, que \mathbb{K} es un cuerpo de característica 0 algebraicamente cerrado, y en esta sección que los polinomios C - A considerados son mónicos.

Sea por lo tanto $P(X) = X^2 + aX + b \in \mathbb{K}[X]$ un polinomio C - A de grado 2. Si llamamos $\alpha \in \mathbb{K}$ a la raíz común entre P y P' entonces α es raíz doble de P , y en consecuencia $P(X) = (X - \alpha)^2$.

Supongamos ahora que $P \in \mathbb{K}[X]$ es un polinomio C - A de grado 3. En este caso, si llamamos $\alpha_1 \in \mathbb{K}$ a la raíz común entre P y P' y $\alpha_2 \in \mathbb{K}$ a la raíz común entre P y P'' , entonces α_1 es raíz doble de P y, por lo tanto, existe $\beta \in \mathbb{K}$ tal que

$$\begin{aligned} P(X) &= (X - \alpha_1)^2(X - \beta), \\ P'(X) &= 2(X - \alpha_1)(X - \beta) + (X - \alpha_1)^2, \\ P''(X) &= 4(X - \alpha_1) + 2(X - \beta). \end{aligned}$$

Además α_2 es raíz de P , por lo que debemos mirar dos casos: $\alpha_2 = \alpha_1$ ó $\alpha_2 = \beta$.

- (i) Si $\alpha_2 = \alpha_1$ entonces α_2 es una raíz triple de P , y en consecuencia $P(X) = (X - \alpha_2)^3$;
- (ii) si $\alpha_2 = \beta$ entonces $P''(\alpha_2) = 4(\alpha_2 - \alpha_1) = 0$, luego $\alpha_2 = \alpha_1$ y en consecuencia α_2 es una raíz triple de P , con lo cual $P(X) = (X - \alpha_2)^3$.

1.3. Formulación equivalente para grado ≥ 3

Sea $P(X) = \sum_{i=0}^n a_i X^i \in \mathbb{K}[X]$ un polinomio de grado $n \geq 3$, entonces tenemos que $\forall k \in \{1, 2, \dots, n-1\}$:

$$P^{(k)}(X) = \sum_{i=k}^n i(i-1)\dots(i-k+1)a_i X^{i-k} = k! \sum_{i=k}^n \binom{i}{k} a_i X^{i-k}.$$

Como para $k \leq i \leq n$ vale que

$$\begin{aligned} \binom{i}{k} \binom{n}{i} &= \frac{i!}{k!(i-k)!} \cdot \frac{n!}{i!(n-i)!} = \frac{n!}{k!(i-k)!(n-i)!} = \\ &= \frac{n!}{k!(n-k)!} \cdot \frac{(n-k)!}{(i-k)!(n-i)!} = \binom{n}{k} \binom{n-k}{n-i}, \end{aligned}$$

tenemos que $\frac{\binom{i}{k}}{\binom{n}{k}} = \frac{\binom{n-k}{n-i}}{\binom{n}{i}}$ y

$$\frac{P^{(k)}(X)}{k! \binom{n}{k}} = \sum_{i=k}^n \frac{\binom{i}{k}}{\binom{n}{k}} a_i X^{i-k} = \sum_{i=k}^n \frac{\binom{n-k}{n-i}}{\binom{n}{i}} a_i X^{i-k}.$$

Supongamos ahora que $P(X)$ es un polinomio $C-A$ y sean $\alpha_1, \alpha_2, \dots, \alpha_{n-1} \in \mathbb{K}$ tales que $P^{(k)}(\alpha_k) = P(\alpha_k) = 0 \forall k \in \{1, 2, \dots, n-1\}$. Entonces debe ocurrir que

$$\sum_{i=k}^n \binom{n-k}{n-i} \alpha_k^{i-k} \frac{a_i}{\binom{n}{i}} = \sum_{i=0}^n \binom{n}{i} \alpha_k^i \frac{a_i}{\binom{n}{i}} = 0 \quad \forall k \in \{1, 2, \dots, n-1\},$$

o también, reemplazando i por $n-j$:

$$\sum_{j=0}^{n-k} \binom{n-k}{j} \alpha_k^{n-k-j} \frac{a_{n-j}}{\binom{n}{j}} = \sum_{j=0}^n \binom{n}{j} \alpha_k^{n-j} \frac{a_{n-j}}{\binom{n}{j}} = 0 \quad \forall k \in \{1, 2, \dots, n-1\}.$$

Esto puede resumirse en la siguiente igualdad matricial:

$$\begin{pmatrix} \alpha_{n-1} & 1 & 0 & 0 & \dots & 0 & 0 \\ \alpha_{n-2}^2 & 2\alpha_{n-2} & 1 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots \\ \alpha_1^{n-1} & (n-1)\alpha_1^{n-2} & \binom{n-1}{2}\alpha_1^{n-3} & \binom{n-1}{3}\alpha_1^{n-4} & \dots & 1 & 0 \\ \alpha_1^n & n\alpha_1^{n-1} & \binom{n}{2}\alpha_1^{n-2} & \binom{n}{3}\alpha_1^{n-3} & \dots & n\alpha_1 & 1 \\ \alpha_2^n & n\alpha_2^{n-1} & \binom{n}{2}\alpha_2^{n-2} & \binom{n}{3}\alpha_2^{n-3} & \dots & n\alpha_2 & 1 \\ \alpha_3^n & n\alpha_3^{n-1} & \binom{n}{2}\alpha_3^{n-2} & \binom{n}{3}\alpha_3^{n-3} & \dots & n\alpha_3 & 1 \\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots \\ \alpha_{n-1}^n & n\alpha_{n-1}^{n-1} & \binom{n}{2}\alpha_{n-1}^{n-2} & \binom{n}{3}\alpha_{n-1}^{n-3} & \dots & n\alpha_{n-1} & 1 \end{pmatrix} \cdot \begin{pmatrix} a_n \\ \frac{a_{n-1}}{n} \\ \frac{a_{n-2}}{\binom{n}{2}} \\ \frac{a_{n-3}}{\binom{n}{3}} \\ \vdots \\ \frac{a_1}{n} \\ a_0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

$$\text{Sea } M_n = \begin{pmatrix} \alpha_{n-1} & 1 & 0 & 0 & \dots & 0 & 0 \\ \alpha_{n-2}^2 & 2\alpha_{n-2} & 1 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots \\ \alpha_1^{n-1} & (n-1)\alpha_1^{n-2} & \binom{n-1}{2}\alpha_1^{n-3} & \binom{n-1}{3}\alpha_1^{n-4} & \dots & 1 & 0 \\ \alpha_1^n & n\alpha_1^{n-1} & \binom{n}{2}\alpha_1^{n-2} & \binom{n}{3}\alpha_1^{n-3} & \dots & n\alpha_1 & 1 \\ \alpha_2^n & n\alpha_2^{n-1} & \binom{n}{2}\alpha_2^{n-2} & \binom{n}{3}\alpha_2^{n-3} & \dots & n\alpha_2 & 1 \\ \alpha_3^n & n\alpha_3^{n-1} & \binom{n}{2}\alpha_3^{n-2} & \binom{n}{3}\alpha_3^{n-3} & \dots & n\alpha_3 & 1 \\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots \\ \alpha_{n-1}^n & n\alpha_{n-1}^{n-1} & \binom{n}{2}\alpha_{n-1}^{n-2} & \binom{n}{3}\alpha_{n-1}^{n-3} & \dots & n\alpha_{n-1} & 1 \end{pmatrix} \in \mathbb{K}^{(2n-2) \times (n+1)}.$$

Tenemos entonces que M_n es una matriz tal que $\text{rg}(M_n) \in \{n, n+1\}$, ya que $2n-2 \geq n+1 \iff n \geq 3$ (y por ende $\text{rg}(M_n) \leq n+1$), y además las primeras n filas de M_n son li.

Por lo tanto, concluimos que existe $P(X)$ polinomio C - A de grado n con $\alpha_1, \alpha_2, \dots, \alpha_{n-1} \in \mathbb{K}$ tales que $P^{(k)}(\alpha_k) = P(\alpha_k) = 0 \forall k \in \{1, 2, \dots, n-1\}$ si y sólo si el sistema lineal de ecuaciones:

$$M_n \cdot \vec{x} = \vec{0} \quad (1.1)$$

tiene solución no trivial (y dicha solución contiene información sobre los coeficientes de $P(X)$). En efecto, lo único que no es inmediato es que una solución no trivial representa un polinomio C - A de grado n ; pero entonces, si la primera coordenada de \vec{x} fuera nula, mirando las primeras n filas de la matriz M_n puede verse que las demás coordenadas de \vec{x} también resultan nulas. Luego, una solución no trivial del sistema (1.1) tiene primera coordenada no nula y por lo tanto el polinomio correspondiente tiene grado igual a n .

Por otro lado, es claro que el sistema (1.1) tiene solución no trivial si y sólo si $\text{rg}(M_n) = n$.

Tomando la matriz M_n por bloques de la siguiente manera:

$$M_n = \left(\begin{array}{c|c} A_n & U_n \\ \hline B_n & C_n \end{array} \right), \text{ con } A_n = \begin{pmatrix} \alpha_{n-1} \\ \alpha_{n-2}^2 \\ \vdots \\ \alpha_1^{n-1} \\ \alpha_1^n \end{pmatrix} \in \mathbb{K}^{n \times 1}, B_n = \begin{pmatrix} \alpha_2^n \\ \alpha_3^n \\ \vdots \\ \alpha_{n-1}^n \end{pmatrix} \in \mathbb{K}^{(n-2) \times 1},$$

$$U_n = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 & 0 \\ 2\alpha_{n-2} & 1 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ (n-1)\alpha_1^{n-2} & \binom{n-1}{2}\alpha_1^{n-3} & \binom{n-1}{3}\alpha_1^{n-4} & \dots & 1 & 0 \\ n\alpha_1^{n-1} & \binom{n}{2}\alpha_1^{n-2} & \binom{n}{3}\alpha_1^{n-3} & \dots & n\alpha_1 & 1 \end{pmatrix} \in \mathbb{K}^{n \times n},$$

que es triangular inferior e inversible, y

$$C_n = \begin{pmatrix} n\alpha_2^{n-1} & \binom{n}{2}\alpha_2^{n-2} & \binom{n}{3}\alpha_2^{n-3} & \dots & n\alpha_2 & 1 \\ n\alpha_3^{n-1} & \binom{n}{2}\alpha_3^{n-2} & \binom{n}{3}\alpha_3^{n-3} & \dots & n\alpha_3 & 1 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ n\alpha_{n-1}^{n-1} & \binom{n}{2}\alpha_{n-1}^{n-2} & \binom{n}{3}\alpha_{n-1}^{n-3} & \dots & n\alpha_{n-1} & 1 \end{pmatrix} \in \mathbb{K}^{(n-2) \times n},$$

tenemos que definiendo $T_n = \left(\begin{array}{c|c} U_n^{-1} & 0 \\ \hline -C_n U_n^{-1} & I_{n-2} \end{array} \right) \in \mathbb{K}^{(2n-2) \times (2n-2)}$ (inversible),

$$T_n M_n = \left(\begin{array}{c|c} U_n^{-1} & 0 \\ \hline -C_n U_n^{-1} & I_{n-2} \end{array} \right) \left(\begin{array}{c|c} A_n & U_n \\ \hline B_n & C_n \end{array} \right) = \left(\begin{array}{c|c} U_n^{-1} A_n & I_n \\ \hline B_n - C_n U_n^{-1} A_n & 0 \end{array} \right)$$

y tiene el mismo rango que M_n , que queríamos que sea n . Esto ocurrirá si y sólo si

$$B_n - C_n U_n^{-1} A_n = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}. \quad (1.2)$$

Nuestro siguiente objetivo será por lo tanto calcular U_n^{-1} . Para esto, necesitamos algunas definiciones.

Notación 1.1 Consideremos la siguiente notación:

- $\mathbb{N}^\bullet = \bigcup_{m \in \mathbb{N}_0} \mathbb{N}^m,$

- para $\vec{v} = (v_1, \dots, v_m) \in \mathbb{N}^\bullet$: $l(\vec{v}) = m$, $|\vec{v}| = \sum_{i=1}^m v_i$ y

$$\binom{|\vec{v}|}{\vec{v}} = \begin{cases} \frac{|\vec{v}|!}{v_1! \dots v_m!} & \text{si } m \in \mathbb{N}, \\ 1 & \text{si } m = 0. \end{cases}$$

Lema 1.2 Sea $m \in \mathbb{N}$ y sea $\vec{v} = (v_1, v_2, \dots, v_m) \in \mathbb{N}^m$. Entonces

$$\binom{|\vec{v}|}{\vec{v}} = \binom{|\vec{v}|}{v_1} \binom{|\vec{v}| - v_1}{(v_2, v_3, \dots, v_m)} = \binom{|\vec{v}| - v_1}{(v_2, v_3, \dots, v_m)} \binom{|\vec{v}|}{v_m}.$$

Demostración: En efecto, tenemos que

$$\begin{aligned} \binom{|\vec{v}|}{\vec{v}} &= \frac{(v_1 + v_2 + \dots + v_m)!}{v_1!v_2!\dots v_m!} = \\ &= \frac{(v_1 + v_2 + \dots + v_m)!}{v_1!(v_2 + v_3 + \dots + v_m)!} \cdot \frac{(v_2 + v_3 + \dots + v_m)!}{v_2!v_3!\dots v_m!} = \binom{|\vec{v}|}{v_1} \binom{|(v_2, v_3, \dots, v_m)|}{(v_2, v_3, \dots, v_m)}. \end{aligned}$$

También, de forma análoga,

$$\begin{aligned} \binom{|\vec{v}|}{\vec{v}} &= \frac{(v_1 + v_2 + \dots + v_m)!}{v_1!v_2!\dots v_m!} = \\ &= \frac{(v_1 + v_2 + \dots + v_{m-1})!}{v_1!v_2!\dots v_{m-1}!} \cdot \frac{(v_1 + v_2 + \dots + v_m)!}{(v_1 + v_2 + \dots + v_{m-1})!v_m!} = \binom{|(v_1, v_2, \dots, v_{m-1})|}{(v_1, v_2, \dots, v_{m-1})} \binom{|\vec{v}|}{v_m}. \end{aligned}$$

□

Definición 1.3 Para $n \in \mathbb{N}_0$, definimos los siguientes polinomios:

- $Q_0 \equiv 1 \in \mathbb{K}$;
- Para $n \in \mathbb{N}$:

$$\begin{aligned} Q_n(X_0, X_1, \dots, X_{n-1}) &= \sum_{\substack{\vec{v} \in \mathbb{N}^m \\ |\vec{v}|=n}} (-1)^{n-l(\vec{v})} \binom{n}{\vec{v}} \vec{X}^{\vec{v}} \\ &= \sum_{m=1}^n \left(\sum_{\substack{\vec{v} \in \mathbb{N}^m \\ |\vec{v}|=n}} (-1)^{n-m} \binom{n}{\vec{v}} \vec{X}^{\vec{v}} \right) \in \mathbb{K}[X_0, X_1, \dots, X_{n-1}], \end{aligned}$$

donde si $\vec{X} = (X_0, X_1, \dots, X_{n-1})$ y $\vec{v} = (v_1, v_2, \dots, v_m) \in \mathbb{N}^m$ es tal que $|\vec{v}| = n$, entonces

$$\vec{X}^{\vec{v}} = X_0^{v_1} X_{v_1}^{v_2} X_{v_1+v_2}^{v_3} \dots X_{v_1+v_2+\dots+v_{m-1}}^{v_m}.$$

Observación 1.4 Notar que en la definición anterior, los vectores \vec{X} y \vec{v} no tienen necesariamente la misma longitud y la notación $\vec{X}^{\vec{v}}$ representa algo distinto a lo usual.

Observación 1.5 De la definición anterior se deduce fácilmente que X_0 divide a $Q_n(X_0, \dots, X_{n-1})$ para todo $n \in \mathbb{N}$.

A modo de ejemplo, para $n = 1, 2, 3, 4$ y 5 resulta:

- $Q_1(X_0) = X_0$,

- $Q_2(X_0, X_1) = -X_0^2 + 2X_0X_1,$
- $Q_3(X_0, X_1, X_2) = X_0^3 - 3X_0^2X_2 - 3X_0X_1^2 + 6X_0X_1X_2,$
- $Q_4(X_0, X_1, X_2, X_3) = -X_0^4 + 4X_0^3X_3 + 6X_0^2X_2^2 + 4X_0X_1^3 - 12X_0^2X_2X_3 - 12X_0X_1^2X_3 - 12X_0X_1X_2^2 + 24X_0X_1X_2X_3,$
- $Q_5(X_0, X_1, X_2, X_3, X_4) = X_0^5 - 5X_0^4X_4 - 10X_0^3X_3^2 - 10X_0^2X_2^3 - 5X_0X_1^4 + 20X_0^3X_3X_4 + 30X_0^2X_2^2X_4 + 30X_0^2X_2X_3^2 + 20X_0X_1^3X_4 + 30X_0X_1^2X_3^2 + 20X_0X_1X_2^3 - 60X_0^2X_2X_3X_4 - 60X_0X_1^2X_3X_4 - 60X_0X_1X_2^2X_4 - 60X_0X_1X_2X_3^2 + 120X_0X_1X_2X_3X_4.$

El siguiente resultado nos resultará de gran utilidad en el cálculo de la matriz inversa en cuestión.

Proposición 1.6 *Para todo $n \in \mathbb{N}$ vale que*

1. $Q_n(X_0, X_1, \dots, X_{n-1}) = \sum_{k=1}^n (-1)^{k-1} \binom{n}{k} X_0^k \cdot Q_{n-k}(X_k, X_{k+1}, \dots, X_{n-1}),$
o equivalentemente, $\sum_{k=0}^n (-1)^k \binom{n}{k} X_0^k \cdot Q_{n-k}(X_k, X_{k+1}, \dots, X_{n-1}) = 0;$
2. $Q_n(X_0, X_1, \dots, X_{n-1}) = \sum_{k=1}^n (-1)^{k-1} \binom{n}{k} Q_{n-k}(X_0, X_1, \dots, X_{n-k-1}) \cdot X_{n-k}^k,$
o equivalentemente, $\sum_{k=0}^n (-1)^k \binom{n}{k} Q_{n-k}(X_0, X_1, \dots, X_{n-k-1}) \cdot X_{n-k}^k = 0.$

Demostración:

1. Separando la sumatoria en la definición de Q_n según el valor de la primer coordenada de \vec{v} y usando el Lema 1.2, tenemos que

$$\begin{aligned}
Q_n(X_0, X_1, \dots, X_{n-1}) &= \sum_{\substack{\vec{v} \in \mathbb{N}^\bullet \\ |\vec{v}|=n}} (-1)^{n-l(\vec{v})} \binom{n}{\vec{v}} \vec{X}^{\vec{v}} = \\
&= \sum_{k=1}^n \left(\sum_{\substack{\vec{w} \in \mathbb{N}^\bullet \\ |\vec{w}|=n-k}} (-1)^{n-l(\vec{w})-1} \binom{n}{k} \binom{n-k}{\vec{w}} X_0^k \cdot (X_k, X_{k+1}, \dots, X_{n-1})^{\vec{w}} \right) = \\
&= \sum_{k=1}^n (-1)^{k-1} \binom{n}{k} X_0^k \left(\sum_{\substack{\vec{w} \in \mathbb{N}^\bullet \\ |\vec{w}|=n-k}} (-1)^{n-k-l(\vec{w})} \binom{n-k}{\vec{w}} (X_k, X_{k+1}, \dots, X_{n-1})^{\vec{w}} \right) =
\end{aligned}$$

$$= \sum_{k=1}^n (-1)^{k-1} \binom{n}{k} X_0^k \cdot Q_{n-k}(X_k, X_{k+1}, \dots, X_{n-1}).$$

2. De manera análoga, separando la sumatoria en la definición de Q_n según el valor de la última coordenada de \vec{v} , tenemos que:

$$\begin{aligned} Q_n(X_0, X_1, \dots, X_{n-1}) &= \sum_{\substack{\vec{v} \in \mathbb{N}^\bullet \\ |\vec{v}|=n}} (-1)^{n-l(\vec{v})} \binom{n}{\vec{v}} \vec{X}^{\vec{v}} = \\ &= \sum_{k=1}^n \left(\sum_{\substack{\vec{w} \in \mathbb{N}^\bullet \\ |\vec{w}|=n-k}} (-1)^{n-l(\vec{w})-1} \binom{n-k}{\vec{w}} \binom{n}{k} (X_0, X_1, \dots, X_{n-k-1})^{\vec{w}} \cdot X_{n-k}^k \right) = \\ &= \sum_{k=1}^n (-1)^{k-1} \binom{n}{k} \left(\sum_{\substack{\vec{w} \in \mathbb{N}^\bullet \\ |\vec{w}|=n-k}} (-1)^{n-k-l(\vec{w})} \binom{n-k}{\vec{w}} (X_0, X_1, \dots, X_{n-k-1})^{\vec{w}} \right) X_{n-k}^k = \\ &= \sum_{k=1}^n (-1)^{k-1} \binom{n}{k} Q_{n-k}(X_0, X_1, \dots, X_{n-k-1}) \cdot X_{n-k}^k. \end{aligned}$$

□

Estamos ahora en condiciones de dar la fórmula para la inversa de la matriz U_n definida anteriormente.

