Universidad de Valladolid

FACULTAD DE CIENCIAS

DEPARTAMENTO DE ÁLGEBRA, ANÁLISIS MATEMÁTICO, GEOMETRÍA Y TOPOLOGÍA.

TESIS DOCTORAL:

PERSPECTIVAS ARITMÉTICAS PARA LA CONJETURA DE CASAS-ALVERO

Presentada por
Rosa María de Frutos Marín
para optar al grado de
doctora por la Universidad de Valladolid

Dirigida por:
Antonio Campillo López

PERSPECTIVAS ARITMÉTICAS PARA LA CONJETURA DE CASAS-ALVERO

Memoria presentada por

Rosa María de Frutos Marín

para acceder al grado de doctor en Matemáticas

Dirigida por

Antonio Campillo López

Universidad de Valladolid

21 de Diciembre de 2012

A la memoria de mis padres, Felipe y Merche

Para Elisa,
y para Miguel

Índice general

Introducción

En el artículo de Eduardo Casas-Alvero publicado en 2001 con título *Higher order polars* [Cas], dedicado a la relación entre las singularidades de un germen de curva plana y las de sus sucesivas curvas polares, el autor plantea, por cuestiones técnicas en su investigación, un problema sobre raíces compartidas por un polinomio de una variable y sus sucesivas derivadas. A pesar de la apariencia elemental de su formulación dicho problema permanece abierto, y es bien conocido por la comunidad matemática como *Conjetura de Casas-Alvero* como, por ejemplo, se muestra en la *Feature* de Jan Draisma y Johan de Jong [D-J] publicada por la *Newsletter* de la EMS en junio de 2011. No obstante, Eduardo Casas-Alvero ya había difundido el problema con anterioridad a 2001 entre especialistas en álgebra y geometría, al haber verificado la dificultad de resolverlo con las técnicas disponibles. He aquí, en su versión más básica, el enunciado de la conjetura de Casas-Alvero.

> Sea $P_n(X)$ un polinomio mónico de grado n con coeficientes en el cuerpo $\mathbb{C}$ de los números complejos. Si $P_n(X)$ comparte una raíz con cada una de sus $n-1$ primeras derivadas $P_n'(X)$, $P_n''(X), \ldots, P_n^{(n-1)}(X)$, entonces existe $\alpha \in \mathbb{C}$ tal que $P_n(X) = \big(X-\alpha\big)^n$.

En esta Memoria se presentan de forma organizada sucesivos avances sobre la conjetura que han ido obteniéndose en los últimos años, así como el desarrollo de los métodos generales que permiten comprenderlos en sus aspectos conceptuales. Se ha redactado en forma autocontenida tratando de mostrar, por una parte, hasta qué punto las técnicas son susceptibles de proporcionar resultados sobre la conjetura y, por otra, de descubrir cómo y dónde se localizan escollos de gran dificultad o de práctica imposibilidad de ser superados. Si bien la formulación y el análisis de la conjetura de Casas-Alvero es algebraico-geométrica, el denominador común de los métodos y resultados de la Memoria se puede considerar más bien propio de la teoría de números.

En particular, la Memoria ofrece diversas perspectivas aritméticas para la conjetura, sin excluir otras de naturaleza geométrica o computacional, así como diferentes formulaciones equivalentes de la misma. Entre otras, se muestra que la conjetura puede formularse en

términos exclusivamente aritméticos, o que es equivalente a determinadas propagaciones o desplazamientos de sus hipótesis. Pero el enfoque predominante es la reducción de la conjetura a otra, módulo un número primo que sea eficaz para probarla en el nuevo escenario. En la Memoria se utilizan hasta siete reducciones distintas, con diferentes consecuencias prácticas; pero se muestra que todas ellas poseen idéntica eficacia, proporcionando así un planteamiento consistente para la conjetura de Casas-Alvero en característica arbitraria.

Los avances y resultados que se presentan en la Memoria, y que se resumen a partir del próximo párrafo, han sido obtenidos por la autora a partir de 2005 en las fechas que se precisan en esta introducción. También se precisan las referencias de resultados de otros autores que han ido apareciendo en la literatura desde entonces. En el momento de presentar esta Memoria su contenido se puede entender como una referencia general para todos ellos, así como para determinar límites de aplicación de los métodos disponibles y para realizar futuras investigaciones sobre la conjetura.

Con objeto de acceder a la etapa investigadora del programa de doctorado en Matemáticas en la Universidad de Valladolid (en la que imparto docencia como profesora Titular de Escuela Universitaria desde 1989) presenté en 2005 el trabajo [Fru1] en el que proporcionaba una solución a la conjetura de Casas-Alvero para el caso en el que el polinomio $P_n(X)$ dispone solo de tres monomios. Este resultado, que en la Memoria figura como corolario 2.3.4, expone ya muy claramente, en términos aritméticos, el tamaño de las dificultades que cabe esperar para la prueba de la conjetura en general.