Definición 1.7 Si $n \in \mathbb{N}$, sea $V_n \in \mathbb{K}^{n \times n}$ dada por

$$V_n = \begin{pmatrix} v_{1,1} & 0 & 0 & \dots & 0 & 0 \\ v_{2,1} & v_{2,2} & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ v_{n-1,1} & v_{n-1,2} & v_{n-1,3} & \dots & v_{n-1,n-1} & 0 \\ v_{n,1} & v_{n,2} & v_{n,3} & \dots & v_{n,n-1} & v_{n,n} \end{pmatrix},$$

con $v_{i,j} = (-1)^{i-j} \binom{i}{j} Q_{i-j}(\alpha_{n-i}, \alpha_{n-i+1}, \dots, \alpha_{n-j-1}) \forall 1 \leq j \leq i \leq n$, donde $\alpha_0 = \alpha_1$.

Lema 1.8 Para todo $n \in \mathbb{N}$, $U_n^{-1} = V_n$.

Demostración: Anteriormente, teníamos que

$$U_n = \begin{pmatrix} u_{1,1} & 0 & 0 & \dots & 0 & 0 \\ u_{2,1} & u_{2,2} & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ u_{n-1,1} & u_{n-1,2} & u_{n-1,3} & \dots & u_{n-1,n-1} & 0 \\ u_{n,1} & u_{n,2} & u_{n,3} & \dots & u_{n,n-1} & u_{n,n} \end{pmatrix},$$

con $u_{i,j} = \binom{i}{j} \alpha_{n-i}^{i-j} \forall 1 \leq j \leq i \leq n$, $\alpha_0 = \alpha_1$. Luego,

$$V_n \cdot U_n = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 & 0 \\ \lambda_{2,1} & 1 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ \lambda_{n-1,1} & \lambda_{n-1,2} & \lambda_{n-1,3} & \dots & 1 & 0 \\ \lambda_{n,1} & \lambda_{n,2} & \lambda_{n,3} & \dots & \lambda_{n,n-1} & 1 \end{pmatrix},$$

donde para $1 \leq j < i \leq n$:

$$\begin{aligned} \lambda_{i,j} &= \sum_{l=1}^n (V_n)_{i,l} (U_n)_{l,j} = \sum_{l=j}^i v_{i,l} \cdot u_{l,j} \\ &= \sum_{l=j}^i (-1)^{i-l} \binom{i}{l} Q_{i-l}(\alpha_{n-i}, \alpha_{n-i+1}, \dots, \alpha_{n-l-1}) \cdot \binom{l}{j} \alpha_{n-l}^{l-j} \\ &\stackrel{\underbrace{\quad}}{=} \sum_{k=0}^{i-j} (-1)^{i-j-k} \binom{i}{j+k} Q_{i-j-k}(\alpha_{n-i}, \alpha_{n-i+1}, \dots, \alpha_{n-j-k-1}) \cdot \binom{j+k}{j} \alpha_{n-j-k}^k \\ &= (-1)^{i-j} \sum_{k=0}^{i-j} (-1)^k \binom{i}{j+k} \binom{j+k}{j} Q_{i-j-k}(\alpha_{n-i}, \alpha_{n-i+1}, \dots, \alpha_{n-j-k-1}) \cdot \alpha_{n-j-k}^k. \end{aligned}$$

Dado que

$$\begin{aligned} \binom{i}{j+k} \binom{j+k}{j} &= \frac{i!}{(i-j-k)!(j+k)!} \cdot \frac{(j+k)!}{j!k!} = \frac{i!}{(i-j-k)!j!k!} = \\ &= \frac{i!}{j!(i-j)!} \cdot \frac{(i-j)!}{(i-j-k)!k!} = \binom{i}{j} \binom{i-j}{k}, \end{aligned}$$

resulta que

$$\begin{aligned} \lambda_{i,j} &= (-1)^{i-j} \sum_{k=0}^{i-j} (-1)^k \binom{i}{j} \binom{i-j}{k} Q_{i-j-k}(\alpha_{n-i}, \alpha_{n-i+1}, \dots, \alpha_{n-j-k-1}) \cdot \alpha_{n-j-k}^k \\ &= (-1)^{i-j} \binom{i}{j} \underbrace{\left(\sum_{k=0}^{i-j} (-1)^k \binom{i-j}{k} Q_{i-j-k}(\alpha_{n-i}, \alpha_{n-i+1}, \dots, \alpha_{n-j-k-1}) \cdot \alpha_{n-j-k}^k \right)}_{= 0 \text{ (Prop. 1,6(2))}} \\ &= 0, \end{aligned}$$

lo que demuestra que $V_n = U_n^{-1}$. \square

Finalmente, volviendo a la ecuación (1.2) tenemos que:

$$\begin{aligned}
 & B_n - C_n \cdot U_n^{-1} \cdot A_n = \\
 & = \begin{pmatrix} \alpha_2^n \\ \alpha_3^n \\ \vdots \\ \alpha_{n-1}^n \end{pmatrix} - \begin{pmatrix} \binom{n}{1}\alpha_2^{n-1} & \binom{n}{2}\alpha_2^{n-2} & \binom{n}{3}\alpha_2^{n-3} & \dots & \binom{n}{n-1}\alpha_2 & 1 \\ \binom{n}{1}\alpha_3^{n-1} & \binom{n}{2}\alpha_3^{n-2} & \binom{n}{3}\alpha_3^{n-3} & \dots & \binom{n}{n-1}\alpha_3 & 1 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ \binom{n}{1}\alpha_{n-1}^{n-1} & \binom{n}{2}\alpha_{n-1}^{n-2} & \binom{n}{3}\alpha_{n-1}^{n-3} & \dots & \binom{n}{n-1}\alpha_{n-1} & 1 \end{pmatrix} \\
 & \cdot \begin{pmatrix} 1 & 0 & \dots & 0 & 0 \\ -2Q_1(\alpha_{n-2}) & 1 & \dots & 0 & 0 \\ 3Q_2(\alpha_{n-3}, \alpha_{n-2}) & -3Q_1(\alpha_{n-3}) & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ (-1)^{n-2} \binom{n-1}{1} Q_{n-2}(\alpha_1, \dots, \alpha_{n-2}) & (-1)^{n-3} \binom{n-1}{2} Q_{n-3}(\alpha_1, \dots, \alpha_{n-3}) & \dots & 1 & 0 \\ (-1)^{n-1} \binom{n}{1} Q_{n-1}(\alpha_0, \dots, \alpha_{n-2}) & (-1)^{n-2} \binom{n}{2} Q_{n-2}(\alpha_0, \dots, \alpha_{n-3}) & \dots & -\binom{n}{n-1} Q_1(\alpha_0) & 1 \end{pmatrix} \\
 & \cdot \begin{pmatrix} \alpha_{n-1} \\ \alpha_{n-2}^2 \\ \alpha_{n-3}^3 \\ \vdots \\ \alpha_1^{n-1} \\ \alpha_0^n \end{pmatrix} = \begin{pmatrix} \alpha_2^n \\ \alpha_3^n \\ \vdots \\ \alpha_{n-1}^n \end{pmatrix} - \begin{pmatrix} \binom{n}{1}\alpha_2^{n-1} & \binom{n}{2}\alpha_2^{n-2} & \binom{n}{3}\alpha_2^{n-3} & \dots & \binom{n}{n-1}\alpha_2 & 1 \\ \binom{n}{1}\alpha_3^{n-1} & \binom{n}{2}\alpha_3^{n-2} & \binom{n}{3}\alpha_3^{n-3} & \dots & \binom{n}{n-1}\alpha_3 & 1 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ \binom{n}{1}\alpha_{n-1}^{n-1} & \binom{n}{2}\alpha_{n-1}^{n-2} & \binom{n}{3}\alpha_{n-1}^{n-3} & \dots & \binom{n}{n-1}\alpha_{n-1} & 1 \end{pmatrix} \\
 & \cdot \begin{pmatrix} \alpha_{n-1} \\ -2Q_1(\alpha_{n-2})\alpha_{n-1} + \alpha_{n-2}^2 \\ 3Q_2(\alpha_{n-3}, \alpha_{n-2})\alpha_{n-1} - 3Q_1(\alpha_{n-3})\alpha_{n-2}^2 + \alpha_{n-3}^3 \\ \vdots \\ \sum_{k=1}^{n-1} (-1)^{n-1-k} \binom{n-1}{k} Q_{n-1-k}(\alpha_1, \dots, \alpha_{n-1-k}) \alpha_{n-k}^k \\ \sum_{k=1}^n (-1)^{n-k} \binom{n}{k} Q_{n-k}(\alpha_0, \dots, \alpha_{n-k-1}) \alpha_{n-k}^k \end{pmatrix} \stackrel{\text{Prop. 1,6 (2)}}{=} \\
 & = \begin{pmatrix} \alpha_2^n \\ \alpha_3^n \\ \vdots \\ \alpha_{n-1}^n \end{pmatrix} - \begin{pmatrix} \binom{n}{1}\alpha_2^{n-1} & \binom{n}{2}\alpha_2^{n-2} & \binom{n}{3}\alpha_2^{n-3} & \dots & \binom{n}{n-1}\alpha_2 & 1 \\ \binom{n}{1}\alpha_3^{n-1} & \binom{n}{2}\alpha_3^{n-2} & \binom{n}{3}\alpha_3^{n-3} & \dots & \binom{n}{n-1}\alpha_3 & 1 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ \binom{n}{1}\alpha_{n-1}^{n-1} & \binom{n}{2}\alpha_{n-1}^{n-2} & \binom{n}{3}\alpha_{n-1}^{n-3} & \dots & \binom{n}{n-1}\alpha_{n-1} & 1 \end{pmatrix}
 \end{aligned}$$

$$\begin{aligned}
 & \cdot \begin{pmatrix} Q_1(\alpha_{n-1}) \\ -Q_2(\alpha_{n-2}, \alpha_{n-1}) \\ Q_3(\alpha_{n-3}, \alpha_{n-2}, \alpha_{n-1}) \\ \vdots \\ (-1)^{n-2} Q_{n-1}(\alpha_1, \dots, \alpha_{n-1}) \\ (-1)^{n-1} Q_n(\alpha_0, \dots, \alpha_{n-1}) \end{pmatrix} = \begin{pmatrix} \sum_{j=0}^n (-1)^j \binom{n}{j} \alpha_2^{n-j} Q_j(\alpha_{n-j}, \dots, \alpha_{n-1}) \\ \sum_{j=0}^n (-1)^j \binom{n}{j} \alpha_3^{n-j} Q_j(\alpha_{n-j}, \dots, \alpha_{n-1}) \\ \vdots \\ \sum_{j=0}^n (-1)^j \binom{n}{j} \alpha_{n-1}^{n-j} Q_j(\alpha_{n-j}, \dots, \alpha_{n-1}) \end{pmatrix} = \\
 & = \begin{pmatrix} \sum_{j=0}^{n-1} (-1)^j \binom{n}{j} \alpha_2^{n-j} Q_j(\alpha_{n-j}, \dots, \alpha_{n-1}) \\ \sum_{j=0}^{n-1} (-1)^j \binom{n}{j} \alpha_3^{n-j} Q_j(\alpha_{n-j}, \dots, \alpha_{n-1}) \\ \vdots \\ \sum_{j=0}^{n-1} (-1)^j \binom{n}{j} \alpha_{n-1}^{n-j} Q_j(\alpha_{n-j}, \dots, \alpha_{n-1}) \end{pmatrix} + (-1)^n \cdot \begin{pmatrix} Q_n(\alpha_0, \dots, \alpha_{n-1}) \\ Q_n(\alpha_0, \dots, \alpha_{n-1}) \\ \vdots \\ Q_n(\alpha_0, \dots, \alpha_{n-1}) \end{pmatrix} \stackrel{\text{Prop. 1,6 (1)}}{=} \\
 & = (-1)^{n-1} \cdot \begin{pmatrix} Q_n(\alpha_2, \alpha_1, \dots, \alpha_{n-1}) - Q_n(\alpha_1, \alpha_1, \dots, \alpha_{n-1}) \\ Q_n(\alpha_3, \alpha_1, \dots, \alpha_{n-1}) - Q_n(\alpha_1, \alpha_1, \dots, \alpha_{n-1}) \\ \vdots \\ Q_n(\alpha_{n-1}, \alpha_1, \dots, \alpha_{n-1}) - Q_n(\alpha_1, \alpha_1, \dots, \alpha_{n-1}) \end{pmatrix}.
 \end{aligned}$$

Por lo tanto, tenemos que

$$B_n - C_n \cdot U_n^{-1} \cdot A_n = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

si y sólo si

$$Q_n(\alpha_1, \alpha_1, \dots, \alpha_{n-1}) = Q_n(\alpha_i, \alpha_1, \dots, \alpha_{n-1}) \quad \forall i \in \{2, \dots, n-1\}.$$

En conclusión, para $n \geq 3$, la Conjetura de Casas-Alvero en grado n puede reformularse de la siguiente manera: para todos $\alpha_1, \dots, \alpha_{n-1} \in \mathbb{K}$,

$$\begin{aligned}
 Q_n(\alpha_1, \alpha_1, \dots, \alpha_{n-1}) = Q_n(\alpha_2, \alpha_1, \dots, \alpha_{n-1}) = \dots = Q_n(\alpha_{n-1}, \alpha_1, \dots, \alpha_{n-1}) & \implies \\
 \implies \alpha_1 = \alpha_2 = \dots = \alpha_{n-1}. &
 \end{aligned}$$

1.4. Polinomios de grado 4

En este caso, sea $P \in \mathbb{K}[X]$ un polinomio C - A de grado 4, y sean $\alpha_1, \alpha_2, \alpha_3$ las raíces comunes entre P y P', P'', P''' respectivamente ($\alpha_1, \alpha_2, \alpha_3 \in \mathbb{K}$).

Por los comentarios hechos en la Sección 1.1 podemos suponer, sin pérdida de generalidad, que $\alpha_1 = 0$. Por otro lado, por la Observación 1.5 tenemos que

$$Q_4(0, 0, \alpha_2, \alpha_3) = 0,$$

y por lo tanto debemos probar que la única solución del sistema

$$\begin{cases} Q_4(\alpha_2, 0, \alpha_2, \alpha_3) = 0 \\ Q_4(\alpha_3, 0, \alpha_2, \alpha_3) = 0 \end{cases}$$

es $\alpha_2 = \alpha_3 = 0$.

Entonces:

$$\begin{aligned} \begin{cases} Q_4(\alpha_2, 0, \alpha_2, \alpha_3) = 5\alpha_2^4 - 8\alpha_2^3\alpha_3 = 0 \\ Q_4(\alpha_3, 0, \alpha_2, \alpha_3) = 3\alpha_3^4 + 6\alpha_2^2\alpha_3^2 - 12\alpha_2\alpha_3^3 = 0 \end{cases} &\implies \\ \implies \begin{cases} \alpha_2^3 \cdot (5\alpha_2 - 8\alpha_3) = 0 \\ 3\alpha_3^2 \cdot (2\alpha_2^2 - 4\alpha_2\alpha_3 + \alpha_3^2) = 0 \end{cases} & . \end{aligned}$$

Analicemos tres casos:

1. Si $\alpha_2 = 0$ entonces $3\alpha_3^4 = 0 \implies \alpha_3 = 0$, y por lo tanto $\alpha_1 = \alpha_2 = \alpha_3 = 0$.
2. Si $\alpha_3 = 0$ entonces $5\alpha_2^4 = 0 \implies \alpha_2 = 0$, y por lo tanto $\alpha_1 = \alpha_2 = \alpha_3 = 0$.
3. Si $\alpha_2 \neq 0$ y $\alpha_3 \neq 0$, tenemos que:

$$\begin{aligned} \begin{cases} 5\alpha_2 - 8\alpha_3 = 0 \\ 2\alpha_2^2 - 4\alpha_2\alpha_3 + \alpha_3^2 = 0 \end{cases} &\implies \begin{cases} \alpha_3 \left(5 \cdot \frac{\alpha_2}{\alpha_3} - 8 \right) = 0 \\ \alpha_3^2 \left(2 \cdot \frac{\alpha_2^2}{\alpha_3^2} - 4 \cdot \frac{\alpha_2}{\alpha_3} + 1 \right) = 0 \end{cases} \implies \\ \implies \begin{cases} \frac{\alpha_2}{\alpha_3} = \frac{8}{5} \\ 2 \left(\frac{\alpha_2}{\alpha_3} \right)^2 - 4 \left(\frac{\alpha_2}{\alpha_3} \right) + 1 = 0 \end{cases} &\implies \\ \implies 2 \left(\frac{8}{5} \right)^2 - 4 \left(\frac{8}{5} \right) + 1 = 0 &\longrightarrow \text{ABS!} \end{aligned}$$

En consecuencia, $\alpha_1 = \alpha_2 = \alpha_3 = 0$ es una raíz de P de multiplicidad 4, como queríamos probar.

1.5. Polinomios de grado 5

En este caso, sea $P(X) \in \mathbb{K}[X]$ un polinomio $C-A$ de grado 5, y sean $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ las raíces comunes entre P y P', P'', P''', P^{IV} respectivamente ($\alpha_1, \alpha_2, \alpha_3, \alpha_4 \in \mathbb{K}$).

Análogamente al caso anterior, por los comentarios hechos en la Sección 1.1, podemos suponer sin pérdida de generalidad que $\alpha_1 = 0$. Por otro lado, por la Observación 1.5, tenemos que

$$Q_5(0, 0, \alpha_2, \alpha_3, \alpha_4) = 0,$$

y por lo tanto, debemos probar que la única solución del sistema

$$\begin{cases} Q_5(\alpha_2, 0, \alpha_2, \alpha_3, \alpha_4) = 0 \\ Q_5(\alpha_3, 0, \alpha_2, \alpha_3, \alpha_4) = 0 \\ Q_5(\alpha_4, 0, \alpha_2, \alpha_3, \alpha_4) = 0 \end{cases}$$

es $\alpha_2 = \alpha_3 = \alpha_4 = 0$.

Luego, como:

$$\begin{aligned} Q_5(\alpha_2, 0, \alpha_2, \alpha_3, \alpha_4) &= -9\alpha_2^5 + 25\alpha_2^4\alpha_4 + 20\alpha_2^3\alpha_3^2 - 40\alpha_2^3\alpha_3\alpha_4, \\ Q_5(\alpha_3, 0, \alpha_2, \alpha_3, \alpha_4) &= -9\alpha_3^5 + 15\alpha_3^4\alpha_4 - 10\alpha_2^3\alpha_3^2 + 30\alpha_2\alpha_3^4 + \\ &\quad + 30\alpha_2^2\alpha_3^2\alpha_4 - 60\alpha_2\alpha_3^3\alpha_4, \\ Q_5(\alpha_4, 0, \alpha_2, \alpha_3, \alpha_4) &= -4\alpha_4^5 - 10\alpha_3^2\alpha_4^3 + 20\alpha_3\alpha_4^4 - 10\alpha_2^3\alpha_4^2 + 30\alpha_2^2\alpha_4^3 + \\ &\quad + 30\alpha_2\alpha_3^2\alpha_4^2 - 60\alpha_2\alpha_3\alpha_4^3, \end{aligned}$$

debemos considerar el sistema

$$\begin{cases} \alpha_2^3(9\alpha_2^2 - 25\alpha_2\alpha_4 - 20\alpha_3^2 + 40\alpha_3\alpha_4) = 0 \\ \alpha_3^2(9\alpha_3^3 - 15\alpha_3^2\alpha_4 + 10\alpha_2^3 - 30\alpha_2^2\alpha_4 - 30\alpha_2\alpha_3^2 + 60\alpha_2\alpha_3\alpha_4) = 0 \\ 2\alpha_4^2(2\alpha_4^3 + 5\alpha_3^2\alpha_4 - 10\alpha_3\alpha_4^2 + 5\alpha_2^3 - 15\alpha_2^2\alpha_4 - 15\alpha_2\alpha_3^2 + 30\alpha_2\alpha_3\alpha_4) = 0 \end{cases}.$$

Analicemos cuatro casos:

1. Si $\alpha_2 = 0$, tenemos que:

$$\begin{cases} 3\alpha_3^4(3\alpha_3 - 5\alpha_4) = 0 \\ 2\alpha_4^3(5\alpha_3^2 - 10\alpha_3\alpha_4 + 2\alpha_4^2) = 0 \end{cases}.$$

Luego, vale que $\alpha_3 = \alpha_4 = 0$ ó $\alpha_3 \neq 0$ y $\alpha_4 \neq 0$, en cuyo caso tenemos que

$$\begin{cases} \frac{\alpha_3}{\alpha_4} = \frac{5}{3} \\ 5\left(\frac{\alpha_3}{\alpha_4}\right)^2 - 10\left(\frac{\alpha_3}{\alpha_4}\right) + 2 = 0 \end{cases} \longrightarrow \text{ABS!}$$

2. Si $\alpha_3 = 0$, tenemos que:

$$\begin{cases} \alpha_2^4(9\alpha_2 - 25\alpha_4) = 0 \\ 2\alpha_4^2(5\alpha_2^3 - 15\alpha_2^2\alpha_4 + 2\alpha_4^3) = 0 \end{cases}.$$

Luego, vale que $\alpha_2 = \alpha_4 = 0$ ó $\alpha_2 \neq 0$ y $\alpha_4 \neq 0$, en cuyo caso tenemos que

$$\begin{cases} \frac{\alpha_2}{\alpha_4} = \frac{25}{9} \\ 5\left(\frac{\alpha_2}{\alpha_4}\right)^3 - 15\left(\frac{\alpha_2}{\alpha_4}\right)^2 + 2 = 0 \end{cases} \longrightarrow ABS!$$

3. Si $\alpha_4 = 0$, tenemos que:

$$\begin{cases} \alpha_2^3(9\alpha_2^2 - 20\alpha_3^2) = 0 \\ \alpha_3^2(10\alpha_2^3 - 30\alpha_2\alpha_3^2 + 9\alpha_3^3) = 0 \end{cases}.$$

Luego, vale que $\alpha_2 = \alpha_3 = 0$ ó $\alpha_2 \neq 0$ y $\alpha_3 \neq 0$, en cuyo caso tenemos que

$$\begin{cases} \left(\frac{\alpha_2}{\alpha_3}\right)^2 = \frac{20}{9} \\ 10\left(\frac{\alpha_2}{\alpha_3}\right)^2 \cdot \left(\frac{\alpha_2}{\alpha_3}\right) - 30\left(\frac{\alpha_2}{\alpha_3}\right) + 9 = 0 \end{cases} \implies$$

$$\implies \begin{cases} \left(\frac{\alpha_2}{\alpha_3}\right)^2 = \frac{20}{9} \\ \left(10 \cdot \frac{20}{9} - 30\right) \left(\frac{\alpha_2}{\alpha_3}\right) + 9 = 0 \end{cases} \longrightarrow ABS!$$

4. Si $\alpha_2 \neq 0$, $\alpha_3 \neq 0$ y $\alpha_4 \neq 0$, tenemos que:

$$\begin{cases} 9\alpha_2^2 - 25\alpha_2\alpha_4 - 20\alpha_3^2 + 40\alpha_3\alpha_4 = 0 & (E_1) \\ 9\alpha_3^3 - 15\alpha_3^2\alpha_4 + 10\alpha_2^3 - 30\alpha_2^2\alpha_4 - 30\alpha_2\alpha_3^2 + 60\alpha_2\alpha_3\alpha_4 = 0 & (E_2) \\ 2\alpha_4^3 - 10\alpha_3\alpha_4^2 + 5\alpha_3^2\alpha_4 + 5\alpha_2^3 - 15\alpha_2^2\alpha_4 - 15\alpha_2\alpha_3^2 + 30\alpha_2\alpha_3\alpha_4 = 0 & (E_3) \end{cases}.$$

Reemplazando la ecuación E_3 por $E_2 - 2E_3$ y la ecuación E_2 por $3\alpha_2E_1 - 2E_2$, nos queda que:

$$\begin{cases} 9\alpha_2^2 - 25\alpha_2\alpha_4 - 20\alpha_3^2 + 40\alpha_3\alpha_4 = 0 \\ 7\alpha_2^3 - 15\alpha_2^2\alpha_4 - 18\alpha_3^3 + 30\alpha_3^2\alpha_4 = 0 \\ 9\alpha_3^3 - 25\alpha_3^2\alpha_4 + 20\alpha_3\alpha_4^2 - 4\alpha_4^3 = 0 \end{cases} \implies$$

$$\Rightarrow \begin{cases} \alpha_4^2 \cdot \left(9 \left(\frac{\alpha_2}{\alpha_4} \right)^2 - 25 \left(\frac{\alpha_2}{\alpha_4} \right) - 20 \left(\frac{\alpha_3}{\alpha_4} \right)^2 + 40 \left(\frac{\alpha_3}{\alpha_4} \right) \right) = 0 \\ \alpha_4^3 \cdot \left(7 \left(\frac{\alpha_2}{\alpha_4} \right)^3 - 15 \left(\frac{\alpha_2}{\alpha_4} \right)^2 - 18 \left(\frac{\alpha_3}{\alpha_4} \right)^3 + 30 \left(\frac{\alpha_3}{\alpha_4} \right)^2 \right) = 0 \\ \alpha_4^3 \cdot \left(9 \left(\frac{\alpha_3}{\alpha_4} \right)^3 - 25 \left(\frac{\alpha_3}{\alpha_4} \right)^2 + 20 \left(\frac{\alpha_3}{\alpha_4} \right) - 4 \right) = 0 \end{cases} .$$

Si llamamos $\mu = \frac{\alpha_2}{\alpha_4} \neq 0$ y $\xi = \frac{\alpha_3}{\alpha_4} \neq 0$, tenemos que:

$$\begin{cases} 9\mu^2 - 25\mu = 20\xi^2 - 40\xi & (E_4) \\ 7\mu^3 - 15\mu^2 = 18\xi^3 - 30\xi^2 & (E_5) \\ 9\xi^3 - 25\xi^2 + 20\xi - 4 = 0 & (E_6) \end{cases} .$$

Reemplazando la ecuación E_5 por $-E_4 + E_5 + 2E_6$, nos queda que

$$\begin{cases} 9\mu^2 - 25\mu = 20\xi^2 - 40\xi \\ (\mu - 1)(7\mu^2 - 17\mu + 8) = 7\mu^3 - 24\mu^2 + 25\mu - 8 = 0 \\ (\xi - 1)(9\xi^2 - 16\xi + 4) = 9\xi^3 - 25\xi^2 + 20\xi - 4 = 0 \end{cases} .$$

Consideremos tres casos:

a) Si $\mu = 1$, entonces vale que:

$$\begin{cases} 20\xi^2 - 40\xi + 16 = 0 \\ 9\xi^3 - 25\xi^2 + 20\xi - 4 = 0 \end{cases} ,$$

pero esto es imposible ya que

$$32 = (135\xi^2 - 195\xi + 52)(20\xi^2 - 40\xi + 16) - (300\xi - 200)(9\xi^3 - 25\xi^2 + 20\xi - 4).$$

b) Si $\xi = 1$, entonces vale que:

$$\begin{cases} 9\mu^2 - 25\mu + 20 = 0 \\ 7\mu^3 - 24\mu^2 + 25\mu - 8 = 0 \end{cases} ,$$

pero esto es imposible ya que

$$1544 = (585\mu - 1238)(7\mu^3 - 24\mu^2 + 25\mu - 8) - (455\mu^2 - 1259\mu + 418)(9\mu^2 - 25\mu + 20).$$

c) Si $\mu \neq 1$ y $\xi \neq 1$, entonces vale que:

$$\begin{cases} 9\mu^2 - 25\mu = 20\xi^2 - 40\xi & (E_7) \\ 7\mu^2 - 17\mu + 8 = 0 & (E_8) \\ 9\xi^2 - 16\xi + 4 = 0 & (E_9) \end{cases} .$$

Reemplazando la ecuación E_7 por $E_7 - \frac{9}{7}E_8 + \frac{20}{9}E_9$, nos queda que

$$\begin{cases} -\frac{22}{7}\mu - \frac{88}{63} = -\frac{40}{9}\xi \\ 7\mu^2 - 17\mu + 8 = 0 \\ 9\xi^2 - 16\xi + 4 = 0 \end{cases} .$$

Despejando ξ en la primera ecuación y reemplazando en la tercera, tenemos que

$$\mu^2 - \frac{1448}{891}\mu - \frac{304}{9801} = 0.$$

Reduciendo la ecuación E_8 módulo esta última tenemos que

$$-\frac{5011}{891}\mu + \frac{80536}{9801} = 0 ,$$

pero esto es imposible ya que $\mu = \frac{80536}{55121}$ no es solución de ninguna de las dos cuadráticas anteriores.

En consecuencia, $\alpha_1 = \alpha_2 = \alpha_3 = \alpha_4 = 0$ es una raíz de P de multiplicidad 5, como queríamos probar.

Capítulo 2

Resultados varios relacionados con la conjetura

En este capítulo estudiaremos diversos resultados relacionados con la Conjetura de Casas-Alvero.

En la Sección 2.1 se incluye una demostración de un caso particular del Principio de Transfer, en el cual se establece que la conjetura es cierta en grado n para polinomios con coeficientes en un cuerpo \mathbb{K} de característica cero algebraicamente cerrado si y sólo si es cierta en grado n para polinomios con coeficientes en cualquier cuerpo de característica cero algebraicamente cerrado. Esta flexibilidad hará que en lo sucesivo nos enfoquemos, sin pérdida de generalidad, en polinomios con coeficientes en \mathbb{C} .

En la Sección 2.2, siguiendo [7], se define lo que es un “casi contraejemplo” a la conjetura y se prueba la existencia de ellos.

Por último, en la Sección 2.3, se incluyen resultados provenientes de [7] y [2] en los que se estudian diversas propiedades del conjunto de raíces de un polinomio C - A .

2.1. El Principio de Transfer aplicado a la conjetura

El Principio de Transfer es una herramienta muy poderosa que permite, por ejemplo, extender ciertos resultados probados sobre un cuerpo de característica cero algebraicamente cerrado a otro cuerpo con las mismas propiedades, sin necesidad de replicar la demostración o adaptarla de un cuerpo a otro, lo cual no siempre es sencillo ni factible.

La idea central es probar que la conjetura para grado n en un cuerpo \mathbb{K} de característica

cero algebraicamente cerrado puede reformularse como una cierta propiedad que no involucra al propio cuerpo \mathbb{K} sino solamente a su subcuerpo primo, que resulta isomorfo a \mathbb{Q} . De esta manera, la veracidad de la conjetura resulta independiente del cuerpo original.

Sea entonces \mathbb{K} de característica cero algebraicamente cerrado; por simplicidad suponemos directamente $\mathbb{Q} \subseteq \mathbb{K}$. Dado que ya vimos que la conjetura es cierta para polinomios de grado 1 y 2 en cualquier cuerpo de característica cero, podemos restringirnos a polinomios de grado $n \geq 3$; y como vimos en la Sección 1.3, la conjetura es cierta en grado n para polinomios en $\mathbb{K}[X]$ si y sólo si para todos $\alpha_1, \dots, \alpha_{n-1} \in \mathbb{K}$:

$$\begin{aligned} Q_n(\alpha_1, \alpha_1, \dots, \alpha_{n-1}) = Q_n(\alpha_2, \alpha_1, \dots, \alpha_{n-1}) = \dots = Q_n(\alpha_{n-1}, \alpha_1, \dots, \alpha_{n-1}) &\implies \\ \implies \alpha_1 = \alpha_2 = \dots = \alpha_{n-1} \end{aligned}$$

(donde el polinomio Q_n es el de la Definición 1.3); es decir, si $\alpha_1, \dots, \alpha_{n-1} \in \mathbb{K}$ son tales que

$$\left\{ \begin{array}{l} Q_n(\alpha_2, \alpha_1, \dots, \alpha_{n-1}) - Q_n(\alpha_1, \alpha_1, \dots, \alpha_{n-1}) = 0 \\ Q_n(\alpha_3, \alpha_1, \dots, \alpha_{n-1}) - Q_n(\alpha_1, \alpha_1, \dots, \alpha_{n-1}) = 0 \\ \vdots \\ Q_n(\alpha_{n-1}, \alpha_1, \dots, \alpha_{n-1}) - Q_n(\alpha_1, \alpha_1, \dots, \alpha_{n-1}) = 0 \end{array} \right. ,$$

entonces tenemos que

$$\left\{ \begin{array}{l} \alpha_2 - \alpha_1 = 0 \\ \alpha_3 - \alpha_1 = 0 \\ \vdots \\ \alpha_{n-1} - \alpha_1 = 0 \end{array} \right. .$$

En consecuencia, definiendo para $i \in \{2, 3, \dots, n-1\}$ los polinomios $T_i, U_i \in \mathbb{K}[X_1, X_2, \dots, X_{n-1}]$ de la siguiente manera:

- $T_i(X_1, X_2, \dots, X_{n-1}) = Q_n(X_i, X_1, X_2, \dots, X_{n-1}) - Q_n(X_1, X_1, X_2, \dots, X_{n-1})$ y
- $U_i(X_1, X_2, \dots, X_{n-1}) = X_i - X_1,$

concluimos que la conjetura es cierta en grado n para polinomios en $\mathbb{K}[X]$ si y sólo si para todo $\vec{\alpha} = (\alpha_1, \dots, \alpha_{n-1}) \in \mathbb{K}^{n-1}$ vale que

$$\text{si } \left\{ \begin{array}{l} T_2(\vec{\alpha}) = 0 \\ T_3(\vec{\alpha}) = 0 \\ \vdots \\ T_{n-1}(\vec{\alpha}) = 0 \end{array} \right. , \text{ entonces } \left\{ \begin{array}{l} U_2(\vec{\alpha}) = 0 \\ U_3(\vec{\alpha}) = 0 \\ \vdots \\ U_{n-1}(\vec{\alpha}) = 0 \end{array} \right. .$$

Por el Teorema de los Ceros de Hilbert (ver por ejemplo [11, Theorem 1]), esto equivale a que $U_j \in \sqrt{I} \forall j \in \{2, 3, \dots, n-1\}$, donde $I = \langle T_2, T_3, \dots, T_{n-1} \rangle \subseteq \mathbb{K}[X_1, X_2, \dots, X_{n-1}]$ y \sqrt{I} es su ideal radical; en otras palabras, $\forall j \in \{2, 3, \dots, n-1\}$ existe $N_j \in \mathbb{N}$ tal que $U_j^{N_j} \in I$.

En resumidas cuentas, según lo visto hasta aquí, podemos afirmar que la conjetura es cierta en grado n para polinomios en $\mathbb{K}[X]$ si y sólo si para todo $j \in \{2, 3, \dots, n-1\}$ existen $N_j \in \mathbb{N}$ y polinomios $R_{ij} \in \mathbb{K}[X_1, X_2, \dots, X_{n-1}] \forall i \in \{2, 3, \dots, n-1\}$ tales que

$$\sum_{i=2}^{n-1} T_i R_{ij} = U_j^{N_j}. \quad (2.1)$$

El siguiente paso entonces será, para cada $j \in \{2, 3, \dots, n-1\}$ y tomando $N_j \in \mathbb{N}$ fijo, analizar el hecho de que existan los polinomios $R_{ij} \in \mathbb{K}[X_1, X_2, \dots, X_{n-1}]$ como en (2.1); siendo nuestro objetivo probar que dicha existencia resulta independiente del cuerpo \mathbb{K} .

Observación 2.1 Para todos $i, j \in \{2, 3, \dots, n-1\}$ vale:

- $T_i, U_j^{N_j} \in \mathbb{Z}[X_1, \dots, X_{n-1}] \setminus \{0\}$: en efecto, lo único que no es inmediato es que $T_i \neq 0$, pero siguiendo la Definición 1.3, es fácil ver que el coeficiente que acompaña al monomio X_i^n en $Q_n(X_i, X_1, \dots, X_{n-1})$ es

$$(-1)^{n-1} \binom{n}{(n)} + (-1)^{n-2} \binom{n}{(i, n-i)} = (-1)^{n-1} \left(1 - \binom{n}{i} \right) \neq 0,$$

y por la Observación 1.5, X_1 divide a $Q_n(X_1, X_1, \dots, X_{n-1})$, con lo cual el monomio X_i^n no aparece en su fórmula expandida.

- T_i es homogéneo de grado n y $U_j^{N_j}$ es homogéneo de grado N_j , por lo que podemos suponer sin pérdida de generalidad que todos los polinomios R_{ij} en (2.1) son homogéneos de grado $N_j - n$: en efecto, si alguno no fuera homogéneo reemplazamos simultáneamente todos los R_{ij} por sus respectivas componentes homogéneas de grado $N_j - n$ manteniéndose dicha igualdad.

Luego llamando $\vec{X} = (X_1, X_2, \dots, X_{n-1})$, $\vec{v} = (v_1, \dots, v_{n-1}) \in \mathbb{N}_0^{n-1}$ y utilizando ahora sí la notación habitual para monomios $\vec{X}^{\vec{v}} = X_1^{v_1} \dots X_{n-1}^{v_{n-1}}$ (a diferencia de la utilizada en la Definición 1.3), tenemos que si

$$T_i = \sum_{\substack{\vec{e} \in \mathbb{N}_0^{n-1} \\ |\vec{e}|=n}} t_{i\vec{e}} \vec{X}^{\vec{e}} \quad \forall i \in \{2, 3, \dots, n-1\},$$

$$R_{ij} = \sum_{\substack{\vec{g} \in \mathbb{N}_0^{n-1} \\ |\vec{g}|=N_j-n}} r_{ij\vec{g}} \vec{X}^{\vec{g}} \quad \forall i, j \in \{2, 3, \dots, n-1\},$$

y

$$U_j^{N_j} = \sum_{\substack{\vec{f} \in \mathbb{N}_0^{n-1} \\ |\vec{f}| = N_j}} u_{j\vec{f}} \vec{X}^{\vec{f}} \quad \forall j \in \{2, 3, \dots, n-1\},$$

para cada $j \in \{2, 3, \dots, n-1\}$ la ecuación (2.1) nos queda:

$$\sum_{i=2}^{n-1} \left(\sum_{\substack{\vec{e} \in \mathbb{N}_0^{n-1} \\ |\vec{e}| = n}} t_{i\vec{e}} \vec{X}^{\vec{e}} \right) \left(\sum_{\substack{\vec{g} \in \mathbb{N}_0^{n-1} \\ |\vec{g}| = N_j - n}} r_{ij\vec{g}} \vec{X}^{\vec{g}} \right) = \sum_{\substack{\vec{f} \in \mathbb{N}_0^{n-1} \\ |\vec{f}| = N_j}} u_{j\vec{f}} \vec{X}^{\vec{f}}.$$

Esto es equivalente a que $\forall \vec{f} \in \mathbb{N}_0^{n-1}$ tal que $|\vec{f}| = N_j$, vale que

$$\sum_{i=2}^{n-1} \sum_{\substack{\vec{g} \in \mathbb{N}_0^{n-1}, |\vec{g}| = N_j - n \\ \vec{e} \in \mathbb{N}_0^{n-1}, |\vec{e}| = n \\ \vec{g} + \vec{e} = \vec{f}}} t_{i\vec{e}} r_{ij\vec{g}} = u_{j\vec{f}}. \quad (2.2)$$

Sea

$$\{\vec{f} \in \mathbb{N}_0^{n-1} \mid |\vec{f}| = N_j\} = \{\vec{f}_1, \vec{f}_2, \dots, \vec{f}_{B_j}\}$$

y

$$\{\vec{g} \in \mathbb{N}_0^{n-1} \mid |\vec{g}| = N_j - n\} = \{\vec{g}_1, \vec{g}_2, \dots, \vec{g}_{C_j}\}.$$

En vista de las ecuaciones (2.2), la existencia de los polinomios R_{ij} queda determinada por un sistema lineal de B_j ecuaciones (una por cada coeficiente de $U_j^{N_j}$) y $(n-2)C_j$ incógnitas (una por cada coeficiente de cada R_{ij} de grado $N_j - n$). Es decir, para cada $j \in \{2, 3, \dots, n-1\}$ podemos plantear un sistema lineal de ecuaciones de la forma

$$\mathcal{T}_j \cdot \mathcal{R}_j = \mathcal{U}_j$$

donde la matriz $\mathcal{T}_j \in \mathbb{Z}^{B_j \times (n-2)C_j}$ está formada por 0 y coeficientes de los polinomios T_2, T_3, \dots, T_{n-1} , el vector de incógnitas $\mathcal{R}_j \in \mathbb{K}^{(n-2)C_j}$ representa los coeficientes de los polinomios $R_{2j}, R_{3j}, \dots, R_{(n-1)j}$ y $\mathcal{U}_j \in \mathbb{Z}^{B_j}$ está formado por coeficientes del polinomio $U_j^{N_j}$.

Pero entonces, dado que tanto \mathcal{T}_j como \mathcal{U}_j son matrices con coeficientes en $\mathbb{Z} \subseteq \mathbb{Q}$, por argumentos estándar de álgebra lineal, si este sistema tiene una solución en $\mathbb{K}^{(n-2)C_j}$, entonces también tiene una solución en $\mathbb{Q}^{(n-2)C_j}$.

Finalmente, la conclusión es que la conjetura es cierta en grado n para polinomios en $\mathbb{K}[X]$ si y sólo si para todo $j \in \{2, 3, \dots, n-1\}$ existe $N_j \in \mathbb{N}$ tal que el sistema de ecuaciones

$$\mathcal{T}_j \cdot \mathcal{R}_j = \mathcal{U}_j,$$

que tiene coeficientes en \mathbb{Z} , tiene solución en $\mathbb{Q}^{(n-2)C_j}$, que es una condición independiente del cuerpo \mathbb{K} .

De esta manera, hemos probado el siguiente

Teorema 2.2 *Sea \mathbb{K} un cuerpo de característica cero algebraicamente cerrado y $n \in \mathbb{N}$. La conjetura de Casas-Alvero es cierta para polinomios de grado n con coeficientes en \mathbb{K} si y sólo si es cierta para polinomios de grado n con coeficientes en cualquier cuerpo de característica cero algebraicamente cerrado.*

2.2. “Casi contraejemplos” a la conjetura

Un “casi contraejemplo” a la conjetura de Casas-Alvero es un polinomio que tiene una raíz en común con todas sus derivadas no constantes salvo quizás una de ellas, y sin embargo, no tiene una única raíz. En esta sección probaremos la existencia de “casi contraejemplos” a la conjetura, resultado que proviene de [7].