Esta solución comprende tres etapas sucesivas. La primera consiste en asociar a los tres grados, i, j, n (con $i < j < n$) de los monomios de $P_n(X)$, el número entero dado por

$$\Delta = (-1)^{\rho\sigma}\left[a^{\,\rho}\,(b-c)^{\rho}(b-ac)^{\sigma} - (-1)^{\sigma}(a-1)^{\rho+\sigma}(b-1)^{\rho}\right]$$

donde $a=\binom{n}{i}$, $b=\binom{n}{j}$, $c=\binom{n\text{-}i}{n\text{-}j}$ y $\rho=\frac{n-j}{d}$, $\sigma=\frac{j-i}{d}$, con $d=\text{m.c.d.}\big(n-j, j-i\big)$, y en demostrar que, para los polinomios considerados, la conjetura queda reducida a la condición $\Delta \neq 0$. La segunda, en darse cuenta de que la conjetura para esta clase de polinomios equivale a afirmar que dicha condición se satisface para *todas* las selecciones posibles de los valores i, j, n, es decir, a resolver un problema diofántico concreto. La tercera, en demostrar que para i, j, n dados tiene que existir necesariamente algún número primo p con la propiedad de que sea Δ distinto de cero módulo p.

Cada etapa tiene su peculiaridad. La primera, la complejidad de la expresión del entero Δ. La segunda, la dificultad de probar que la ecuación $\Delta = 0$ no tiene soluciones enteras i, j, n, con $n > j > i > 0$. La tercera, que la prueba de la existencia de p no necesita ser constructiva. Nótese que, de haberse encontrado una solución para la ecuación en la segunda etapa, se habría tenido un contraejemplo para la conjetura, pero ello no ha podido suceder debido a la existencia del primo p en la tercera etapa. Más aún, el comentario 2.3.5 pone de

manifiesto cómo la afirmación de que p existe se debe, en el fondo, a un hecho combinatorio.

Desconozco si la conjetura es cierta para polinomios con cuatro monomios. La observación 5.6.9 permite recuperar la primera y la segunda etapa para este caso, por medio de un entero $\delta = \delta(n, \{i, j, k\})$ cuya no anulación equivale a la prueba de la conjetura y que, como viene dado por una resultante, dispone de una expresión explícita en términos de los grados de los cuatro monomios. La gran complejidad de dicha expresión hace que probar la no existencia de soluciones de la ecuación $\delta = 0$ se presente como un problema intratable. La tercera etapa reduce la prueba de la conjetura a la existencia de un primo conveniente para cada valor de los cuatro grados, pero de dicha existencia no tenemos constancia por el momento. No está descartada una eventual solución de esta ecuación y, por tanto, un contraejemplo a la conjetura.

Las clases de polinomios con pocos monomios (dos, tres o cuatro) dan lugar a una estrategia recurrente a lo largo de la Memoria que nos permite delimitar, desde una perspectiva aritmética, el conocimiento progresivo sobre la conjetura. Para solo dos monomios, de grados i, n, la validez de la conjetura equivale, por el corolario 2.2.3, a la tautológica condición $\Delta(n, \{i\}) = \binom{n}{i} - 1 \neq 0$. En general, dado el grado n y un subconjunto I de $\{1, 2, \ldots, n-1\}$ se tiene un *I-problema parcial de Casas-Alvero* que, esencialmente, no es otra cosa que la conjetura de Casas-Alvero para la clase de polinomios de grado n cuyos monomios diferentes del líder tienen sus grados en I.

La transformada de Tschirnhausen descrita en la sección 1.1 preserva las hipótesis y la tesis de la conjetura; puesto que, efectuada sobre un polinomio de grado n y en las condiciones del problema, permite obviar tanto el término *vicelíder* (de grado $n-1$) como el término independiente, se deduce que el J-problema de Casas-Alvero, donde $J = \{1, 2, \ldots, n-2\}$, es equivalente a la propia conjetura en grado n. Por esta razón, a lo largo de la Memoria nos ceñimos a considerar I-problemas parciales para subconjuntos I de J, siendo el caso particular $I = J$ coincidente con el *problema total* en grado n.