Proposición 2.3 *Sea $n \in \mathbb{N}$, $n \geq 2$ y sea $h \in \{1, 2, \dots, n-1\}$. Entonces existe $P_{n,h} \in \mathbb{R}[X]$ de grado n tal que*

$$\text{gr}(\text{mcd}(P_{n,h}, P_{n,h}^{(k)})) \geq 1 \quad \forall k \in \{1, 2, \dots, h-1, h+1, \dots, n-1\}$$

y $P_{n,h}$ tiene al menos dos raíces distintas.

Antes de demostrar esta proposición, probaremos algunos resultados auxiliares.

Lema 2.4 *Sea $P \in \mathbb{R}[X]$ de grado $n \in \mathbb{N}$ con todas sus raíces reales y pertenecientes a un intervalo $[a, b]$ ($a, b \in \mathbb{R}$, $a < b$), y sea m el máximo de las multiplicidades de las raíces de P . Entonces para todo $k \in \{1, 2, \dots, n-1\}$, $P^{(k)}$ tiene todas sus raíces reales y pertenecientes a $[a, b]$, y el máximo de las multiplicidades de las raíces de $P^{(k)}$ es $\text{máx}\{m-k, 1\}$.*

Demostración: Basta con probar que para $k = 1$, P' tiene todas sus raíces reales y pertenecientes a $[a, b]$, y el máximo de las multiplicidades de las raíces de P' es $\text{máx}\{m-1, 1\}$. Luego, para $k > 1$ se procede fácilmente por inducción.

Sea $P \in \mathbb{R}[X]$ de grado $n \in \mathbb{N}$ con todas sus raíces reales. Sean r_1, r_2, \dots, r_ℓ dichas raíces, con $a \leq r_1 < r_2 < \dots < r_\ell \leq b$. Para cada $j \in \{1, 2, \dots, \ell\}$ sea $m_j \in \mathbb{N}$ la multiplicidad de r_j en P ; entonces vale que $\sum_{j=1}^{\ell} m_j = n$.

Derivando este polinomio, resulta que $P'(X)$ tiene grado $n - 1$ y además r_1, r_2, \dots, r_ℓ son raíces de P' tales que para cada $j \in \{1, 2, \dots, \ell\}$ la multiplicidad de r_j en P' es $m_j - 1$.

Por otro lado, por el Teorema de Rolle existen $s_1, s_2, \dots, s_{\ell-1} \in \mathbb{R}$ raíces de P' con

$$r_j < s_j < r_{j+1}$$

para todo $j \in \{1, 2, \dots, \ell - 1\}$. Entonces hasta ahora encontramos al menos

$$\left(\sum_{j=1}^{\ell} (m_j - 1) \right) + (\ell - 1) = \sum_{j=1}^{\ell} m_j - \ell + \ell - 1 = n - 1$$

raíces de P' (contadas con multiplicidad), que tiene grado $n - 1$. Por lo tanto, éstas son todas sus raíces y podemos concluir además que $s_1, \dots, s_{\ell-1}$ son simples. Por último, como

$$a \leq r_1 < s_1 < r_2 < s_2 < r_3 < \dots < r_{\ell-1} < s_{\ell-1} < r_\ell \leq b,$$

entonces todas pertenecen al intervalo $[a, b]$. \square

Otro resultado necesario para probar la existencia de “casi contraejemplos” es lo que se conoce como el Teorema de Continuidad de las Raíces en función de los coeficientes. La demostración de este teorema que incluiremos más abajo se basa en el conocido Teorema de Rouché cuyo enunciado se exhibe a continuación.

Teorema 2.5 (de Rouché) *Sea $\mathcal{U} \subseteq \mathbb{C}$ abierto simplemente conexo y sean $f, g : \mathcal{U} \rightarrow \mathbb{C}$ funciones holomorfas en \mathcal{U} . Sea $C \subseteq \mathcal{U}$ una curva cerrada simple. Si $|f(z)| > |g(z)| \forall z \in C$ entonces f y $f + g$ tienen las mismas cantidad de raíces contadas con multiplicidad en el interior de C .*

Demostración: Ver [4, Capítulo 6, Sección 63] \square

Teorema 2.6 (de Continuidad de las Raíces) *Sea*

$$P(X) = X^n + \sum_{i=0}^{n-1} a_i X^i \in \mathbb{C}[X]$$

un polinomio de grado n ($n \in \mathbb{N}$) con ℓ raíces distintas $\alpha_1, \alpha_2, \dots, \alpha_\ell \in \mathbb{C}$ ($1 \leq \ell \leq n$), con multiplicidad m_1, m_2, \dots, m_ℓ respectivamente. Entonces para todo $\varepsilon > 0$ tal que los conjuntos $\{z \in \mathbb{C} : |z - \alpha_j| \leq \varepsilon\}$ ($j \in \{1, 2, \dots, \ell\}$) son disjuntos 2 a 2 existe $\delta > 0$ tal que todo polinomio mónico de grado n :

$$Q(X) = X^n + \sum_{i=0}^{n-1} b_i X^i \in \mathbb{C}[X]$$

que verifica que $|a_i - b_i| < \delta \forall i \in \{0, \dots, n-1\}$, tiene exactamente m_j raíces contadas con multiplicidad en $\{z \in \mathbb{C} : |z - \alpha_j| < \varepsilon\} \forall j \in \{1, 2, \dots, \ell\}$.

Demostración: Sea ε como en el enunciado. Para cada $j \in \{1, 2, \dots, \ell\}$ sea $C_j = \{z \in \mathbb{C} : |z - \alpha_j| = \varepsilon\}$ (disjuntos 2 a 2), y $\lambda_j = \min\{|P(z)| : z \in C_j\}$. Estos mínimos existen pues la función $|P(z)|$ es continua y $C_j \subseteq \mathbb{C}$ es compacto $\forall j \in \{1, 2, \dots, \ell\}$. Más aún, $\lambda_j > 0$ para todo j ya que las raíces de P , que son los puntos α_j , se encuentran fuera de los conjuntos C_j .

Ahora, para cada $j \in \{1, 2, \dots, \ell\}$ definimos $\mu_j = \max\left\{1 + \sum_{i=1}^{n-1} |z^i| : z \in C_j\right\} > 0$. Luego elegimos $\delta > 0$ tal que $\delta < \frac{\lambda_j}{\mu_j} \forall j \in \{1, 2, \dots, \ell\}$.

Entonces si $Q(X) = X^n + \sum_{i=0}^{n-1} b_i X^i$, con $b_0, b_1, \dots, b_{n-1} \in \mathbb{C}$ tales que $|a_i - b_i| < \delta \forall i \in \{0, \dots, n-1\}$, tenemos que para todo $j \in \{1, 2, \dots, \ell\}$ y para todo $z \in C_j$ vale que

$$\begin{aligned} |Q(z) - P(z)| &= |b_0 - a_0 + \sum_{i=1}^{n-1} (b_i - a_i)z^i| \leq |b_0 - a_0| + \sum_{i=1}^{n-1} |b_i - a_i||z^i| < \\ &< \delta \left(1 + \sum_{i=1}^{n-1} |z^i|\right) \leq \delta \mu_j < \lambda_j \leq |P(z)|. \end{aligned}$$

En consecuencia, por el Teorema de Rouché, P y $Q = P + (Q - P)$ tienen las mismas cantidad de raíces contadas con mutiplicidad en $\{z \in \mathbb{C} : |z - \alpha_j| < \varepsilon\} \forall j \in \{1, 2, \dots, \ell\}$. \square

A partir del Teorema de Continuidad de las Raíces, podemos obtener el siguiente resultado:

Proposición 2.7 Sea $n \in \mathbb{N}$ y sea $T_n \subseteq \mathbb{R}^n$ definido de la siguiente manera:

$$\begin{aligned} T_n &= \{(a_0, a_1, \dots, a_{n-1}) \in \mathbb{R}^n \text{ tal que } X^n + \sum_{i=0}^{n-1} a_i X^i \text{ tiene} \\ &\text{todas sus raíces reales y en el intervalo } [0, 1]\}. \end{aligned}$$

Entonces la función $\xi_n : T_n \rightarrow [0, 1]$ definida por:

$$\xi_n(a_0, a_1, \dots, a_{n-1}) = \min \left\{ \text{raíces reales de } X^n + \sum_{i=0}^{n-1} a_i X^i \right\}$$

es continua.

Demostración: Sea $(a_0, a_1, \dots, a_{n-1}) \in T_n$, $P(X) = X^n + \sum_{i=0}^{n-1} a_i X^i$ y sean $0 \leq \alpha_1 < \alpha_2 < \dots < \alpha_\ell \leq 1 \in \mathbb{R}$ las raíces de P , con multiplicidad m_1, m_2, \dots, m_ℓ respectivamente. Entonces vale que $\xi_n(a_0, a_1, \dots, a_{n-1}) = \alpha_1$.

Sea $\varepsilon > 0$. Consideramos $\varepsilon' > 0$ tal que $\varepsilon' \leq \varepsilon$ y los conjuntos $\{z \in \mathbb{C} : |z - \alpha_j| \leq \varepsilon'\}$ ($j \in \{1, 2, \dots, \ell\}$) son disjuntos 2 a 2. En particular, notemos que

$$\alpha_1 + \varepsilon' < \alpha_j - \varepsilon'$$

para todo $j \in \{2, \dots, \ell\}$.

Por el Teorema 2.6, existe $\delta > 0$ tal que si $(b_0, b_1, \dots, b_{n-1}) \in T_n$ cumple que $|a_i - b_i| < \delta \forall i \in \{0, 1, \dots, n-1\}$, el polinomio $Q(X) = X^n + \sum_{i=0}^{n-1} b_i X^i$ tiene exactamente m_j raíces

contadas con multiplicidad en $\{z \in \mathbb{C} : |z - \alpha_j| < \varepsilon'\} \forall j \in \{1, 2, \dots, \ell\}$, y como $\sum_{j=1}^{\ell} m_j = n$, Q no tiene otras raíces fuera de estos conjuntos. Además, dado que $(b_0, b_1, \dots, b_{n-1}) \in T_n$ todas las raíces de Q resultarán reales y en el intervalo $[0, 1]$. Si $\beta_1 = \xi_n(b_0, b_1, \dots, b_{n-1})$, resta demostrar que $|\alpha_1 - \beta_1| < \varepsilon$.

Por el absurdo, si $|\alpha_1 - \beta_1| \geq \varepsilon \geq \varepsilon'$, existe $j \in \{2, \dots, \ell\}$ tal que $\beta_1 \in \{z \in \mathbb{C} : |z - \alpha_j| < \varepsilon'\}$. Por otro lado, existe β raíz de Q tal que $\beta \in \{z \in \mathbb{C} : |z - \alpha_1| < \varepsilon'\}$. Finalmente tenemos que

$$\beta < \alpha_1 + \varepsilon' < \alpha_j - \varepsilon' < \beta_1,$$

contradiciendo la definición de β_1 . □

Ahora sí podemos probar el resultado principal de la sección.

Demostración de la Proposición 2.3: Si $n = 2$ y $h = 1$, cualquier polinomio $P_{n,h}$ con dos raíces distintas sirve como “casi contraejemplo”. Supongamos por lo tanto que $n \geq 3$.

Para $\vec{t} = (t_1, t_2, \dots, t_{n-2}) \in [0, 1]^{n-2}$ notamos

$$Q_{\vec{t}}(X) = X(X-1) \prod_{i=1}^{n-2} (X-t_i) \in \mathbb{R}[X]$$

y para cada $k \in \{1, 2, \dots, n-1\}$ consideramos las siguientes funciones (utilizando la notación de la Proposición 2.7):

- $\Psi_k : [0, 1]^{n-2} \rightarrow \mathbb{R}^{n-k}$ definida por $\Psi_k(\vec{t}) = (a_0, a_1, \dots, a_{n-k-1})$, donde

$$X^{n-k} + \sum_{i=0}^{n-k-1} a_i X^i = \frac{1}{n(n-1)\dots(n-k+1)} Q_{\vec{t}}^{(k)}(X).$$

Notemos que esta función es continua ya que sus coordenadas son polinomios en $(t_1, t_2, \dots, t_{n-2})$ y además, por el Lema 2.4, $\text{Im}(\Psi_k) \subseteq T_{n-k}$.

- $\sigma_k : [0, 1]^{n-2} \longrightarrow [0, 1]$ dada por la composición $\sigma_k = \xi_{n-k} \circ \Psi_k$, que resulta continua por ser composición de funciones continuas.

Por último, para cada $h \in \{1, 2, \dots, n-1\}$ consideramos la función continua $\Gamma_h : [0, 1]^{n-2} \longrightarrow [0, 1]^{n-2}$ definida por:

$$\Gamma_h(\vec{t}) = (\sigma_1(\vec{t}), \sigma_2(\vec{t}), \dots, \sigma_{h-1}(\vec{t}), \sigma_{h+1}(\vec{t}), \dots, \sigma_{n-1}(\vec{t})).$$

Por el Teorema de Punto Fijo de Brouwer (ver por ejemplo [12, Corollary 1.18]), existe $\vec{\gamma} = (\gamma_1, \gamma_2, \dots, \gamma_{n-2}) \in [0, 1]^{n-2}$ tal que $\Gamma_h(\vec{\gamma}) = \vec{\gamma}$. Definimos entonces $P_{n,h} \in \mathbb{R}[X]$ de la siguiente manera:

$$P_{n,h}(X) = Q_{\vec{\gamma}}(X) = X(X-1) \prod_{i=1}^{n-2} (X - \gamma_i).$$

Este polinomio cumple que

- $\text{gr}(P_{n,h}) = n$;
- si $k \in \{1, 2, \dots, h-1\}$, entonces γ_k verifica que $P_{n,h}(\gamma_k) = 0$ y

$$\gamma_k = \sigma_k(\vec{\gamma}) = \xi_{n-k} \circ \Psi_k(\vec{\gamma}) = \min\{\text{raíces reales de } \frac{1}{n(n-1)\dots(n-k+1)} Q_{\vec{\gamma}}^{(k)}(X)\}.$$

Luego, γ_k es una raíz real de $Q_{\vec{\gamma}}^{(k)} = P_{n,h}^{(k)}$. Esto prueba que

$$\text{gr}(\text{mcd}(P_{n,h}, P_{n,h}^{(k)})) \geq 1 \quad \forall k \in \{1, 2, \dots, h-1\};$$

- si $k \in \{h+1, h+2, \dots, n-1\}$, entonces γ_{k-1} verifica que $P_{n,h}(\gamma_{k-1}) = 0$ y

$$\gamma_{k-1} = \sigma_k(\vec{\gamma}) = \xi_{n-k} \circ \Psi_k(\vec{\gamma}) = \min\{\text{raíces reales de } \frac{1}{n(n-1)\dots(n-k+1)} Q_{\vec{\gamma}}^{(k)}(X)\}.$$

Luego γ_{k-1} es una raíz real de $Q_{\vec{\gamma}}^{(k)} = P_{n,h}^{(k)}$. Esto prueba que

$$\text{gr}(\text{mcd}(P_{n,h}, P_{n,h}^{(k)})) \geq 1 \quad \forall k \in \{h+1, h+2, \dots, n-1\}.$$

- 0 y 1 son raíces de $P_{n,h}$.

En consecuencia, $P_{n,h} \in \mathbb{R}[X]$ de grado n verifica que

$$\text{gr}(\text{mcd}(P_{n,h}, P_{n,h}^{(k)})) \geq 1 \quad \forall k \in \{1, 2, \dots, h-1, h+1, \dots, n-1\}$$

y tiene al menos dos raíces distintas (0 y 1), como queríamos demostrar. \square

2.3. Sobre el conjunto de raíces de un polinomio de Casas-Alvero

En esta sección, estudiamos diversas propiedades del conjunto de raíces de un polinomio C - A , provenientes de [2] y [7].

Para empezar, consideremos la siguiente

Definición 2.8 Sea $P \in \mathbb{C}[X]$ un polinomio C - A de grado $n \in \mathbb{N}$. Decimos que un conjunto $T \subseteq \mathbb{C}$ es un conjunto testigo para P si existe $f : \{1, \dots, n-1\} \rightarrow T$ sobreyectiva tal que para todo $k \in \{1, \dots, n-1\}$,

$$P(f(k)) = P^{(k)}(f(k)) = 0.$$

Notemos que necesariamente, un conjunto testigo para P es un conjunto formado por raíces de P . La idea detrás de esta definición es que un polinomio C - A podría tener, en principio, otras raíces además de las que intervienen en las condiciones para que el polinomio sea, en efecto, C - A .

Es claro que la conjetura es cierta si y sólo si todo conjunto testigo para un polinomio C - A tiene cardinal 1. Por otro lado, la conjetura dice que el conjunto de raíces de un polinomio C - A tiene cardinal 1. En consecuencia, en esta sección estudiaremos separadamente restricciones para el cardinal de un conjunto testigo y para el cardinal del conjunto de raíces de un polinomio C - A .

Comencemos estudiando entonces el cardinal de los conjuntos testigo.

Proposición 2.9 Sean $P \in \mathbb{C}[X]$ un polinomio C - A de grado $n \in \mathbb{N}$ y sea T un conjunto testigo para P . Entonces $\#T \neq 2$.

Demostración: Sea $f : \{1, \dots, n-1\} \rightarrow T$ sobreyectiva tal que para todo $k \in \{1, \dots, n-1\}$, $P(f(k)) = P^{(k)}(f(k)) = 0$ y supongamos por el absurdo que $\#T = 2$. Por lo visto en la Sección 1.1, podemos suponer sin pérdida de generalidad que P es mónico y que $T = \{0, 1\}$, y por lo tanto $P(0) = P(1) = 0$.

Probemos primero, por inducción decreciente en k , que para todo $k \in \{1, 2, \dots, n\}$ vale que

- $P^{(k)} \in \mathbb{R}[X]$;
- $P^{(k)} > 0$ ó $P^{(k)} < 0$ en el intervalo $(0, 1)$.

Si $k = n$, $P^{(n)} = n!$ verifica las 2 condiciones. Supongamos que lo afirmado es cierto para $k = k_0 \in \{2, 3, \dots, n\}$. Entonces tenemos que $P^{(k_0)} \in \mathbb{R}[X]$ y además $P^{(k_0)} > 0$ ó $P^{(k_0)} < 0$ en el intervalo $(0, 1)$. Luego, $P^{(k_0-1)}$ es primitiva de $P^{(k_0)}$ y, por hipótesis, $P^{(k_0-1)}(0) = 0$ ó $P^{(k_0-1)}(1) = 0$.

Esto nos permite afirmar que

$$P^{(k_0-1)}(X) = \int_0^X P^{(k_0)}(t)dt \quad \text{ó} \quad P^{(k_0-1)}(X) = \int_1^X P^{(k_0)}(t)dt,$$

con lo cual en cualquiera de los casos $P^{(k_0-1)} \in \mathbb{R}[X]$.

Además, como $P^{(k_0)} > 0$ ó $P^{(k_0)} < 0$ en el intervalo $(0, 1)$ entonces $P^{(k_0-1)}$ es estrictamente creciente ó estrictamente decreciente en el intervalo $[0, 1]$, y como $P^{(k_0-1)}(0) = 0$ ó $P^{(k_0-1)}(1) = 0$ entonces $P^{(k_0-1)} > 0$ ó $P^{(k_0-1)} < 0$ en el intervalo $(0, 1)$.

Ahora, por lo visto recién, tenemos que $P' \in \mathbb{R}[X]$ y además $P' > 0$ ó $P' < 0$ en el intervalo $(0, 1)$. Como P es primitiva de P' y $P(0) = 0$ entonces $P(X) = \int_0^X P'(t)dt \in \mathbb{R}[X]$. Pero además como $P' > 0$ ó $P' < 0$ en el intervalo $(0, 1)$ entonces P es estrictamente creciente ó estrictamente decreciente en el intervalo $[0, 1]$, y a su vez $P(0) = P(1) = 0$, lo cual es un absurdo. \square

Para probar el resto de los resultados, incluiremos primero algunas definiciones, teoremas y lemas auxiliares. Para simplificar la notación, en lo que sigue identificaremos los conjuntos \mathbb{C} y \mathbb{R}^2 de la manera habitual.

Definición 2.10 Sea $A \subseteq \mathbb{C}$ un conjunto convexo. Un vértice de A es un punto $v \in A$ que verifica la siguiente propiedad:

$$\text{para todos } v_1, v_2 \in A \text{ y } t \in (0, 1), \text{ si } tv_1 + (1-t)v_2 = v \text{ entonces } v_1 = v_2 = v.$$

Lema 2.11 Sean $A', A \subseteq \mathbb{C}$ conjuntos convexos, con $A' \subseteq A$. Si v es un vértice de A que pertenece a A' , entonces v es un vértice de A' .