Salvo en el último capítulo, los polinomios se representan a lo largo de la Memoria mediante expresiones a las que llamaremos *de coeficientes presentados* , y consideraremos *derivadas netas* en vez de derivadas ordinarias. Esta elección ha permitido utilizar frecuentemente combinatoria en lugar de cálculo. Un polinomio mónico presentado sobre un cuerpo $\mathbb{K}$ tiene la forma

$$P_n(X) = X^n + \tbinom{n}{1} b_1 X^{n-1} + \tbinom{n}{2} b_2 X^{n-2} + \ldots + \tbinom{n}{n-i} b_{n-i} X^i + \ldots + \tbinom{n}{n-1} b_{n-1} X + \tbinom{n}{n} b_n,$$

y su derivada neta de orden i es el polinomio presentado —también mónico— dado por

$$P_n{}^{[i]}(X) = X^{n-i} + \tbinom{n-i}{1} b_1 X^{n-1-i} + \tbinom{n-i}{2} b_2 X^{n-2-i} + \ldots + \tbinom{n-i}{n-i} b_{n-i}\,.$$

Entre sus propiedades útiles encontramos la igualdad $\left(P_n{}^{[i]}(X)\right)^{[j]} = P_n{}^{[i+j]}(X)$, y destaca el hecho de que la derivada neta de orden i de un polinomio presentado de grado n

cuyos coeficientes están dados por la $(n\text{-}1)$-upla $(b_2,\ldots,b_n)$ es exactamente el polinomio presentado de grado $n-i$ cuyos coeficientes están dados por la $(n\text{-}i\text{-}1)$-upla $(b_2,\ldots,b_{n\text{-}i})$. Si la característica de $\mathbb{K}$ es cero entonces existe un único polinomio con coeficientes presentados para cada polinomio dado por sus coeficientes ordinarios; sin embargo, si tiene característica positiva no está garantizada ni la existencia ni la unicidad en general, como se muestra en el comentario 3.2.4.

Dado I, si consideramos a las variables $b_{n\text{-}i}$ $(i\in I)$ como coordenadas homogéneas en un espacio proyectivo pesado en el que $b_{n\text{-}i}$ tiene peso $n-i$, y denotamos por $P_n(X)$ el polinomio presentado de grado n cuyos monomios no líderes son aquellos que tienen grado en I y cuyos coeficientes están dados por los respectivos $b_{n\text{-}i}$, entonces el teorema de los ceros de Hilbert homogéneo permite formular la I-conjetura de Casas-Alvero en forma idealística, afirmando en concreto que el radical del ideal $\mathcal{I}$ generado por las resultantes $H^{[i]}$ de $P_n(X)$ y $P_n^{[i]}(X)$, con $i\in I$, es igual al ideal generado por los $b_{n\text{-}i}$, $i\in I$. Este hecho sugiere la posibilidad de probar la I-conjetura mostrando que los $b_{n\text{-}i}$ pertenecen al radical de $\mathcal{I}$ mediante el uso de bases de Groebner. Sin embargo, tal como se muestra en la sección 2.4, cuando los grados son genéricos tal procedimiento no es postulable ni siquiera para el caso en que I tiene cardinal dos. En efecto, en una etapa de la aplicación del algoritmo de Buchberger el entero Δ aparece como coeficiente en un monomio candidato a ser líder, siendo entonces preceptivo, para continuar aplicando el algoritmo, comprobar si dicho entero es nulo o no; tarea esta que equivale a la propia demostración de la I-conjetura. En la referida sección se muestra, de hecho, que esta obstrucción se presenta cualquiera que sea la forma de plantear la computación.

La observación anterior me permitió asumir en 2005 la imposibilidad de probar la conjetura mediante el empleo de bases de Groebner cuando el grado n es arbitrario; sin embargo, los métodos computacionales sí son aplicables cuando se fijan valores pequeños de n. Como ejemplo, en la subsección 1.3.3 se ofrece una descripción explícita sencilla del algoritmo de Buchberger que ilustra la prueba de la conjetura para $n=4$, proceso que se vuelve mucho más complejo para $n=5$. El software que he utilizado para todos los cálculos que se reflejan en la Memoria ha sido DERIVE, empleado en ámbitos docentes, priorizando la comprensión conceptual de los métodos a la potencia del cómputo.

En 2006 se publicó el trabajo de Gema Díaz Toca y Laureano González Vega [D-G], en el que se establece la base computacional para la prueba de la conjetura para valores concretos de n. Mostraron, en particular, la validez de la conjetura para $n\leq 7$, y evidenciaron la complicación que supone el cálculo para valores mayores de n. A la vez, también en 2006, se publicó el artículo de Hans-Christian Graf von Bothmer, Oliver Labs, Joseph Schicho y Christiaan van de Woestijne [BLSW] en el que se prueba la conjetura para infinitos valores de n y, como aportación aún más importante, se introduce la reducción de la conjetura

módulo un número primo p como técnica para probarla.