Demostración: La demostración es directa a partir de la definición de vértice. \square

Lema 2.12 Si $A \subset \mathbb{C}$ es la cápsula convexa del conjunto $\{\beta_1, \beta_2, \dots, \beta_\ell\}$ y v es un vértice de A , entonces existe $i \in \{1, 2, \dots, \ell\}$ tal que $v = \beta_i$.

Demostración: Sin pérdida de generalidad, podemos suponer que $\beta_1, \beta_2, \dots, \beta_\ell$ son distintos dos a dos. Si $v \in A$ entonces $v = \sum_{j=1}^{\ell} \lambda_j \beta_j$, con $\lambda_j \in [0, 1]$ para todo $j \in \{1, 2, \dots, \ell\}$,

$\sum_{j=1}^{\ell} \lambda_j = 1$. Ahora bien, si existe $i \in \{1, 2, \dots, \ell\}$ tal que $\lambda_i = 1$ entonces para todo $j \neq i$ vale que $\lambda_j = 0$, y en consecuencia $v = \beta_i$. Supongamos entonces que existen $i, i' \in \{1, 2, \dots, \ell\}$ tales que $\lambda_i, \lambda_{i'} \in (0, 1)$ y $v = \sum_{j=1}^{\ell} \lambda_j \beta_j$. Entonces existe $\varepsilon > 0$ tal que $\lambda_i - \varepsilon, \lambda_{i'} - \varepsilon, \lambda_i + \varepsilon, \lambda_{i'} + \varepsilon \in (0, 1)$. Luego, sean

$$v_1 = \left(\sum_{\substack{1 \leq j \leq \ell \\ j \neq i, j \neq i'}} \lambda_j \beta_j \right) + (\lambda_i + \varepsilon) \beta_i + (\lambda_{i'} - \varepsilon) \beta_{i'}$$

y

$$v_2 = \left(\sum_{\substack{1 \leq j \leq \ell \\ j \neq i, j \neq i'}} \lambda_j \beta_j \right) + (\lambda_i - \varepsilon) \beta_i + (\lambda_{i'} + \varepsilon) \beta_{i'}$$

Entonces tenemos que $v_1, v_2 \in A$ y además que $v = \frac{1}{2}v_1 + \frac{1}{2}v_2$ con $v_1 \neq v_2$. En consecuencia, v no es vértice de A . \square

Notación 2.13 Sea $P \in \mathbb{C}[X]$ un polinomio de grado $n \in \mathbb{N}$ y sean $\beta_1, \beta_2, \dots, \beta_{\ell} \subseteq \mathbb{C}$ sus distintas raíces, con $1 \leq \ell \leq n$. Notaremos $A_P \subseteq \mathbb{C}$ a la cápsula convexa del conjunto de raíces de P , o sea, de $\{\beta_1, \beta_2, \dots, \beta_{\ell}\}$.

Teorema 2.14 (de Gauss-Lucas) Sea $P \in \mathbb{C}[X]$ un polinomio de grado $n \in \mathbb{N}$ y sean $\beta_1, \beta_2, \dots, \beta_{\ell}$ sus distintas raíces de multiplicidad $m_1, m_2, \dots, m_{\ell}$ respectivamente, con $1 \leq \ell \leq n$. Entonces toda raíz de P' pertenece a A_P (y en consecuencia $A_{P'} \subseteq A_P$).

Demostración: Sin pérdida de generalidad, supongamos que P es mónico. Sea $P(X) = \prod_{i=1}^{\ell} (X - \beta_i)^{m_i}$. Entonces vale que

$$P'(X) = \sum_{i=1}^{\ell} m_i (X - \beta_i)^{m_i - 1} \prod_{\substack{1 \leq j \leq \ell \\ j \neq i}} (X - \beta_j)^{m_j}.$$

Ahora bien, sea $z \in \mathbb{C}$ una raíz de P' . Si z también es raíz de P entonces $z = \beta_i$ para algún $i \in \{1, 2, \dots, \ell\}$ y por lo tanto $z \in A_P$. Supongamos entonces que $P(z) \neq 0$; entonces vale que

$$\frac{P'(z)}{P(z)} = 0,$$

$$\frac{\sum_{i=1}^{\ell} \left(m_i (z - \beta_i)^{m_i-1} \prod_{\substack{1 \leq j \leq \ell \\ j \neq i}} (z - \beta_j)^{m_j} \right)}{\prod_{i=1}^{\ell} (z - \beta_i)^{m_i}} = 0$$

y por lo tanto

$$\sum_{i=1}^{\ell} \frac{m_i}{z - \beta_i} = 0.$$

Considerando que $\frac{m_i}{z - \beta_i} = \frac{m_i(\bar{z} - \bar{\beta}_i)}{|z - \beta_i|^2}$ para todo $i \in \{1, 2, \dots, \ell\}$ tenemos que

$$\sum_{i=1}^{\ell} \frac{m_i(\bar{z} - \bar{\beta}_i)}{|z - \beta_i|^2} = 0,$$

con lo cual, si conjugamos ambos miembros de la última igualdad nos queda que

$$\sum_{i=1}^{\ell} \frac{m_i(z - \beta_i)}{|z - \beta_i|^2} = 0.$$

Entonces resulta que

$$\left(\sum_{i=1}^{\ell} \frac{m_i}{|z - \beta_i|^2} \right) z = \sum_{i=1}^{\ell} \frac{m_i}{|z - \beta_i|^2} \beta_i$$

Si llamamos $\lambda_i = \frac{\frac{m_i}{|z - \beta_i|^2}}{\sum_{i=1}^{\ell} \frac{m_i}{|z - \beta_i|^2}}$ nos queda que $z = \sum_{i=1}^{\ell} \lambda_i \beta_i$, donde $\lambda_i \in [0, 1] \forall i \in$

$\{1, 2, \dots, \ell\}$ y $\sum_{i=1}^{\ell} \lambda_i = 1$. Por lo tanto, $z \in A_P$. □

Como consecuencia de este teorema, podemos enunciar el siguiente

Corolario 2.15 *Sea $P \in \mathbb{C}[X]$ un polinomio de grado $n \in \mathbb{N}$, $\{\beta_1, \beta_2, \dots, \beta_\ell\}$ sus raíces distintas entre sí de multiplicidad m_1, m_2, \dots, m_ℓ respectivamente, con $1 \leq \ell \leq n$. Si β_i es vértice de A_P , entonces $P^{(k)}(\beta_i) \neq 0 \forall k \in \{m_i, m_i + 1, \dots, n - 1\}$.*

Demostración: Por el absurdo, si existe $k \in \{m_i, m_i + 1, \dots, n - 1\}$ tal que $P^{(k)}(\beta_i) = 0$, entonces $\beta_i \in A_{P^{(k)}}$. Como consecuencia del Teorema 2.14, $A_{P^{(k)}} \subseteq A_{P^{(m_i)}}$, y por lo tanto $\beta_i \in A_{P^{(m_i)}}$. Luego, como β_i es vértice de A_P y $A_{P^{(m_i)}} \subseteq A_P$ entonces por el Lema 2.11, β_i es vértice de $A_{P^{(m_i)}}$ y por lo tanto, por el Lema 2.12, β_i es raíz de $P^{(m_i)}$. Esto es un absurdo pues β_i es raíz de P de multiplicidad m_i , con lo cual $P^{(m_i)}(\beta_i) \neq 0$. □

Ahora sí podemos probar el segundo resultado de la sección referido al cardinal de los conjuntos testigo.

Proposición 2.16 Sean $P \in \mathbb{C}[X]$ un polinomio C-A de grado $n \in \mathbb{N}$ y sea T un conjunto testigo para P . Entonces $\#T \neq n - 1$.

Demostración: Sea $f : \{1, \dots, n - 1\} \rightarrow T$ sobreyectiva tal que para todo $k \in \{1, \dots, n - 1\}$, $P(f(k)) = P^{(k)}(f(k)) = 0$, y notemos $\alpha_k = f(k)$. Supongamos entonces por el absurdo que $T = \{\alpha_1, \alpha_2, \dots, \alpha_{n-1}\}$ tiene cardinal $n - 1$. Entonces tenemos que $\alpha_k \neq \alpha_h \forall k, h \in \{1, 2, \dots, n - 1\}$ con $k \neq h$.

Por lo visto en la Sección 1.1, podemos suponer sin pérdida de generalidad que P es mónico. Como $P(\alpha_1) = P'(\alpha_1) = 0$ resulta que α_1 es raíz doble de P , con lo cual

$$P(X) = (X - \alpha_1)^2 \prod_{k=2}^{n-1} (X - \alpha_k).$$

Ahora bien, es claro que A_P tiene al menos 2 vértices, y en consecuencia al menos uno de ellos será una raíz simple de P . Si llamamos α_i a dicho vértice, entonces $i \in \{2, 3, \dots, n - 1\}$; luego, por el Corolario 2.15 $P^{(k)}(\alpha_i) \neq 0 \forall k \in \{1, 2, \dots, n - 1\}$ ya que α_i es raíz simple de P . Entonces $P^{(i)}(\alpha_i) \neq 0$, lo que es un absurdo pues $P(\alpha_k) = P^{(k)}(\alpha_k) = 0 \forall k \in \{1, 2, \dots, n - 1\}$. \square

A partir de ahora, nos enfocaremos en estudiar restricciones sobre el cardinal del conjunto de raíces de un polinomio C-A.

Antes veamos un lema auxiliar.

Lema 2.17 Sean $n, m \in \mathbb{N}$, con $m \leq n$. Entonces

$$\sum_{k=m}^n (-1)^k \binom{n}{k} = (-1)^m \binom{n-1}{m-1}.$$

Demostración: Sabemos que para todo $k, n \in \mathbb{N}$, $k < n$ vale $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$.

Luego, tenemos que

$$\begin{aligned}
 \sum_{k=m}^n (-1)^k \binom{n}{k} &= (-1)^n \binom{n}{n} + \sum_{k=m}^{n-1} (-1)^k \left(\binom{n-1}{k-1} + \binom{n-1}{k} \right) \\
 &= (-1)^n + \sum_{k=m}^{n-1} (-1)^k \binom{n-1}{k-1} - \sum_{k=m}^{n-1} (-1)^{k+1} \binom{n-1}{k} \\
 &= (-1)^n + \sum_{k=m}^{n-1} (-1)^k \binom{n-1}{k-1} - \underbrace{\sum_{h=m+1}^n (-1)^h \binom{n-1}{h-1}}_{h=k+1} \\
 &= (-1)^n + (-1)^m \binom{n-1}{m-1} - (-1)^n \binom{n-1}{n-1} \\
 &= (-1)^m \binom{n-1}{m-1}
 \end{aligned}$$

□

Ahora enunciemos y demostremos la siguiente

Proposición 2.18 *Sea $P \in \mathbb{C}[X]$ un polinomio C-A de grado $n \in \mathbb{N}$, sean $\beta_1, \beta_2, \dots, \beta_\ell$ sus distintas raíces de multiplicidad m_1, m_2, \dots, m_ℓ respectivamente, con $1 \leq \ell \leq n$. Si $\ell \geq 2$ entonces P tiene al menos 2 raíces distintas que no son vértices de A_P .*

Demostración: Supongamos primero que todas las raíces de P son vértices de A_P . Sea m el máximo de m_1, \dots, m_ℓ ; como $\ell \geq 2$ entonces $m \leq n-1$ y, por lo visto en el Corolario 2.15, $P^{(m)}(\beta_i) \neq 0 \forall i \in \{1, 2, \dots, \ell\}$, con lo cual P y $P^{(m)}$ no tienen raíces comunes, lo que es un absurdo pues P es un polinomio C-A.

Supongamos, de ahora en más, que hay exactamente una raíz de P que no es vértice de A_P . Por lo visto en la Sección 1.1 podemos suponer sin pérdida de generalidad que P es mónico y que $\beta_\ell = 0$ es dicha raíz. Si m es el máximo de $m_1, \dots, m_{\ell-1}$, entonces tenemos que $1 \leq m \leq n-1$ y, por lo visto en el Corolario 2.15, $P^{(k)}(\beta_i) \neq 0 \forall i \in \{1, 2, \dots, \ell-1\}$ y $\forall k \in \{m, m+1, \dots, n-1\}$.

Como P es un polinomio C-A, para todo $k \in \{m, m+1, \dots, n-1\}$ debe ocurrir que $P^{(k)}(0) = 0$, es decir que 0 es una raíz de $P^{(k)}$ de multiplicidad al menos $n-k$. En consecuencia, como P es mónico y $\text{gr}(P^{(k)}) = n-k$, resulta que

$$P^{(k)}(X) = \frac{n!}{(n-k)!} X^{n-k} \quad \forall k \in \{m, m+1, \dots, n-1\}. \quad (2.3)$$

Ahora bien, sin pérdida de generalidad supongamos que β_1 tiene multiplicidad m . Entonces $P^{(k)}(\beta_1) = 0 \forall k \in \{0, 1, \dots, m-1\}$ ($P^{(0)} = P$). Mirando el polinomio de Taylor de P

centrado en β_1 , resulta que

$$P(X) = \sum_{k=0}^n \frac{P^{(k)}(\beta_1)}{k!} (X - \beta_1)^k = \sum_{k=m}^n \frac{P^{(k)}(\beta_1)}{k!} (X - \beta_1)^k.$$

Evaluando en $X = 0$, resulta que

$$0 = P(0) = \sum_{k=m}^n \frac{P^{(k)}(\beta_1)}{k!} (-\beta_1)^k.$$

De la ecuación (2.3), nos queda que

$$\begin{aligned} 0 &= \sum_{k=m}^n \binom{n}{k} (\beta_1)^{n-k} (-\beta_1)^k, \\ 0 &= (\beta_1)^n \sum_{k=m}^n (-1)^k \binom{n}{k}, \\ 0 &= (\beta_1)^n (-1)^m \binom{n-1}{m-1}, \end{aligned}$$

por el Lema 2.17. En consecuencia $\beta_1 = 0$, que es un absurdo.

Por lo tanto, concluimos que deben existir al menos 2 raíces de P que no son vértices de A_P . \square

Como consecuencia de esta proposición, haremos la siguiente

Observación 2.19 *Todo polinomio C-A en $\mathbb{C}[X]$ con más de una raíz tiene al menos 4 raíces distintas en \mathbb{C} . En efecto, tomando $P \in \mathbb{C}[X]$ un polinomio C-A con más de una raíz en \mathbb{C} y mirando la cápsula convexa de sus raíces A_P , entonces P tiene al menos 2 raíces que son vértices de A_P y, por lo demostrado en la Proposición 2.18, al menos 2 que no lo son. Luego, P tiene al menos 4 raíces distintas.*

Para finalizar el capítulo, probemos la siguiente proposición que muestra que, en realidad, un polinomio C-A que no tenga una única raíz tiene al menos 5 raíces distintas:

Proposición 2.20 *Sea $P \in \mathbb{C}[X]$ un polinomio un polinomio C-A con más de una raíz en \mathbb{C} . Entonces P tiene al menos 5 raíces distintas en \mathbb{C} .*

Demostración: Como mencionamos en la Introducción, la conjetura de Casas-Alvero está demostrada para polinomios de grado menor o igual que 7 (ver [6]). Luego, si P es un polinomio de grado n , podemos suponer $n \geq 8$.

Por la Observación 2.19, basta con ver que si $P \in \mathbb{C}[X]$ es un polinomio un polinomio C - A con más de una raíz, entonces no puede tener exactamente 4 raíces distintas.

Supongamos, por el absurdo, que existe $P \in \mathbb{C}[X]$ polinomio C - A de grado $n \in \mathbb{N}$ con exactamente 4 raíces en \mathbb{C} . Es claro que al menos 2 de ellas son vértices de A_P , y por la Proposición 2.18, al menos dos de ellas no son vértices de A_P . Por lo tanto, tenemos que A_P tiene exactamente 2 vértices, con lo cual es un segmento en \mathbb{C} . Por lo visto en la Sección 1.1, podemos suponer que P es mónico y que sus 4 raíces son reales, por lo que $P \in \mathbb{R}[X]$.

Llamemos m al máximo de las multiplicidades de estas 4 raíces; entonces vale que $2 \leq m \leq n - 3$. Analicemos varios casos:

1. Si $m \leq n - 5$, nuevamente por lo visto en la Sección 1.1 podemos suponer que las 4 raíces de P son $a < 0 < 1 < b$. Como a y b son vértices de A_P , por el Corolario 2.15 no pueden ser raíces de $P^{(k)}$ para ningún $k \in \{m, m + 1, \dots, n - 1\}$; luego podemos suponer además que $P^{(n-1)}(0) = 0$. Más aún, por el Lema 2.4, para $k \in \{m, m + 1, \dots, n - 1\}$ las raíces de $P^{(k)}$ son simples; entonces necesariamente tenemos que

$$P^{(n-1)}(0) = P^{(n-2)}(1) = P^{(n-3)}(0) = P^{(n-4)}(1) = P^{(n-5)}(0) = 0.$$

Luego, teniendo en cuenta que P es mónico, resulta que

$$P^{(n-1)} = n!X, \quad P^{(n-2)} = \frac{n!}{2}(X^2 - 1), \quad P^{(n-3)} = \frac{n!}{6}(X^3 - 3X), \quad P^{(n-4)} = \frac{n!}{24}(X^4 - 6X^2 + 5)$$

y

$$P^{(n-5)} = \frac{n!}{120}(X^5 - 10X^3 + 25X) = \frac{n!}{120}X(X^2 - 5)^2,$$

que no tiene todas sus raíces simples, lo que es un absurdo.

2. Si $m = n - 4$, nuevamente por lo visto en la Sección 1.1 podemos suponer, sin pérdida de generalidad, que las 4 raíces de P son $a < 0 < b < 1$ y, de manera similar al ítem anterior, que

$$P^{(n-1)}(0) = P^{(n-2)}(b) = P^{(n-3)}(0) = P^{(n-4)}(b) = 0.$$

En consecuencia, como P es mónico podemos afirmar que

$$P^{(n-1)} = n!X, \quad P^{(n-2)} = \frac{n!}{2}(X^2 - b^2), \quad P^{(n-3)} = \frac{n!}{6}(X^3 - 3b^2X)$$

y

$$P^{(n-4)} = \frac{n!}{24}(X^4 - 6b^2X^2 + 5b^4) = \frac{n!}{24}(X^2 - 5b^2)(X^2 - b^2).$$

Por el Teorema 2.14 sabemos que $[-\sqrt{5}b, \sqrt{5}b] = A_{P^{(n-4)}} \subseteq A_P = [a, 1]$, pero además, como a y 1 son vértices de A_P , por el Corolario 2.15, sabemos que no son raíces de $P^{(n-4)}$, con lo que concluimos que $A_{P^{(n-4)}} \subseteq (a, 1)$, y en consecuencia

$$a < -\sqrt{5}b < -b.$$

Ahora bien, si llamamos m_a , m_0 , m_b y m_1 a las multiplicidades de a , 0 , b y 1 respectivamente tenemos que estos valores son 1 , 1 , 2 y $n-4$ en algún orden. Además, como $P^{(n-4)}(b) = 0$, entonces $m_b \neq n-4$.

Por otro lado, supongamos $P(X) = X^n + \sum_{i=0}^{n-1} a_i X^i$. Las condiciones $P^{(n-1)}(0) = P^{(n-3)}(0) = 0$ implican $a_{n-1} = a_{n-3} = 0$, y luego podemos concluir que

$$m_a a + m_b b + m_1 = -a_{n-1} = 0 \quad (2.4)$$

y

$$m_a a^3 + m_b b^3 + m_1 = -3a_{n-3} + 3a_{n-1}a_{n-2} - a_{n-1}^3 = 0, \quad (2.5)$$

de lo que se deduce que

$$m_a a(a^2 - 1) = m_b b(1 - b^2). \quad (2.6)$$

Como $m_b b(1 - b^2) > 0$ y $a < 0$ entonces también vale que $-1 < a$; luego

$$m_a > -am_a = m_b b + m_1 > m_1.$$

Esto implica además que $m_a \geq 2 \geq m_1$.

Consideremos dos casos:

- a) Si $m_a = 2$ entonces $m_b = m_1 = 1$ y $m_0 = n-4$. De las ecuaciones (2.4) y (2.5) resulta que

$$2a + b + 1 = 2a^3 + b^3 + 1 = 0,$$

con lo cual

$$2a^3 + (-1 - 2a)^3 + 1 = -6a(a+1)^2 = 0,$$

lo que es un absurdo.

- b) Si $m_a = n-4$ entonces en la ecuación (2.6) tenemos que

$$(-a)(1 - a^2) = \frac{m_b}{n-4} b(1 - b^2) < b(1 - b^2).$$

Como la función $\phi : \mathbb{R} \rightarrow \mathbb{R}$ definida por $\phi(t) = t(1 - t^2)$ es estrictamente creciente en $[0, \frac{1}{\sqrt{3}}]$ y $0 < b < -a$, entonces necesariamente $-a > \frac{1}{\sqrt{3}}$. Volviendo a la ecuación (2.4), nos queda que

$$n-4 = m_b \frac{b}{-a} + m_1 \frac{1}{-a} < \frac{m_b}{\sqrt{5}} + m_1 \sqrt{3} \leq \frac{1}{\sqrt{5}} + 2\sqrt{3} < 4,$$

ya que $\{m_b, m_1\} \subseteq \{1, 2\}$ pero no puede ser que sean simultáneamente $m_b = 2$ y $m_1 = 2$. Esto es un absurdo pues estamos suponiendo que $n \geq 8$.