Los autores de [BLSW] utilizan coeficientes ordinarios para los polinomios y derivadas de Hasse, omitiendo el uso de la transformación de Tschirnhausen y empleando, por tanto, una variable más. Considerando el polinomio $P_n(X) = X^n + a_1 X^{n-1} + \ldots + a_{n-1} X + a_0$ y, para cada $i = 1, \ldots, n-1$, su derivada de Hasse de orden i,

$$P_n^{<i>}(X) = \binom{n}{i} X^{n-i} + \binom{n-1}{i} X^{n-i-1} + \ldots + \binom{i}{i} a_{n-i},$$

hemos denotado por $G^{<i>}$ a la resultante entre $P_n(X)$ y $P_n^{<i>}(X)$. En el espacio proyectivo pesado en el que las a_{n-i} son coordenadas homogéneas de peso $n-i$, el ideal generado por los $G^{<i>}$ es homogéneo, definiendo un subesquema de dicho espacio que en la Memoria denotamos por X_n' y del que diremos que es un *esquema de coeficientes ordinarios*.

Aunque un esquema está dado por una determinada asignación funtorial de un conjunto a cada anillo conmutativo, en esta Memoria solamente nos resulta útil la asignación sobre los cuerpos y, más en concreto, sobre el cuerpo $\mathbb{C}$ de los números complejos y sobre las clausuras algebraicas $\overline{\mathbb{F}}_p$ de los cuerpos $\mathbb{F}_p$, donde p es un número primo. Un espacio proyectivo pesado es un ejemplo de esquema, y cada ideal generado por polinomios homogéneos pesados en las variables consideradas define en él un subesquema proyectivo.

Es un resultado no trivial pero bien conocido en geometría que, si Y es un esquema proyectivo, entonces la condición $Y(\mathbb{C}) = \emptyset$ es equivalente a que sea $Y(\overline{\mathbb{F}}_p) = \emptyset$ para algún primo p y que, si este es el caso, entonces se cumple $Y(\overline{\mathbb{F}}_p) = \emptyset$ para todos excepto para una cantidad finita de primos p. La proposición 3.0.3 aporta una prueba constructiva de este resultado en términos de los anillos de enteros de los cuerpos de números, cuya teoría [Sam] es especializada pero más práctica y asequible que la de esquemas. El planteamiento de [BLSW] aplica el mencionado resultado al esquema proyectivo X_n' para reducir la conjetura a probar que se tiene $X_n'(\overline{\mathbb{F}}_p) = \emptyset$ para un primo p conveniente. Los autores demuestran que en los casos $n = p^r$ y $n = 2p^r$ el primo p sirve para estos fines. También es fácilmente deducible de sus resultados que lo mismo sucede si es $n = 3p^r$ y p no es 2.

Estos avances me sugirieron, en 2006, aplicar 3.0.3 al esquema proyectivo de coeficientes presentados Y_n, definido como aquel cuyas variables pesadas son las b_{n-i} y el ideal está generado por las resultantes $H^{[i]}$, $i \in J$. Entre las razones que motivan el estudio de este esquema —que se ve favorecido por la particularidad de que las derivadas netas sean polinomios mónicos—, destaca el interés en averiguar si podía darse el caso de que, siendo $X_n'(\overline{\mathbb{F}}_p) \neq \emptyset$, fuera sin embargo $Y_n(\overline{\mathbb{F}}_p) = \emptyset$ —o viceversa—, de tal modo que el primo en cuestión serviría para probar la conjetura por medio de uno de los esquemas aun cuando ese mismo primo no sirviera para ello utilizando el otro. Como ya se ha apuntado anteriormente, esto no sucede en ningún caso; este hecho es un resultado no trivial que se demuestra en la Memoria (teorema 5.3.1).

Hay, además, una propiedad para cuya visualización y manejo son particularmente adecuados los esquemas de coeficientes presentados, y que estimula el empleo de los esquemas $Z_{n,I}$, análogos a Y_n —de hecho, subesquemas del mismo— que son específicos para el análisis de los problemas parciales. En el estudio de estos esquemas he concentrado la atención y el trabajo hasta 2008 y, en consecuencia, la Memoria les dedica un papel central. Dado un conjunto de exponentes I y el primo p, denotamos por I_p al subconjunto formado por aquellos $i \in I$ tales que $\binom{n}{i}$ es no nulo módulo p. La propiedad arriba aludida constituye el enunciado del teorema 3.3.5, o de *resolución por elevación*,

$$Z_{n,I_p}\big(\overline{\mathbb{F}}_p\big) = \emptyset \quad \Longleftrightarrow \quad Z_{n,I}\big(\overline{\mathbb{F}}_p\big) = \emptyset,$$

que, en particular, establece que p es eficaz para probar la I-conjetura si y solo si lo es para probar la I_p-conjetura. Este teorema remite, pues, el análisis de la conjetura para casos en que el cardinal de I puede ser arbitrario a la localización de primos p tales que el conjunto I_p resulte mucho más conveniente.

Su demostración, que reúne varios de los ingredientes más empleados en la Memoria —en particular, el hecho combinatorio 2.3.5 ya referido anteriormente—es tributaria del teorema 3.3.1, o de *resolución por interpretación*, el cual establece la legitimidad de conclusiones que, siendo obvias en característica cero, no son en absoluto triviales en característica p. En concreto, el teorema de resolución por interpretación permite deducir de la igualdad $P_n(X) = X^n$, cuando se verifica sobre el cuerpo $\overline{\mathbb{F}}_p$, la igualdad $P_n{}^{[i]}(X) = X^{n-i}$ cualquiera que sea el orden i de derivación, pese a todas las distorsiones que puede inducir, módulo p, la presencia en sus términos de factores enteros de la forma $\binom{n}{n-k}$ o $\binom{n-i}{n-k}$, respectivamente. Es destacable el hecho de que su prueba sea totalmente conceptual, libre de todo cálculo aritmético.

El teorema de resolución por elevación supone un incentivo para tratar de investigar bajo qué condiciones se verifica $Z_{n,I}\big(\overline{\mathbb{F}}_p\big) = \emptyset$. Como en el caso del cuerpo $\mathbb{C}$, en la Memoria se muestra la completa resolución de los casos en que I tiene cardinal 1 o 2, en las secciones 2.2 y 2.3, consistente en un cuidadoso desarrollo de los mismos métodos que se habían empleado para el caso de $\mathbb{C}$ de modo que sean válidos en característica positiva. La revisión del proceso, que arranca del cálculo de las resultantes definidas como un determinante, permite también valorar la dificultad de abordar cálculos similares para cardinales de I mayores o iguales que 3.

Observemos que el teorema de resolución por interpretación, conjuntamente con la proposición 3.1.4, permitiría probar de modo inmediato que la I-conjetura de Casas-Alvero es en ambos casos cierta —como, por otra parte, ya habían establecido los corolarios 2.2.3 y 2.3.4—, pues se tendría que $Z_{n,I}\big(\overline{\mathbb{F}}_p\big) = \emptyset$ sin más que tomar un primo p tal que I_p sea vacío, primo cuya existencia nos consta gracias, de nuevo, a 2.3.5; sin embargo este no

es ahora nuestro objetivo: lo que queremos es caracterizar la condición $Z_{n,I}(\overline{\mathbb{F}}_p)=\emptyset$ en términos de los datos n, I, p, para lo cual, como se ha dicho, es preciso validar sobre $\overline{\mathbb{F}}_p$ los cálculos contenidos en 2.2 y 2.3, originalmente realizados en característica cero. Los resultados se recogen en el teorema 3.5.1 que, concretamente, proporciona las siguientes caracterizaciones:

- $Z_{n,\{i\}}(\overline{\mathbb{F}}_p)=\emptyset$ si y solo si $\binom{n}{i}\not\equiv 1 \mod p$.
- $Z_{n,\{i,j\}}(\overline{\mathbb{F}}_p)=\emptyset$ si y solo si se cumplen las tres condiciones siguientes:
  - (i) $a\not\equiv 1 \mod p$
  - (ii) $b\not\equiv 1 \mod p$
  - (iii) $a^{\rho}(b-c)^{\rho}(b-ac)^{\sigma}-(-1)^{\sigma}(a-1)^{\rho+\sigma}(b-1)^{\rho}\not\equiv 0 \mod p$,

siendo $a=\binom{n}{i}$, $b=\binom{n}{j}$, $c=\binom{n\text{-}i}{n\text{-}j}$ y $\rho=\frac{n\text{-}j}{d}$, $\sigma=\frac{j\text{-}i}{d}$, con $d=\text{m.c.d.}(n-j, j-i)$

En la Memoria se obtienen variadas aplicaciones de estos resultados que, combinados entre sí, se expresan como el ya comentado teorema 3.3.1, o como las proposiciones 3.5.3 y 3.5.5, según que el cardinal de I_p sea cero, uno o dos. Se deducen como respectivos corolarios 3.3.2, 3.5.4 y 3.5.6, nuevas pruebas de los resultados acerca de la validez de la conjetura en los casos de $n=p^r$, $2p^r$, $3p^r$. También como consecuencia de 3.5.1 obtuve en 2007 el corolario 4.2.2, que afirma que la conjetura de Casas-Alvero es cierta para todos los grados $n=4p^r$ siempre que p sea un primo diferente de 3, 5 o 7. Este resultado, que comuniqué en [Fru2], fue redescubierto en 2011 por Jan Draisma y Johan de Jong como resultado central de su trabajo [D-J].