3. Si $m = n - 3$, procedemos de manera similar a los casos anteriores. Por lo visto en la Sección 1.1 podemos suponer, sin pérdida de generalidad, que las 4 raíces de P son $a < 0 < b < 1$ y que

$$P^{(n-1)}(0) = P^{(n-2)}(b) = P^{(n-3)}(0) = 0.$$

En consecuencia, como P es mónico podemos afirmar que

$$P^{(n-1)} = n!X, \quad P^{(n-2)} = \frac{n!}{2}(X^2 - b^2), \quad P^{(n-3)} = \frac{n!}{6}(X^3 - 3b^2X)$$

Por el Teorema 2.14 sabemos que $[-\sqrt{3b}, \sqrt{3b}] = A_{P^{(n-3)}} \subseteq A_P = [a, 1]$, pero además, como a y 1 son vértices de A_P , por el Corolario 2.15, sabemos que no son raíces de $P^{(n-3)}$, con lo que concluimos que $A_{P^{(n-3)}} \subseteq (a, 1)$, y en consecuencia

$$a < -\sqrt{3b} < -b.$$

Si llamamos nuevamente m_a, m_0, m_b y m_1 a las multiplicidades de $a, 0, b$ y 1 respectivamente tenemos que estos valores son 1, 1, 1 y $n - 3$ en algún orden.

De manera análoga al caso anterior, de las condiciones $P^{(n-1)}(0) = P^{(n-3)}(0) = 0$ podemos concluir que

$$m_a a + m_b b + m_1 = 0 \tag{2.7}$$

y

$$m_a a^3 + m_b b^3 + m_1 = 0,$$

de lo que se deduce que

$$m_a a(a^2 - 1) = m_b b(1 - b^2), \tag{2.8}$$

y como $m_b b(1 - b^2) > 0$ y $a < 0$ entonces también vale que $-1 < a$; luego

$$m_a > -a m_a = m_b b + m_1 > m_1.$$

Esto implica que $m_a = n - 3$ y $m_0 = m_b = m_1 = 1$.

De la ecuación (2.8) tenemos que

$$(-a)(1 - a^2) = \frac{1}{n-3} b(1 - b^2) < b(1 - b^2).$$

Como la función $\phi : \mathbb{R} \rightarrow \mathbb{R}$ definida por $\phi(t) = t(1 - t^2)$ es estrictamente creciente en $[0, \frac{1}{\sqrt{3}}]$ y $0 < b < -a$, entonces necesariamente $-a > \frac{1}{\sqrt{3}}$.

Volviendo a la ecuación (2.7), nos queda que

$$n - 3 = \frac{b}{-a} + \frac{1}{-a} < \frac{1}{\sqrt{3}} + \sqrt{3} < 3,$$

lo que es un absurdo pues estamos suponiendo que $n \geq 8$.

□

Capítulo 3

La conjetura en infinitos grados

En este capítulo estudiaremos uno de los avances más importantes que se conocen en torno a la resolución de la Conjetura de Casas-Alvero, que es la veracidad de la conjetura para infinitos grados. Este resultado proviene originalmente de [8], pero el desarrollo que seguiremos aquí será el realizado en [7].

3.1. Valuaciones

En esta sección incluiremos algunos resultados introductorios relacionados con la teoría de valuaciones. Los mismos son centrales en el desarrollo del capítulo.

Definición 3.1 *Sea \mathbb{K} un cuerpo. Una valuación sobre \mathbb{K} es una función $v : \mathbb{K} \rightarrow \mathbb{R} \cup \{+\infty\}$ que verifica las siguientes propiedades:*

- (i) $v^{-1}(\{+\infty\}) = \{0\}$;
- (ii) $v(\alpha\alpha') = v(\alpha) + v(\alpha') \quad \forall \alpha, \alpha' \in \mathbb{K}$;
- (iii) $v(\alpha + \alpha') \geq \min\{v(\alpha), v(\alpha')\} \quad \forall \alpha, \alpha' \in \mathbb{K}$.

Ejemplos 3.2

1. Si \mathbb{K} es cuerpo, la función $v_0 : \mathbb{K} \rightarrow \mathbb{R} \cup \{+\infty\}$ tal que

- $v_0(0) = +\infty$,
- $v_0(\alpha) = 0 \quad \forall \alpha \in \mathbb{K} \setminus \{0\}$.

es valuación, la cual denominaremos valuación trivial o nula sobre \mathbb{K} .

2. Para todo $p \in \mathbb{N}$ primo, las valuaciones p -ádicas $v_p : \mathbb{Q} \rightarrow \mathbb{R} \cup \{+\infty\}$ definidas por

- $v_p(0) = +\infty$,
- si $n \in \mathbb{Z}$, entonces $v_p(n) = \max\{k \in \mathbb{N}_0 : p^k | n\}$,
- si $q = \frac{a}{b} \in \mathbb{Q}$ ($a, b \in \mathbb{Z}$, $b \neq 0$), entonces $v_p(q) = v_p(a) - v_p(b)$.

son valuaciones sobre \mathbb{Q} .

Observación 3.3 En toda valuación $v : \mathbb{K} \rightarrow \mathbb{R} \cup \{+\infty\}$ valen las siguientes propiedades:

- $v(1) = v(-1) = 0$ y $v(\alpha) = v(-\alpha) \forall \alpha \in \mathbb{K}$;
- $v(\alpha^n) = n \cdot v(\alpha) \forall \alpha \in \mathbb{K} \setminus \{0\}$ y $\forall n \in \mathbb{Z}$.

Comencemos estudiando algunas propiedades relacionadas con valuaciones.

Proposición 3.4 Sea \mathbb{K} un cuerpo y sea $v : \mathbb{K} \rightarrow \mathbb{R} \cup \{+\infty\}$ una valuación no trivial. Si definimos

- $\mathbf{R} = \{\alpha \in \mathbb{K} : v(\alpha) \geq 0\}$,
- $\mathbf{M} = \{\alpha \in \mathbb{K} : v(\alpha) > 0\}$,
- $\mathcal{K} = \mathbf{R}/\mathbf{M}$,

entonces vale que

- (i) \mathbf{R} es un subanillo propio de \mathbb{K} ;
- (ii) \mathbf{M} es el único ideal maximal de \mathbf{R} ;
- (iii) \mathcal{K} es un cuerpo algebraicamente cerrado si \mathbb{K} lo es.

Demostración:

- (i)
 - Como $v(0) = +\infty$ y $v(1) = v(-1) = 0$ entonces $0, 1, -1 \in \mathbf{R}$;
 - si $\alpha \in \mathbf{R}$ entonces $v(\alpha) \geq 0$; luego $v(-\alpha) = v(\alpha) \geq 0$, con lo cual $-\alpha \in \mathbf{R}$;

- si $\alpha, \alpha' \in \mathbf{R}$ entonces $v(\alpha) \geq 0$ y $v(\alpha') \geq 0$. Luego $v(\alpha + \alpha') \geq \min\{v(\alpha), v(\alpha')\} \geq 0$ y $v(\alpha\alpha') = v(\alpha) + v(\alpha') \geq 0$, por lo que $\alpha + \alpha', \alpha\alpha' \in \mathbf{R}$.

En consecuencia, \mathbf{R} es un subanillo de \mathbb{K} . Como v no es la valuación trivial, existe $\alpha \in \mathbb{K} \setminus \{0\}$ tal que $v(\alpha) \neq 0$. Si $v(\alpha) < 0$, entonces $\alpha \in \mathbb{K} \setminus \mathbf{R}$, con lo cual \mathbf{R} es propio; y si $v(\alpha) > 0$, entonces $v(\alpha^{-1}) = -v(\alpha) < 0$ y por lo tanto $\alpha^{-1} \in \mathbb{K} \setminus \mathbf{R}$, con lo cual \mathbf{R} es propio.

- (ii)
- Como $v(0) = +\infty$ entonces $0 \in \mathbf{M}$;
 - si $\beta, \beta' \in \mathbf{M}$ entonces $v(\beta) > 0$ y $v(\beta') > 0$. Luego $v(\beta + \beta') \geq \min\{v(\beta), v(\beta')\} > 0$, por lo que $\beta + \beta' \in \mathbf{M}$;
 - si $\beta \in \mathbf{M}$ y $\alpha \in \mathbf{R}$ entonces $v(\beta) > 0$ y $v(\alpha) \geq 0$. Luego $v(\beta\alpha) = v(\beta) + v(\alpha) > 0$, y en consecuencia $\beta\alpha \in \mathbf{M}$.

Por lo tanto, \mathbf{M} es un ideal de \mathbf{R} . Además, como $v(1) = 0$ entonces $1 \in \mathbf{R} \setminus \mathbf{M}$, por lo que \mathbf{M} es propio.

Sea ahora $\alpha \in \mathbf{R} \setminus \mathbf{M}$. Entonces $\alpha \neq 0$, $v(\alpha) = 0$ y $v(\alpha^{-1}) = -v(\alpha) = 0$, con lo cual $\alpha^{-1} \in \mathbf{R}$, y en consecuencia α es una unidad de \mathbf{R} . Esto nos permite concluir que \mathbf{M} es el único ideal maximal de \mathbf{R} .

- (iii) Es claro que \mathcal{K} es cuerpo ya que \mathbf{M} es un ideal maximal de \mathbf{R} . Veamos que \mathcal{K} es algebraicamente cerrado si \mathbb{K} lo es.

Sean $n \in \mathbb{N}$, $a_0, a_1, \dots, a_{n-1} \in \mathbf{R}$ y consideramos

$$P(X) = X^n + \sum_{i=0}^{n-1} a_i X^i \in \mathbf{R}[X] \subset \mathbb{K}[X] \quad \text{y} \quad Q(X) = X^n + \sum_{i=0}^{n-1} \bar{a}_i X^i \in \mathcal{K}[X].$$

Queremos probar que Q tiene una raíz en \mathcal{K} : como \mathbb{K} es algebraicamente cerrado, sean $\alpha_1, \alpha_2, \dots, \alpha_n \in \mathbb{K}$ las raíces de $P(X)$. Entonces vale que

$$\alpha_1 \alpha_2 \dots \alpha_n = (-1)^n a_0.$$

Aplicando v a esta igualdad, resulta que

$$\sum_{i=1}^n v(\alpha_i) = v((-1)^n) + v(a_0) = v(a_0) \geq 0$$

pues $a_0 \in \mathbf{R}$. Luego, existe i_0 tal que $v(\alpha_{i_0}) \geq 0$ y en consecuencia $\alpha_{i_0} \in \mathbf{R}$, $\bar{\alpha}_{i_0} \in \mathcal{K}$ y $Q(\bar{\alpha}_{i_0}) = \overline{P(\alpha_{i_0})} = \bar{0} = 0$.

□

Una herramienta fundamental para obtener el resultado principal al final del capítulo es un teorema de suma importancia, que consiste en la existencia de un cuerpo algebraicamente cerrado que extiende a \mathbb{Q} , usualmente llamado “los complejos p -ádicos” y notado \mathbb{C}_p , para el cual es posible extender la valuación v_p con ciertas propiedades de completitud (ver por ejemplo [9, Chapter III]). Este resultado es de hecho el punto de partida de lo que se conoce como “análisis p -ádico”. A su vez, es posible probar que el cuerpo \mathbb{C}_p es isomorfo a \mathbb{C} como extensión de \mathbb{Q} (ver [10, Remark 7.41]), con lo cual se puede pensar por simplicidad que la extensión de la valuación v_p está definida directamente sobre \mathbb{C} .

En resumidas cuentas, tenemos el siguiente

Teorema 3.5 *Para todo $p \in \mathbb{N}$ primo, existe $w_p : \mathbb{C} \rightarrow \mathbb{R} \cup \{+\infty\}$ valuación sobre \mathbb{C} que extiende a v_p , es decir $w_p|_{\mathbb{Q}} = v_p$.*

Observación 3.6 *Para simplificar la lectura del resto del capítulo, haremos el abuso de notación de llamar también v_p a la extensión $w_p : \mathbb{C} \rightarrow \mathbb{R} \cup \{+\infty\}$ del teorema anterior.*

Además, llamaremos respectivamente \mathbf{R}_p , \mathbf{M}_p y \mathcal{K}_p al anillo, ideal maximal y cuerpo cociente definidos como en la Proposición 3.4 cuando se considera concretamente la valuación $v_p : \mathbb{C} \rightarrow \mathbb{R} \cup \{+\infty\}$.

Lema 3.7 *El cuerpo \mathcal{K}_p tiene característica p y es algebraicamente cerrado.*

Demostración: En efecto, tenemos que

$$\underbrace{\bar{1} + \cdots + \bar{1}}_{p \text{ veces}} = \bar{p} = 0$$

ya que $v_p(p) = 1 > 0$ por lo cual $p \in \mathbf{M}_p$. Por otro lado, por la Proposición 3.4, \mathcal{K}_p es algebraicamente cerrado ya que \mathbb{C} lo es. \square

Antes de terminar la sección, incluimos el siguiente lema auxiliar que nos servirá más adelante.

Lema 3.8 *Sean $n, m, p \in \mathbb{N}$ tales que p es primo y $n \geq m$. Entonces:*

$$(i) \binom{n}{m} \equiv \binom{np^e}{mp^e}(p) \quad \forall e \in \mathbb{N}_0;$$

$$(ii) \text{ si } v_p(n) > v_p(m) \text{ entonces } p \mid \binom{n}{m}.$$

Demostración:

(i) Si $e = 0$ es trivial. Luego alcanza con probarlo para $e = 1$, pues de este modo si $e \geq 2$, inductivamente tenemos que

$$\binom{n}{m} \equiv \binom{np}{mp} \equiv \binom{np^2}{mp^2} \equiv \dots \equiv \binom{np^{e-1}}{mp^{e-1}} \equiv \binom{np^e}{mp^e} (p).$$

Para el caso $e = 1$, tenemos que

$$\begin{aligned} \binom{np}{mp} &= \frac{(np)!}{(mp)!((n-m)p)!} = \frac{\prod_{k=0}^{n-1} \left(\prod_{i=1}^p kp + i \right)}{\prod_{k=0}^{m-1} \left(\prod_{i=1}^p kp + i \right) \cdot \prod_{k=0}^{n-m-1} \left(\prod_{i=1}^p kp + i \right)} = \\ &= \frac{\prod_{k=1}^n kp \cdot \prod_{k=0}^{n-1} \left(\prod_{i=1}^{p-1} kp + i \right)}{\prod_{k=1}^m kp \cdot \prod_{k=0}^{m-1} \left(\prod_{i=1}^{p-1} kp + i \right) \cdot \prod_{k=1}^{n-m} kp \cdot \prod_{k=0}^{n-m-1} \left(\prod_{i=1}^{p-1} kp + i \right)} = \\ &= \frac{p^n \cdot n! \cdot \prod_{k=0}^{n-1} \left(\prod_{i=1}^{p-1} kp + i \right)}{p^m \cdot m! \cdot \prod_{k=0}^{m-1} \left(\prod_{i=1}^{p-1} kp + i \right) \cdot p^{n-m} \cdot (n-m)! \cdot \prod_{k=0}^{n-m-1} \left(\prod_{i=1}^{p-1} kp + i \right)} = \\ &= \binom{n}{m} \frac{\prod_{k=0}^{n-1} \left(\prod_{i=1}^{p-1} kp + i \right)}{\prod_{k=0}^{m-1} \left(\prod_{i=1}^{p-1} kp + i \right) \cdot \prod_{k=0}^{n-m-1} \left(\prod_{i=1}^{p-1} kp + i \right)}. \end{aligned}$$

En consecuencia, tenemos que

$$\begin{aligned} \binom{np}{mp} - \binom{n}{m} &= \binom{n}{m} \cdot \left(\frac{\prod_{k=0}^{n-1} \left(\prod_{i=1}^{p-1} kp + i \right)}{\prod_{k=0}^{m-1} \left(\prod_{i=1}^{p-1} kp + i \right) \cdot \prod_{k=0}^{n-m-1} \left(\prod_{i=1}^{p-1} kp + i \right)} - 1 \right) = \\ &= \binom{n}{m} \cdot \frac{\prod_{k=0}^{n-1} \left(\prod_{i=1}^{p-1} kp + i \right) - \prod_{k=0}^{m-1} \left(\prod_{i=1}^{p-1} kp + i \right) \cdot \prod_{k=0}^{n-m-1} \left(\prod_{i=1}^{p-1} kp + i \right)}{\prod_{k=0}^{m-1} \left(\prod_{i=1}^{p-1} kp + i \right) \cdot \prod_{k=0}^{n-m-1} \left(\prod_{i=1}^{p-1} kp + i \right)}. \end{aligned}$$

Como $\binom{np}{mp}, \binom{n}{m} \in \mathbb{Z}$, alcanza con ver que $v_p \left(\binom{np}{mp} - \binom{n}{m} \right) \geq 1$:

$$\begin{aligned} v_p \left(\binom{np}{mp} - \binom{n}{m} \right) &= v_p \left(\binom{n}{m} \right) + \\ &+ v_p \left(\prod_{k=0}^{n-1} \left(\prod_{i=1}^{p-1} kp + i \right) - \prod_{k=0}^{m-1} \left(\prod_{i=1}^{p-1} kp + i \right) \cdot \prod_{k=0}^{n-m-1} \left(\prod_{i=1}^{p-1} kp + i \right) \right) - \\ &- v_p \left(\prod_{k=0}^{m-1} \left(\prod_{i=1}^{p-1} kp + i \right) \cdot \prod_{k=0}^{n-m-1} \left(\prod_{i=1}^{p-1} kp + i \right) \right). \end{aligned}$$

Por el Teorema de Wilson sabemos que $\forall k \in \mathbb{Z}$, $\prod_{i=1}^{p-1} (kp + i) \equiv (p-1)! \equiv -1 \pmod{p}$, por lo cual,

$$\forall j \in \mathbb{N}, \prod_{k=0}^{j-1} \left(\prod_{i=1}^{p-1} kp + i \right) \equiv (-1)^j \pmod{p}.$$

Esto implica que:

- $\prod_{k=0}^{n-1} \left(\prod_{i=1}^{p-1} kp + i \right) \equiv (-1)^n \pmod{p}$;
- $\prod_{k=0}^{m-1} \left(\prod_{i=1}^{p-1} kp + i \right) \cdot \prod_{k=0}^{n-m-1} \left(\prod_{i=1}^{p-1} kp + i \right) \equiv (-1)^m \cdot (-1)^{n-m} \equiv (-1)^n \pmod{p}$.

Luego,

$$\prod_{k=0}^{n-1} \left(\prod_{i=1}^{p-1} kp + i \right) - \prod_{k=0}^{m-1} \left(\prod_{i=1}^{p-1} kp + i \right) \cdot \prod_{k=0}^{n-m-1} \left(\prod_{i=1}^{p-1} kp + i \right) \equiv (-1)^n - (-1)^n \equiv 0 \pmod{p}.$$

Por lo tanto, tenemos que

$$\begin{aligned} v_p \left(\binom{np}{mp} - \binom{n}{m} \right) &= v_p \left(\underbrace{\binom{n}{m}}_{\geq 0} \right) + \\ &+ v_p \left(\underbrace{\left(\prod_{k=0}^{n-1} \left(\prod_{i=1}^{p-1} kp + i \right) - \prod_{k=0}^{m-1} \left(\prod_{i=1}^{p-1} kp + i \right) \cdot \prod_{k=0}^{n-m-1} \left(\prod_{i=1}^{p-1} kp + i \right) \right)}_{\geq 1} \right) - \\ &- v_p \left(\underbrace{\left(\prod_{k=0}^{m-1} \left(\prod_{i=1}^{p-1} kp + i \right) \cdot \prod_{k=0}^{n-m-1} \left(\prod_{i=1}^{p-1} kp + i \right) \right)}_{=0} \right) \geq 1, \end{aligned}$$

que era lo que queríamos demostrar.

(ii) Para esta parte usaremos que $\forall t \in \mathbb{N} \ v_p(t!) = \sum_{i=1}^{\infty} \left[\frac{t}{p^i} \right]$. Al igual que en el ítem anterior, como $\binom{n}{m} \in \mathbb{Z}$ basta con ver que $v_p\left(\binom{n}{m}\right) \geq 1$:

$$\begin{aligned} v_p\left(\binom{n}{m}\right) &= v_p\left(\frac{n!}{m!(n-m)!}\right) = v_p(n!) - v_p(m!) - v_p((n-m)!) = \\ &= \sum_{i=1}^{\infty} \left[\frac{n}{p^i} \right] - \sum_{i=1}^{\infty} \left[\frac{m}{p^i} \right] - \sum_{i=1}^{\infty} \left[\frac{n-m}{p^i} \right] = \sum_{i=1}^{\infty} \left(\left[\frac{n}{p^i} \right] - \left[\frac{m}{p^i} \right] - \left[\frac{n-m}{p^i} \right] \right). \end{aligned}$$

Por un lado, tenemos que $\frac{n}{p^i} = \frac{m}{p^i} + \frac{n-m}{p^i}$ para todo $i \in \mathbb{N}$. Además, si $k = v_p(n)$ y $h = v_p(m)$ entonces $n = p^k a$ con $(a, p) = 1$ y $m = p^h b$ con $(b, p) = 1$. Como $k > h$, tenemos que $n - m = p^h(p^{k-h}a - b)$, donde $p \mid p^{k-h}a$ y $p \nmid b$. Por lo tanto vale que $v_p(n - m) = h$ y entonces $\frac{n}{p^k} = \frac{m}{p^k} + \frac{n-m}{p^k}$, con $\frac{n}{p^k} \in \mathbb{Z}$ y $\frac{m}{p^k}, \frac{n-m}{p^k} \in \mathbb{R} \setminus \mathbb{Z}$.