Para acceder a la prueba de 4.2.2 ha sido fundamental establecer previamente el teorema 4.1.4, o de *eliminación del término vicelíder*, según el cual, para todo primo p se verifica

$$Y_n'(\overline{\mathbb{F}}_p)=\emptyset \quad\Longleftrightarrow\quad Y_n(\overline{\mathbb{F}}_p)=\emptyset,$$

siendo Y_n' el esquema de coeficientes presentados en el cual no se ha descartado la presencia del coeficiente b_1. La demostración de este resultado concerniente a los cuerpos $\overline{\mathbb{F}}_p$ ilustra, en particular, que la transformada de Tschirnhausen puede aplicarse en característica positiva siempre que se consideren polinomios presentados.

La dificultad de probar el resultado 4.1.4 no es conceptual, sino que proviene de la necesidad de demostrar específicamente para las expresiones de coeficientes presentados algunas propiedades que para las expresiones con coeficientes ordinarios son estándar; es el caso, por ejemplo, de la regla de la cadena para la derivada neta que se prueba en 4.1.3. El teorema de eliminación del vicelíder permite, junto con el de resolución por elevación y ciertos cálculos realizados con números combinatorios, demostrar el teorema 4.2.1, o de

resolución por condensación. Este teorema establece la equivalencia

$$Y_{hp^r}\left(\overline{\mathbb{F}}_p\right) = \emptyset \quad \Longleftrightarrow \quad Y_h\left(\overline{\mathbb{F}}_p\right) = \emptyset,$$

aportando la consecuencia de que, si un primo p es eficaz para probar la conjetura de cierto grado h, entonces ese mismo primo es también eficaz para probarla en todo grado de la forma $n = hp^r$. El resultado análogo referente al esquema X_n' se halla en [BLSW]; véase también, en concreto, la contribución de Woestijne [Woe] realizada en 2010.

Otra notable aplicación de 3.3.1 y 3.5.1 es el teorema 3.6.2, el cual afirma que, para $I = \{2, 3, \ldots, n-2\}$, la I-conjetura de Casas-Alvero es cierta en todo grado de la forma $n = p^r + 1$ o bien $n = 2p^r + 1$, donde p es un número primo. En efecto, utilizando las propiedades del triángulo de Tartaglia que se desarrollan en la sección 3.4 se muestra que I_p es vacío si es $n = p^r + 1$, e I_p tiene cardinal 2 y además se satisfacen las condiciones de 3.5.5, si es $n = 2p^r + 1$. El teorema 3.6.2 ha sido redescubierto en 2012 por Wouter Castryck en el caso $n = p + 1$ y por Robert Lauterveer y Miryam Ounaïes [L-O] en el caso $n = p^r + 1$, al estudiar las restricciones para hipotéticos contraejemplos a la conjetura en estos grados.

Merece ser señalado que estos autores también han descubierto en [L-O] y [CLO-1] otra importante restricción, ya que han mostrado con nuestra terminología que, siendo $n = p + 1$, si existiese un contraejemplo en $Y_n(\mathbb{C})$ entonces no solo tendría que verificarse para él que $b_{n\text{-}1}$ fuese distinto de cero, sino que se verificaría también $b_{n\text{-}i} = b_{n\text{-}j} = 0$ para al menos dos índices i, j con $0 < i < j < n-1$ que además satisfacen una igualdad aritmética adicional. Conviene mencionar que la prueba de este último resultado, ajeno a la Memoria, es posible porque sitúa al contraemplo en el escenario de la prueba de 3.0.3 y utiliza argumentos propios de teoría de números.

Este descubrimiento, complementario de 2.2.3 y 2.3.4, aporta otro aliciente adicional para investigar los esquemas de coeficientes presentados. Entre otras aplicaciones, ha permitido a los autores de [CLO-1] simplificar la computación de la validez de la conjetura, que han logrado contrastar con éxito para $n = 12$ mediante la ejecución de algoritmos programados en Magma y varias semanas de cómputo.

La validez del teorema 3.6.2 me permitió en 2009 y 2010 encontrar varios enunciados equivalentes a la conjetura de Casas-Alvero, cuya característica principal es que se formulan en términos exclusivamente de la hipótesis de la misma, sin mención explícita alguna a su tesis. Se trata de las *conjeturas de propagación y desplazamiento de hipótesis* formuladas en las subsecciones 3.6.1 y 3.6.2, y establecidas como equivalentes a la conjetura de Casas-Alvero en los teoremas 3.6.4 y 3.6.6 respectivamente. La de propagación afirma que si el polinomio $P_n(X)$ verifica la hipótesis de Casas-Alvero (*i.e.*, comparte una raíz con cada derivada de grado positivo) entonces igualmente verifica tal hipótesis el polinomio $\left(P_n(X)\right)^d$ para algún entero $d > 1$ que satisfaga $nd = p^r + 1$ o bien $nd = 2p^r + 1$. En su de-

mostración se invoca al clásico teorema de Dirichlet [Ser], para garantizar la existencia de enteros $d > 1$ con esta propiedad. La de desplazamiento, por su parte, afirma que si $P_n(X)$ cumple la hipótesis de Casas-Alvero, entonces también la cumple $X^e \cdot P_n(X)$ para algún entero $e > 0$ tal que para $n+e$ la conjetura de Casas-Alvero ya haya sido probada, o bien que sea $n+e = p^r+1$ o $n+e = 2p^r+1$, entero cuya existencia es, en esta ocasión, obvia.

Es fácil verificar que, salvo unas pocas excepciones, para los primeros cientos de valores de n los enteros d y e toman valores pequeños, especialmente en el caso de e. El corolario 3.6.9 necesita solo del valor $e=1$ para mostrar que la afirmación de que la conjetura de Casas-Alvero es verdadera *en todo grado* n es equivalente a la afirmación de que siempre que un polinomio $P(X)$ satisfaga la hipótesis de Casas-Alvero, también $X \cdot P(X)$ satisface dicha hipótesis. Obsérvese que el enunciado de esta afirmación es *transversal al grado*.

Varias veces en esta introducción hemos calificado a un número primo de *eficaz* para referirnos a la cualidad que permite emplearlo para probar la validez de la conjetura en una determinada situación. Ello no es casual, ya que la noción de *primo eficaz* se introduce técnicamente en la Memoria como una noción relativa a un esquema proyectivo Y dado; en concreto, p es eficaz para Y si se cumple $Y\big(\overline{\mathbb{F}}_p\big) = \emptyset$, lo cual, en virtud de 3.0.3, implica (y en eso consiste su eficacia) que también se cumple $Y\big(\mathbb{C}\big) = \emptyset$. En la Memoria se estudian —de hecho, para cada grado n— siete esquemas proyectivos diferentes, con cada uno de los cuales la conjetura de Casas-Alvero se expresa mediante la condición $Y(\mathbb{C}) = \emptyset$; así pues, fijado un grado, cada uno de ellos dispone de sus primos eficaces si y solo si la conjetura es cierta para ese grado.

Tres de estos esquemas, los de coeficientes presentados Y_n e Y_n' y el de coeficientes ordinarios X_n', han sido ya comentados. En el caso de coeficientes ordinarios, omitiendo la variable a_1 se obtiene un subesquema de X_n' al que denotaremos por X_n. Por otro lado, una tercera vía para expresar un polinomio es la que lo hace en términos de sus raíces, esto es, en la forma

$$P_n(X) = (X - x_1) \cdot (X - x_2) \cdot \cdots \cdot (X - x_n).$$

A diferencia de los coeficientes a_{n-i} o b_{n-i}, las raíces x_1, x_2,..., x_n ocupan posiciones intercambiables; en la sección 5.1 esta simetría inicial se invierte parcialmente en reducir los hipotéticos contraejemplos a una forma prefijada que facilita su búsqueda. La transformación de Tschirnhausen, junto a la condición de compartir una raíz con $P_n^{<n-i>}(X)$, proporciona las restricciones $(1)\colon x_1 + x_2 + \cdots + x_n = 0$; $x_1 = 0$. Asimismo, la condición de compartir una raíz con $P_n^{<1>}(X)$ toma la forma $(2)\colon x_2\,(x_2 - x_3) = 0$. Finalmente, el resto de condiciones se expresan mediante $(3)\colon K^{<2>} = K^{<3>} = \cdots = K^{<n-2>} = 0$, siendo $K^{<i>}$ la resultante $G^{<i>}$ reescrita en términos de sus raíces.

El conjunto de condiciones $(1), (2), (3)$, que considerando el peso usual están dadas por polinomios homogéneos en las variables $x_1, \ldots, x_n$, definen el esquema proyectivo R_n en el

espacio que tiene a estas variables como coordenadas. Si la restricción $x_1+x_2+\cdots+x_n=0$ se sustituye por la —más débil— $K^{<n-1>}=0$, se obtiene el esquema R_n'. Diremos que estos esquemas son *esquemas de raíces*.