Luego, teniendo en cuenta que $[\alpha] + [\beta] \leq [\alpha + \beta] \leq [\alpha] + [\beta] + 1$ si $\alpha, \beta \in \mathbb{R}$ y que $[\alpha + \beta] = [\alpha] + [\beta] + 1$ si $\alpha + \beta \in \mathbb{Z}$ y $\alpha, \beta \notin \mathbb{Z}$, en la última expresión nos queda que

$$\begin{aligned} v_p\left(\binom{n}{m}\right) &= \sum_{i=1}^{\infty} \left(\left[\frac{n}{p^i} \right] - \left[\frac{m}{p^i} \right] - \left[\frac{n-m}{p^i} \right] \right) = \\ &= \left(\sum_{\substack{i=1 \\ i \neq k}}^{\infty} \underbrace{\left(\left[\frac{n}{p^i} \right] - \left[\frac{m}{p^i} \right] - \left[\frac{n-m}{p^i} \right] \right)}_{\geq 0 \ \forall i \in \mathbb{N} \setminus \{k\}} \right) + \underbrace{\left(\left[\frac{n}{p^k} \right] - \left[\frac{m}{p^k} \right] - \left[\frac{n-m}{p^k} \right] \right)}_{=1} \geq 1. \end{aligned}$$

□

3.2. La conjetura en característica p

En esta sección analizaremos lo que sucede en relación a la Conjetura de Casas-Alvero cuando se consideran cuerpos de característica p ($p \in \mathbb{N}$ primo). Sorprendentemente, los resultados obtenidos en estos cuerpos servirán para obtener conclusiones sobre la conjetura para el caso de cuerpos de característica 0, que es el contexto original de interés.

Para empezar y a modo de ejemplo, veamos algunos polinomios en $\mathbb{K}[X]$, donde \mathbb{K} es un cuerpo de característica p .

Ejemplo 3.9

1. $P_1(X) = X^n$ ($n \in \mathbb{N}$): en este caso, es claro que el polinomio P_1 tiene una raíz en común con cada una de sus derivadas hasta orden $n - 1$, y también que tiene al 0 como única raíz;
2. $P_2(X) = X^{p^2} - X^p$: en este caso, el polinomio P_2 tiene todas sus derivadas hasta orden $p^2 - 1$ nulas, y por lo tanto tiene al 0 o al 1 como raíz común con cada una de sus derivadas pertinentes, y sin embargo no tiene una única raíz;
3. $P_3(X) = X^{p+1} - X^p$: aquí tenemos que $P_3'(X) = (p+1)X^p$ y $P_3''(X) = 0$, con lo cual todas las derivadas a partir de la de orden 2 hasta la de orden p son nulas y por lo tanto este polinomio tiene a 0 como raíz común con cada una de sus derivadas hasta orden p , pero no tiene una única raíz ya que 1 también lo es.

El Ejemplo 3.9 sugiere que el hecho de que las derivadas sean idénticamente nulas es un problema para la conjetura en característica p . Un intento de salvar este inconveniente es mediante las derivadas de Hass, cuya definición incluimos a continuación. Si bien este concepto no servirá para hacer un planteo general de la conjetura en característica p , será útil de todos modos para resultados posteriores.

Definición 3.10 Sea \mathbb{K} un cuerpo, $P(X) = \sum_{i=0}^n a_i X^i \in \mathbb{K}[X]$ polinomio de grado n ($n \in \mathbb{N}$). Para $k \in \{1, 2, \dots, n-1\}$, definimos la derivada de Hass de orden k como el siguiente polinomio:

$$H_{(k)}(P)(X) = \sum_{i=k}^n \binom{i}{k} a_i X^{i-k}.$$

Observación 3.11

(i) Si $k \in \{1, 2, \dots, n-1\}$, entonces tenemos que

$$\begin{aligned} k! \cdot H_{(k)}(P)(X) &= k! \cdot \sum_{i=k}^n \binom{i}{k} a_i X^{i-k} = \\ &= \sum_{i=k}^n i(i-1)(i-2) \dots (i-k+1) a_i X^{i-k} = P^{(k)}(X), \end{aligned}$$

con lo cual $H_{(k)}(P) \mid P^{(k)} \forall k \in \{1, 2, \dots, n-1\}$. Esto en particular implica que si $H_{(k)}(P)$ es el polinomio nulo, entonces $P^{(k)}$ también será el polinomio nulo. Además, si \mathbb{K} es un cuerpo de característica p y $k < p$ entonces tenemos que $k! \neq 0$ y por lo tanto

$$H_{(k)}(P)(X) = (k!)^{-1} P^{(k)}(X).$$

(ii) Para la derivada de Hass, no vale que $H_{(k)}(H_{(k')}(P)) = H_{(k+k')}(P)$: por ejemplo, si $P(X) = X^3 \in \mathbb{Z}_2[X]$, tenemos que

$$H_{(1)}(P) = X^2,$$

$$H_{(1)}(H_{(1)}(P)) = 0$$

pero

$$H_{(2)}(P) = X,$$

con lo cual $H_{(1)}(H_{(1)}(P)) \neq H_{(2)}(P)$.

Habiendo introducido este nuevo concepto, analicemos qué ocurre con los mismos ejemplos que vimos anteriormente cuando se considera la derivada de Hass en un cuerpo de característica p .

Revisión del Ejemplo 3.9

1. En cuanto al polinomio $P_1(X) = X^n$, para $k \in \{1, 2, \dots, n-1\}$ tenemos que

$$H_{(k)}(P_1)(X) = \binom{n}{k} X^{n-k}.$$

Nuevamente, es claro que el polinomio P_1 tiene una raíz en común con cada una de sus derivadas de Hass hasta orden $n-1$, y también que tiene una única raíz;

2. si ahora analizamos el polinomio $P_2(X) = X^{p^2} - X^p$, tenemos que

$$H_{(p)}(P_2)(X) = \binom{p^2}{p} X^{p^2-p} - 1 = -1$$

(ya que por el Lema 3.8 (ii) $\binom{p^2}{p} = 0$), con lo cual $H_{(p)}(P_2)$ no tiene raíces y por ende no comparte raíz con P_2 ;

3. si ahora analizamos el polinomio $P_3 = X^{p+1} - X^p$, tenemos que

$$H_{(1)}(P_3)(X) = (p+1)X^p = X^p,$$

$$H_{(k)}(P_3)(X) = \binom{p+1}{k} X^{p+1-k} - \binom{p}{k} X^{p-k} = 0 \quad \forall k \in \{2, 3, \dots, p-1\}$$

y

$$H_{(p)}(P_3)(X) = X - 1.$$

Luego, $\alpha = 0$ es raíz común entre $P_3(X)$ y $H_{(k)}(P_3)(X) \quad \forall k \in \{1, 2, \dots, p-1\}$ y $\alpha = 1$ es raíz compartida entre $P_3(X)$ y $H_{(p)}(P_3)(X)$. Sin embargo, P_3 no tiene una única raíz.

Tras haber analizado algunos ejemplos considerando tanto la derivada tradicional como la de Hass notamos que, dado que a veces la derivada tradicional es el polinomio nulo mientras que la de Hass no lo es, entonces la condición de tener una raíz en común con cada una de las derivadas de Hass hasta orden $n - 1$ es más restrictiva (como ocurre en el caso del polinomio P_2). Aún así, existen polinomios con una raíz en común con cada una de las derivadas de Hass hasta orden $n - 1$ pero que no tienen una única raíz (como ocurre en el caso del polinomio P_3).

No obstante, si bien esto dice que la derivada de Hass no es “suficientemente buena” como para llevar la conjetura a característica p en general, será de suma importancia para los resultados que aparecen en el resto del capítulo.

Definición 3.12 *Sea $p \in \mathbb{N}$ primo, \mathbb{K} un cuerpo de característica p , $P(X) \in \mathbb{K}[X]$ un polinomio de grado $n \in \mathbb{N}$. Decimos que P es un polinomio de Casas-Alvero, o simplemente un polinomio C-A si y sólo si existen $\alpha_1, \alpha_2, \dots, \alpha_{n-1} \in \overline{\mathbb{K}}$ que verifican:*

$$P(\alpha_k) = H_{(k)}(P)(\alpha_k) = 0 \quad \forall k \in \{1, 2, \dots, n - 1\}.$$

Por ejemplo, bajo esta nueva definición los polinomios P_1 y P_3 del Ejemplo 3.9 son polinomios C-A y el polinomio P_2 del mismo ejemplo no lo es.

Enunciado de la Conjetura de Casas-Alvero en característica p : Sea \mathbb{K} un cuerpo de característica p . Si $P(X) \in \mathbb{K}[X]$ un polinomio C-A, entonces P tiene una única raíz en $\overline{\mathbb{K}}$.

Tenemos entonces que el polinomio P_1 del Ejemplo 3.9 es un polinomio C-A que satisface la conjetura, mientras que el polinomio P_3 del mismo ejemplo es un polinomio C-A que no la satisface.

Esto pone de manifiesto que la Conjetura de Casas-Alvero en característica p es falsa si se la considera en forma general. Sin embargo, el resultado principal en la sección siguiente se basa en estudiar, para cada $m \in \mathbb{N}$ fijo, los valores de $p \in \mathbb{N}$ primo tales que la conjetura de Casas-Alvero es cierta para polinomios de grado m en un cuerpo de característica p .

De hecho, para algunos valores de m hacemos este análisis a continuación.

Antes, hagamos algunas observaciones.

Observación 3.13 *Sea \mathbb{K} un cuerpo de característica p y sea $P(X) \in \mathbb{K}[X]$ un polinomio C-A. Al igual que lo analizado en la Sección 1.1 podemos suponer, en caso de ser necesario, que \mathbb{K} es algebraicamente cerrado, P es mónico y que una de las raíces del mismo es algún valor de \mathbb{K} elegido previamente.*

Observación 3.14 Sea \mathbb{K} un cuerpo de característica p y sean $P \in \mathbb{K}[X]$, $\alpha \in \overline{\mathbb{K}}$ tales que

$$P(X) = (X - \alpha)^\ell Q(X)$$

con $\ell \in \mathbb{N}$ y $Q(\alpha) \neq 0$. Para $k \in \mathbb{N}_0$, tenemos que

$$P^{(k)}(X) = \sum_{i=0}^k \binom{k}{i} ((X - \alpha)^\ell)^{(i)} Q^{(k-i)}(X),$$

de lo que se deduce que $P(\alpha) = P'(\alpha) = \dots = P^{(\ell-1)}(\alpha) = 0$ y $P^{(\ell)}(\alpha) = \ell! Q(\alpha)$. Luego, si $\ell < p$ tenemos que α es una raíz de multiplicidad ℓ si y sólo si $P(\alpha) = P'(\alpha) = \dots = P^{(\ell-1)}(\alpha) = 0$ y $P^{(\ell)}(\alpha) \neq 0$. En cambio, si $\ell \geq p$, no puede deducirse la multiplicidad a partir de la anulación de las derivadas.

Empecemos ahora sí con el análisis mencionado anteriormente:

Lema 3.15 La conjetura de Casas-Alvero es cierta para polinomios de grado 1 y 2 con coeficientes en un cuerpo de característica p , para todo $p \in \mathbb{N}$ primo.

Demostración: Si P tiene grado 1 no hay nada que probar puesto que los polinomios de grado 1 tienen una única raíz.

Sea ahora $P \in \mathbb{K}[X]$ un polinomio $C-A$ de grado 2 con \mathbb{K} cuerpo de característica p . Por la Observación 3.13, podemos suponer que \mathbb{K} es algebraicamente cerrado, P es mónico y $\alpha = 0$ es raíz común entre P y $H_{(1)}(P)$. Entonces si $P(X) = X^2 + aX + b$ con $a, b \in \mathbb{K}$, $H_{(1)}(P)(X) = 2X + a$. Como $P(0) = 0$ tenemos que $b = 0$, y como $H_{(1)}(P)(0) = 0$ tenemos que $a = 0$; luego $P(X) = X^2$, que tiene una única raíz. \square

Lema 3.16 La conjetura de Casas-Alvero es cierta para polinomios de grado 3 con coeficientes en un cuerpo de característica p si y sólo si $p \geq 3$.

Demostración: Sea $P \in \mathbb{K}[X]$ un polinomio $C-A$ de grado 3, con \mathbb{K} cuerpo de característica $p \geq 3$. Nuevamente, por la Observación 3.13, podemos suponer que \mathbb{K} es algebraicamente cerrado, P es mónico y $\alpha_2 = 0$ es raíz común entre P y $H_{(2)}(P)$. Entonces, similarmente al lema previo, también podemos suponer que $P(X) = X^3 + aX$, $H_{(1)}(P)(X) = 3X^2 + a$ y $H_{(2)}(P)(X) = 3X$ con $a \in \mathbb{K}$.

Si $p = 3$ entonces $H_{(1)}(P)(X) = a$ y por lo tanto, para que P y $H_{(1)}(P)$ compartan una raíz debe ocurrir que $a = 0$, con lo cual $P(X) = X^3$, que tiene una única raíz.

Si $p \geq 5$, sea α_1 la raíz común entre P y $H_{(1)}(P)$. Si $\alpha_1 = 0$, por las Observaciones 3.11 (i) y 3.14, entonces la multiplicidad de 0 como raíz de P es 3 y en consecuencia P

tiene una única raíz triple. Supongamos por lo tanto que $\alpha_1 \neq 0$; entonces α_1 es raíz de $H_{(1)}(P)(X) = 3X^2 + a$, con lo cual

$$3\alpha_1^2 + a = 0$$

y $\alpha_1 \neq 0$ es raíz de $P(X) = X^3 + aX$, con lo cual

$$\alpha_1^2 + a = 0.$$

Esto implica que $2\alpha_1^2 = 0$, que es un absurdo pues $p \geq 5$.

Para el caso $p = 2$ consideremos el polinomio $P(X) = X^3 + X \in \mathbb{Z}_2[X]$. Entonces $H_{(1)}(P) = X^2 + 1$ y $H_{(2)}(P) = X$, por lo cual $\alpha_1 = 1$ es raíz común entre P y $H_{(1)}(P)$ y $\alpha_2 = 0$ es raíz común entre P y $H_{(2)}(P)$ y en consecuencia P es un polinomio C - A de grado 3 con dos raíces distintas (0 y 1). \square

Para el siguiente lema utilizaremos un concepto clásico en la teoría de ecuaciones polinomiales que introducimos a continuación.

Definición 3.17 Sea \mathbb{K} un cuerpo y sean $P(X) = \sum_{i=0}^n a_i X^i, Q(X) = \sum_{i=0}^m b_i X^i \in \mathbb{K}[X]$ polinomios de grado n y m respectivamente. La matriz de Sylvester de P y Q es la matriz

$$\text{Syl}(P, Q) = \begin{pmatrix} a_n & a_{n-1} & \dots & a_1 & a_0 & 0 & \dots & \dots & 0 \\ 0 & a_n & a_{n-1} & \dots & a_1 & a_0 & 0 & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & \ddots & & \ddots & \ddots & 0 \\ 0 & \dots & \dots & 0 & a_n & a_{n-1} & \dots & a_1 & a_0 \\ b_m & b_{m-1} & \dots & b_0 & 0 & \dots & \dots & \dots & 0 \\ 0 & b_m & b_{m-1} & \dots & b_0 & 0 & \dots & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & & \ddots & \ddots & & \vdots \\ \vdots & & \ddots & \ddots & \ddots & & \ddots & \ddots & \vdots \\ \vdots & & & \ddots & \ddots & \ddots & & \ddots & 0 \\ 0 & \dots & \dots & \dots & 0 & b_m & b_{m-1} & \dots & b_0 \end{pmatrix} \in \mathbb{K}^{(n+m) \times (n+m)}$$

(las primeras m filas contienen los coeficientes de P y las últimas n filas contienen los coeficientes de Q). La resultante entre P y Q , $\text{Res}(P, Q)$ es el determinante de $\text{Syl}(P, Q)$.

Teorema 3.18 Sea \mathbb{K} un cuerpo y sean $P, Q \in \mathbb{K}[X]$ polinomios no constantes. Entonces P y Q tienen una raíz en común en $\overline{\mathbb{K}}$ si y sólo si $\text{Res}(P, Q) = 0$.

Demostración: Ver por ejemplo [5, Chapter 3, Section 6, Proposition 1]. \square

Lema 3.19 *La conjetura de Casas-Alvero es cierta para polinomios de grado 4 con coeficientes en un cuerpo de característica p si y sólo si $p = 2$ ó $p \geq 11$.*

Demostración: Sea $P \in \mathbb{K}[X]$ un polinomio C-A de grado 4, con \mathbb{K} cuerpo de característica p . Nuevamente, por la Observación 3.13, podemos suponer que \mathbb{K} es algebraicamente cerrado, P es mónico y $\alpha_3 = 0$ es raíz común entre P y $H_{(3)}(P)$. Entonces, similarmente a los lemas previos, también podemos suponer que $P(X) = X^4 + aX^2 + bX$, $H_{(1)}(P)(X) = 4X^3 + 2aX + b$, $H_{(2)}(P)(X) = 6X^2 + a$ y $H_{(3)}(P)(X) = 4X$ con $a, b \in \mathbb{K}$.

Si $p = 2$ entonces $H_{(1)}(P) = b$ y $H_{(2)}(P) = a$. En consecuencia, para que P comparta raíz con $H_{(1)}(P)$ y $H_{(2)}(P)$ debe ocurrir que $a = b = 0$, con lo cual $P(X) = X^4$, que tiene una única raíz.

Si $p \geq 11$, analizando resultantes tenemos que

$$\text{Res}(P, H_{(1)}(P)) = \det \begin{pmatrix} 1 & 0 & a & b & 0 & 0 & 0 \\ 0 & 1 & 0 & a & b & 0 & 0 \\ 0 & 0 & 1 & 0 & a & b & 0 \\ 4 & 0 & 2a & b & 0 & 0 & 0 \\ 0 & 4 & 0 & 2a & b & 0 & 0 \\ 0 & 0 & 4 & 0 & 2a & b & 0 \\ 0 & 0 & 0 & 4 & 0 & 2a & b \end{pmatrix} = 0$$

y

$$\text{Res}(P, H_{(2)}(P)) = \det \begin{pmatrix} 1 & 0 & a & b & 0 & 0 \\ 0 & 1 & 0 & a & b & 0 \\ 6 & 0 & a & 0 & 0 & 0 \\ 0 & 6 & 0 & a & 0 & 0 \\ 0 & 0 & 6 & 0 & a & 0 \\ 0 & 0 & 0 & 6 & 0 & a \end{pmatrix} = 0.$$

Esto equivale al siguiente sistema de ecuaciones:

$$\begin{cases} -b^2(4a^3 + 27b^2) = 0 \\ a(25a^3 + 216b^2) = 0 \end{cases}.$$

Analicemos, entonces, varios casos:

1. Si $a = 0$ entonces $27b^4 = 0$, con lo cual, como $p \neq 3$, vale que $b = 0$ y $P(X) = X^4$, que tiene una única raíz;

2. si $b = 0$ entonces $25a^4 = 0$, con lo cual, como $p \neq 5$, vale que $a = 0$ y $P(X) = X^4$, que tiene una única raíz;
3. si $a, b \neq 0$ entonces tenemos que

$$\begin{cases} 4a^3 + 27b^2 = 0 \\ 25a^3 + 216b^2 = 0 \end{cases},$$

que es un sistema lineal de ecuaciones respecto de (a^3, b^2) con coeficientes en \mathbb{K} . Para que el mismo tenga solución $(a^3, b^2) \neq (0, 0)$ debe ocurrir que

$$\det \begin{pmatrix} 4 & 27 \\ 25 & 216 \end{pmatrix} = 0,$$

es decir que $4 \cdot 216 - 27 \cdot 25 = 189 = 3^3 \cdot 7 = 0$, lo cual no ocurre ya que $p \geq 11$.

Por último veamos que, efectivamente, si $p = 3, 5$ ó 7 existen polinomios C - A de grado 4 con coeficientes en un cuerpo de característica p que tienen al menos dos raíces distintas:

- Si $p = 3$, consideramos $P(X) = X^4 - X \in \mathbb{Z}_3[X]$. Entonces $H_{(1)}(P)(X) = X^3 - 1$, $H_{(2)}(P)(X) = 0$ y $H_{(3)}(P)(X) = X$, con lo cual $P(0) = H_{(2)}(P)(0) = H_{(3)}(P)(0) = 0$ y $P(1) = H_{(1)}(P)(1) = 0$ y por lo tanto P es un polinomio C - A de grado 4 con al menos dos raíces distintas (0 y 1);
- si $p = 5$, consideramos $P(X) = X^4 - X^2 \in \mathbb{Z}_5[X]$. Entonces $H_{(1)}(P)(X) = 4X^3 - 2X$, $H_{(2)}(P)(X) = X^2 - 1$ y $H_{(3)}(P)(X) = 4X$, con lo cual $P(0) = H_{(1)}(P)(0) = H_{(3)}(P)(0) = 0$ y $P(1) = H_{(2)}(P)(1) = 0$ y por lo tanto P es un polinomio C - A de grado 4 con al menos dos raíces distintas (0 y 1);
- si $p = 7$, consideramos $P(X) = X^4 + X^2 - 2X \in \mathbb{Z}_7[X]$. Entonces $H_{(1)}(P)(X) = 4X^3 + 2X - 2$, $H_{(2)}(P)(X) = 6X^2 + 1$ y $H_{(3)}(P)(X) = 4X$, con lo cual $P(0) = H_{(3)}(P)(0) = 0$, $P(1) = H_{(2)}(P)(0) = 0$ y $P(3) = H_{(1)}(P)(3) = 0$, por lo que P es un polinomio C - A de grado 4 con al menos tres raíces distintas (0, 1 y 3).

□

A continuación se incluyen los últimos dos lemas auxiliares sobre la conjetura en característica p que necesitaremos antes de probar el resultado principal en la sección siguiente.

Lema 3.20 Sean $m, p \in \mathbb{N}$ con p primo, $e \in \mathbb{N}_0$ y sea $n = mp^e$. Sea \mathbb{K} un cuerpo de característica p y sea $P(X) = \sum_{i=0}^n a_i X^i \in \mathbb{K}[X]$ un polinomio C - A de grado n . Entonces para todo $i \in \{0, 1, \dots, n\}$ tal que $p^e \nmid i$ vale que $a_i = 0$.

Demostración: Si $e = 0$ no hay nada que probar, por lo que podemos suponer que $e \in \mathbb{N}$. Probaremos que para todo $i \in \{0, 1, \dots, n\}$ vale: $p^e | i$ ó $a_i = 0$, por inducción decreciente en i :

- $i = n$: trivial pues $p^e | n$;
- sea $i_0 \in \{0, 1, \dots, n - 1\}$ y supongamos que el lema es cierto $\forall i \in \mathbb{N}$, $i_0 < i \leq n$. Probémoslo para $i = i_0$:

Si $p^e | i_0$ no hay nada que probar. Supongamos por lo tanto que $p^e \nmid i_0$. Entonces tenemos que:

$$H_{(i_0)}(P)(X) = \sum_{h=i_0}^n \binom{h}{i_0} a_h X^{h-i_0}.$$

Consideremos dos casos:

1. Si $i_0 < h \leq n$ y $p^e \nmid h$ entonces por hipótesis inductiva, $a_h = 0$;
2. Si $i_0 < h \leq n$ y $p^e | h$, como $p^e \nmid i_0$ entonces $v_p(h) > v_p(i_0)$ y por el Lema 3.8 (ii), $p \mid \binom{h}{i_0} \implies \binom{h}{i_0} = 0$.

Por lo tanto, para todo $h \in \{i_0 + 1, i_0 + 2, \dots, n\}$ tenemos que $\binom{h}{i_0} a_h = 0$. Luego, tenemos que $H_{(i_0)}(P)(X) = \sum_{h=i_0}^n \binom{h}{i_0} a_h X^{h-i_0} = a_{i_0}$.

En consecuencia, como $H_{(i_0)}(P)(X)$ tiene una raíz (que es común con $P(X)$) debe ocurrir que $a_{i_0} = 0$.

□

Lema 3.21 Sean $m, p \in \mathbb{N}$ con p primo y $e \in \mathbb{N}_0$. Sea \mathbb{K} un cuerpo de característica p , $Q(X) \in \mathbb{K}[X]$ un polinomio de grado m y $P(X) = (Q(X))^{p^e}$. Si $P(X)$ es un polinomio C-A, entonces $Q(X)$ también lo es.

Demostración: Si $e = 0$ no hay nada que probar, por lo que podemos suponer que $e \in \mathbb{N}$.

Para empezar, probemos que para todo $k \in \{1, 2, \dots, m-1\}$, $H_{(kp^e)}(P)(X) = (H_{(k)}(Q)(X))^{p^e}$.

Sea $Q(X) = \sum_{i=0}^m a_i X^i$, $a_m \neq 0$. Entonces para todo $k \in \{1, 2, \dots, m-1\}$:

$$H_{(k)}(Q)(X) = \sum_{i=k}^m \binom{i}{k} a_i X^{i-k}.$$

Por otro lado, tenemos que

$$P(X) = \left(\sum_{i=0}^m a_i X^i \right)^{p^e} = \sum_{i=0}^m a_i^{p^e} X^{ip^e} = \sum_{j=0}^{mp^e} b_j X^j,$$

donde

$$b_j = \begin{cases} a_i^{p^e} & \text{si } i = \frac{j}{p^e} \in \mathbb{N}_0, \\ 0 & \text{si } p^e \nmid j. \end{cases}$$

Luego, si $k \in \{1, 2, \dots, m-1\}$ vale que

$$\begin{aligned} H_{(kp^e)}(P)(X) &= \sum_{j=kp^e}^{mp^e} \binom{j}{kp^e} b_j X^{j-kp^e} \\ &= \sum_{i=k}^m \binom{ip^e}{kp^e} a_i^{p^e} X^{(i-k)p^e}. \end{aligned}$$

Por lo visto en el Lema 3.8 (i), $\binom{ip^e}{kp^e} \equiv \binom{i}{k} (p)$ por lo cual en \mathbb{K} vale que $\binom{ip^e}{kp^e} = \binom{i}{k}$.

En consecuencia,

$$H_{(kp^e)}(P)(X) = \sum_{i=k}^m \binom{i}{k} a_i^{p^e} X^{(i-k)p^e} = \left(\sum_{i=k}^m \binom{i}{k} a_i X^{i-k} \right)^{p^e} = (H_{(k)}(Q)(X))^{p^e},$$

como queríamos probar.

Luego, si $P(X)$ es un polinomio C - A , para todo $k \in \{1, 2, \dots, m-1\}$ existe $\alpha_k \in \overline{\mathbb{K}}$ tal que

$$P(\alpha_k) = H_{(kp^e)}(P)(\alpha_k) = 0.$$

Pero entonces tenemos que

$$(Q(\alpha_k))^{p^e} = (H_{(k)}(Q)(\alpha_k))^{p^e} = 0$$

con lo cual

$$Q(\alpha_k) = H_{(k)}(Q)(\alpha_k) = 0,$$

lo que demuestra que $Q \in \mathbb{K}[X]$ también es un polinomio C - A . \square

3.3. Resultado principal

En esta última sección, y en base a todo lo hecho anteriormente, probaremos la conjetura para infinitos grados. El resultado fundamental que nos permitirá hacer esto, es el siguiente

Teorema 3.22 Sean $m, p \in \mathbb{N}$ con p primo, $e \in \mathbb{N}_0$ y sea $n = mp^e$. Si la conjetura de Casas-Alvero es cierta para polinomios de grado m con coeficientes en un cuerpo de característica p , entonces la conjetura de Casas-Alvero es cierta para polinomios de grado n con coeficientes en \mathbb{C} .

Antes de probar este teorema, recalquemos que por lo expuesto en las Secciones 1.1 y 2.1, esto implica a su vez que la conjetura es cierta para polinomios de grado n con coeficientes en cualquier cuerpo de característica 0.

Demostración: Por el absurdo, supongamos que existe $P(X) = \lambda(X - \alpha_0)(X - \alpha_1) \dots (X - \alpha_{n-1}) \in \mathbb{C}[X]$ polinomio C - A de grado n con al menos 2 raíces distintas ($\lambda \neq 0$).

Por lo visto en la Sección 1.1, podemos suponer $\lambda = 1$ y $\alpha_0 = 0$, y en consecuencia

$$P(X) = X(X - \alpha_1)(X - \alpha_2) \dots (X - \alpha_{n-1}),$$

con $\alpha_{i_0} \neq 0$ para algún $i_0 \in \{1, 2, \dots, n-1\}$.

De acuerdo al Teorema 3.5 y la Observación 3.6, sea v_p la extensión sobre \mathbb{C} de la valuación p -ádica sobre \mathbb{Q} . Sin pérdida de generalidad supongamos que $v_p(\alpha_{n-1})$ es mínimo; entonces $\alpha_{n-1} \neq 0$, pues sabíamos que $\alpha_{i_0} \neq 0$ para algún $i_0 \in \{1, 2, \dots, n-1\}$ con lo cual $v_p(\alpha_{n-1}) \leq v_p(\alpha_{i_0}) < v_p(0) = +\infty$.

En consecuencia, $T(X) = \frac{P(\alpha_{n-1}X)}{\alpha_{n-1}^n} = X(X-1)(X-\gamma_1)(X-\gamma_2) \dots (X-\gamma_{n-2}) \in \mathbb{C}[X]$ es un polinomio C - A , con $\gamma_i = \frac{\alpha_i}{\alpha_{n-1}} \forall i \in \{1, 2, \dots, n-2\}$.

Si ahora consideramos en \mathbb{C} , como indica la Observación 3.6, los conjuntos \mathbf{R}_p y \mathbf{M}_p , resulta que $v_p(\gamma_i) = v_p(\alpha_i) - v_p(\alpha_{n-1}) \geq 0 \forall i \in \{1, 2, \dots, n-2\}$, con lo cual $\gamma_i \in \mathbf{R}_p$, y por lo tanto tenemos que $T(X) \in \mathbf{R}_p[X]$. Luego, también de acuerdo con la Observación 3.6, si consideramos el cuerpo $\mathcal{K}_p = \mathbf{R}_p/\mathbf{M}_p$, que por el Lema 3.7 tiene característica p , entonces

$$\bar{T}(X) = X(X - \bar{1})(X - \bar{\gamma}_1)(X - \bar{\gamma}_2) \dots (X - \bar{\gamma}_{n-2}) \in \mathcal{K}_p[X]$$

es un polinomio C - A de acuerdo a la Definición 3.12 ya que si $\gamma \in \mathbb{C}$ es raíz común entre T y $T^{(k)}$ ($k \in \{1, 2, \dots, n-1\}$) entonces γ es raíz común entre T y $H_{(k)}(T)$, y por ende $\bar{\gamma} \in \mathcal{K}_p$ es raíz común entre \bar{T} y $H_{(k)}(\bar{T})$. Observemos además que $\bar{T}(\bar{0}) = \bar{T}(\bar{1}) = \bar{0}$, con $\bar{0} \neq \bar{1}$.

Por lo tanto, por el Lema 3.20, si $\bar{T}(X) = X^n + \sum_{i=1}^{n-1} \bar{c}_i X^i$ con $c_i \in \mathbf{R}_p$, tenemos que $\bar{c}_i = \bar{0}$

$\forall i \in \{1, 2, \dots, n-1\}$, $p^e \nmid i$. Luego, tenemos que

$$\bar{T}(X) = X^n + \sum_{i=1}^{n-1} \bar{c}_i X^i = X^{mp^e} + \sum_{j=1}^{m-1} \bar{c}_{jp^e} X^{jp^e}.$$

Como \mathcal{K}_p es algebraicamente cerrado, $\forall j \in \{1, 2, \dots, m-1\}$ existe $d_j \in \mathbf{R}_p$ tal que \bar{d}_j es raíz de $X^{p^e} - \bar{c}_{jp^e} \in \mathcal{K}_p[X]$, con lo cual $(\bar{d}_j)^{p^e} = \bar{c}_{jp^e}$. Por lo tanto, tenemos que

$$\bar{T}(X) = X^{mp^e} + \sum_{j=1}^{m-1} (\bar{d}_j)^{p^e} X^{jp^e} = \left(X^m + \sum_{j=1}^{m-1} \bar{d}_j X^j \right)^{p^e}.$$

Luego, si llamamos $\bar{U}(X) = X^m + \sum_{j=1}^{m-1} \bar{d}_j X^j$, resulta que $\bar{U}(X) \in \mathcal{K}_p[X]$ es un polinomio mónico de grado m , con $\bar{T}(X) = (\bar{U}(X))^{p^e}$. Por el Lema 3.21, como $\bar{T}(X)$ es un polinomio C - A entonces $\bar{U}(X)$ también lo es.

Dado que vale que

$$\bar{T}(\bar{0}) = \bar{T}(\bar{1}) = \bar{0},$$

podemos concluir que

$$(\bar{U}(\bar{0}))^{p^e} = (\bar{U}(\bar{1}))^{p^e} = \bar{0}$$

con lo cual

$$\bar{U}(\bar{0}) = \bar{U}(\bar{1}) = \bar{0},$$

y en consecuencia $\bar{U}(X)$ es un polinomio C - A de grado m con coeficientes en \mathcal{K}_p (cuerpo de característica p) con al menos dos raíces distintas ($\bar{0}$ y $\bar{1}$), lo cual es un absurdo dado que estamos suponiendo que la Conjetura de Casas-Alvero es cierta para polinomios de grado m con coeficientes en cuerpos de característica p . \square

A partir de este último teorema, podemos enunciar ahora el teorema principal del capítulo.

Teorema 3.23 (Resultado principal) *Si $n \in \mathbb{N}$ puede escribirse como $n = mp^e$ con $m \in \{1, 2, 3, 4\}$, $p \in \mathbb{N}$, p primo y $e \in \mathbb{N}_0$, con excepción de los casos $(m, p) = (3, 2), (4, 3), (4, 5)$ y $(4, 7)$, entonces la conjetura de Casas-Alvero es cierta para polinomios con coeficientes en \mathbb{C} de grado n .*

Demostración: La demostración es inmediata a partir del Teorema 3.22 y los Lemas 3.15, 3.16 y 3.19. \square

Antes de finalizar la tesis, haremos un pequeño resumen de otros resultados obtenidos en [3] y en [2], en los cuales, con técnicas similares se estudia la Conjetura de Casas-Alvero para polinomios de grado 5, 6 y 7 en cuerpos de característica p :

- En [3] se prueba que la Conjetura de Casas-Alvero es cierta para polinomios de grado 5 con coeficientes en un cuerpo de característica p para p primo distinto de 2, 3, 7, 11, 131, 193, 3541 y 8009.
- En [2] se prueba (con técnicas computacionales) que la Conjetura de Casas-Alvero es cierta para polinomios de grado 6 con coeficientes en un cuerpo de característica p para p primo distinto de los que aparecen en la siguiente tabla (de 53 elementos):

2	5	7	11
13	19	23	29
37	47	61	67
73	97	257	811
983	1069	1087	1187
1487	1499	1901	2287
3209	3877	3881	4019
4943	5471	6983	8699
9337	15131	15823	20771
21379	23993	150203	266587
547061	685177	885061	1030951
7783207	17250187	40362599	9348983563
70016757407	2610767527031	225833117528659	7390044713023799
51313000813080529			

- En [2] se prueba (también con técnicas computacionales) que la Conjetura de Casas-Alvero es cierta para polinomios de grado 7 con coeficientes en un cuerpo de característica p para p primo distinto de los que aparecen en una tabla de 366 elementos que los autores han calculado, en la cual los dos números primos más chicos que no aparecen son 7 y 127, y el mayor de todos es el siguiente número primo de 135 cifras:

24984712021698392647916525667237483011737174983678606896870094983849

9096141806825287856933123954724798488422551659890912229726792102063.

Nuevamente, por el Teorema 3.22, esto implica que si $n \in \mathbb{N}$ puede escribirse como $n = mp^e$ con $m \in \{5, 6, 7\}$, $p \in \mathbb{N}$, p primo y $e \in \mathbb{N}_0$, con excepción de los casos (m, p) recién descriptos, entonces la conjetura de Casas-Alvero es cierta para polinomios con coeficientes en \mathbb{C} de grado n .

A modo de resumen, en la siguiente tabla mostramos los números naturales n entre 1 y 50, destacando aquellos para los cuales la Conjetura de Casas-Alvero queda demostrada para polinomios de grado n con coeficientes en cualquier cuerpo de característica 0, a partir de una escritura $n = mp^e$ conveniente:

1	✓	2 = 1 · 2 ¹	✓	3 = 1 · 3 ¹	✓	4 = 1 · 2 ²	✓
5 = 1 · 5 ¹	✓	6 = 2 · 3 ¹	✓	7 = 1 · 7 ¹	✓	8 = 1 · 2 ³	✓
9 = 1 · 3 ²	✓	10 = 2 · 5 ¹	✓	11 = 1 · 11 ¹	✓	12	
13 = 1 · 13 ¹	✓	14 = 2 · 7 ¹	✓	15 = 3 · 5 ¹	✓	16 = 1 · 2 ⁴	✓
17 = 1 · 17 ¹	✓	18 = 2 · 3 ²	✓	19 = 1 · 19 ¹	✓	20	
21 = 3 · 7 ¹	✓	22 = 2 · 11 ¹	✓	23 = 1 · 23 ¹	✓	24	
25 = 1 · 5 ²	✓	26 = 2 · 13 ¹	✓	27 = 1 · 3 ³	✓	28	
29 = 1 · 29 ¹	✓	30		31 = 1 · 31 ¹	✓	32 = 1 · 2 ⁵	✓
33 = 3 · 11 ¹	✓	34 = 2 · 17 ¹	✓	35		36	
37 = 1 · 37 ¹	✓	38 = 2 · 19 ¹	✓	39 = 3 · 13 ¹	✓	40	
41 = 1 · 41 ¹	✓	42		43 = 1 · 43 ¹	✓	44 = 4 · 11 ¹	✓
45		46 = 2 · 23 ¹	✓	47 = 1 · 47 ¹	✓	48	
49 = 1 · 7 ²	✓	50 = 2 · 5 ²	✓				

Notemos por ejemplo, que para grado $n = 12$, las tres descomposiciones $12 = 3 \cdot 2^2 = 4 \cdot 3^1 = 6 \cdot 2^1$ no sirven ya que los pares $(m, p) = (3, 2)$, $(4, 3)$ y $(6, 2)$ están dentro de los casos excluidos. Sin embargo, una demostración computacional ad hoc para este caso fue dada en [2].

Similarmente, para grado $n = 20$, las tres descomposiciones $20 = 4 \cdot 5^1 = 5 \cdot 2^2 = 10 \cdot 2^1$ no sirven ya que los pares $(m, p) = (4, 5)$, $(5, 2)$ y $(10, 2)$ están dentro de los casos excluidos (para el último caso, es fácil ver que $P(X) = X^{10} + X^2 \in \mathbb{Z}_2[X]$ es un contraejemplo para la Conjetura de Casas-Alvero para polinomios de grado 10 en un cuerpo de característica 2). En consecuencia, el primer caso para el que la conjetura permanece abierta es $n = 20$. En [2], los autores estiman que el tiempo de cómputo para probar la conjetura para este caso mediante las mismas técnicas utilizadas para $n = 12$ es excesivo.

Finalmente, la conclusión es que nuevas ideas son necesarias para la resolución de la Conjetura de Casas-Alvero en el caso general.

Bibliografía

- [1] E. Casas-Alvero, *Higher order polar germs*. J. Algebra 240 (2001), no. 1, 326–337.
- [2] W. Castryck, R. Laterveer, M. Ounaïes, *Constraints on counterexamples to the Casas-Alvero conjecture, and a verification in degree 12*. Math. Comp. 83 (2014), no. 290, 3017–3037.
- [3] M. Chellali, A. Salinier, *La conjecture de Casas Alvero pour les degrés $5p^e$* . An. Univ. Dunrea de Jos Galati 35 (2012), no. 1-2, 54–62.
- [4] R. Churchill, J. Brown, *Variable compleja y aplicaciones. Quinta Edición*. McGraw-Hill, New York, 1992.
- [5] D. Cox, J. Little, D. O’Shea, *Ideals, Varieties and Algorithms, An Introduction to Computational Algebraic Geometry and Commutative Algebra. Third edition*. Undergraduate Texts in Mathematics, Springer-Verlag, New York, 2007.
- [6] G. Diaz-Toca, L. Gonzalez-Vega, *On a conjecture about univariate polynomials and their roots*. En “Algorithmic Algebra and Logic”, Proceedings of the Conference in Honor of the 60th Birthday of Volker Weispfenning, April 3 - 6 2005, Passau, Germany, 83–90.
- [7] J. Draisma, J. de Jong, *On the Casas-Alvero conjecture*. Eur. Math. Soc. Newsl. 80 (2011), 29–33.
- [8] H.-C. Graf von Bothmer, O. Labs, J. Schicho, C. van de Woestijne, *The Casas-Alvero conjecture for infinitely many degrees*. J. Algebra 316 (2007), no. 1, 224–230.
- [9] N. Koblitz, *p -adic Numbers, p -adic Analysis, and Zeta-Functions. Second edition*. Graduate Texts in Mathematics, 58. Springer-Verlag, New York, 1984.
- [10] J. Milne, *Algebraic Number Theory*. Disponible en www.jmilne.org/math/, 2014.

- [11] D. Mumford, *The red book of varieties and schemes. Second, expanded edition.* Lecture Notes in Mathematics, 1358. Springer-Verlag, Berlin, 1999.
- [12] J. Vick, Homology theory. *An introduction to algebraic topology. Second edition.* Graduate Texts in Mathematics, 145. Springer-Verlag, New York, 1994.