Finalmente, si utilizando la expresión con coeficientes ordinarios para un I-polinomio con $I=\{k_1,\ldots,k_r\}$ se habilita la variable s_l para denotar una raíz compartida por $P_n(X)$ y $P_n^{<k_l>}(X)$, $(l=1,\ldots,r)$, se muestra en la sección 5.5 cómo obtener las r condiciones polinómicas homogéneas $M_l(s_1,\ldots,s_r)=0$ que expresan las compatibilidades que las hipótesis de la conjetura imponen a la totalidad de raíces compartidas. El esquema proyectivo que definen los polinomios M_l en el espacio en el que las s_i son coordenadas se denota en la Memoria por $S_{n,I}$, y diremos de él que es un *esquema sintético*. Naturalmente, el esquema $S_{n,J}$ —donde $J=\{1,\ldots,n-2\}$— se aplica al problema total en grado n.

En 2011 he probado uno de los resultados principales de la Memoria. Se trata del teorema 5.3.1 que, junto al teorema 5.5.2 permiten concluir como corolario que todo primo p que sea eficaz para uno cualquiera de los siete esquemas Y_n, X_n, R_n, $S_{n,J}$, Y_n', X_n', R_n', es también eficaz para cada uno de los restantes. La demostración no es trivial; de hecho, su dificultad reside en la equivalencia

$$X_n\big(\overline{\mathbb{F}}_p\big)=\emptyset \iff Y_n\big(\overline{\mathbb{F}}_p\big)=\emptyset,$$

que es el objeto del teorema 5.2.2, junto al teorema de eliminación del vicelíder, que proporciona la equivalencia análoga entre Y_n e Y_n'. Tal equivalencia no era previsible, particularmente, entre los esquemas X_n y X_n', dado que en característica positiva no siempre es posible aplicar la transformada de Tschirnhausen a los polinomios expresados por sus coeficientes ordinarios. Nótese que ha sido demostrada de manera indirecta, gracias al puente que los mencionados teoremas (5.2.2, junto con un análogo para la versión *prima* de los esquemas, como pilares; 4.1.4, a modo de tablero) tienden entre ambos esquemas. La noción de polinomio presentado se manifiesta, de nuevo, como un instrumento valioso en característica positiva.

El fallido intento de localizar primos que, no siendo eficaces para X_n', lo fueran para algún otro esquema ligado a la conjetura, proporciona, gracias al inesperado resultado de que los siete esquemas estudiados tengan los mismos primos ineficaces, una notable consecuencia que cabe atribuir a esta Memoria. En efecto, cada uno de los esquemas plantea sobre $\overline{\mathbb{F}}_p$ un problema de Casas-Alvero en principio diferente; pero el hecho de que, fijado un grado n, la solución a estos siete problemas sea la misma (sí o no, pero igual para todos ellos, según que el primo p sea o no eficaz para probar la conjetura de Casas-Alvero original en grado n) permite afirmar que la conjetura de Casas-Alvero está bien definida en característica positiva y puede formularse a través de cualquiera de los esquemas considerados. Y ello, pese a que no son esquemas isomorfos entre sí.

Todos los primos eficaces con n que, hasta el momento, han servido en la práctica para demostrar la conjetura de Casas-Alvero en grado n han sido menores o iguales que n. El corolario 4.3.2 muestra que solo puede existir un primo que, siendo menor o igual que n, sea eficaz con él, y que, si existe, entonces coincide necesariamente con el *primo dominante* de n, esto es, un primo presente en la factorización de n que supere al producto de las potencias de los otros primos; cabe señalar que el primo dominante de n no siempre existe, y que cuando existe no siempre es eficaz. Procede, en ese caso, centrarse en la búsqueda de primos eficaces mayores que n. Según el *principio de expansión* enunciado en la sección 4.3, el hallazgo de un primo que sea eficaz para n permite decidir que la conjetura es cierta para los grados de la forma np^r.

Para la localización de primos eficaces se puede utilizar, naturalmente, cualquiera de los siete esquemas proyectivos anteriormente descritos. Resultados ya comentados muestran los primos ineficaces para los grados $n=3$ y $n=4$. En 2009 desarrollé el contenido completo de las secciones 4.4 y 5.4 en la forma en que aparecen en la Memoria, y lo comuniqué en [Fru2]; en particular, encontré los nueve primos ineficaces con $n=5$ de dos maneras —una, probando 4.4.3 a través del esquema Y_5; otra, en 5.4.$[n=5]$ mediante R_5—, así como los cincuenta y tres primos ineficaces con $n=6$, probando 5.4.1. Dichos números han sido redescubiertos a través de variantes de los esquemas X_5' y X_6' por Castryck, Lauterveer y Ounaïes [CLO-2] en 2012, y los de $n=5$ alternativamente por Chellali y Salinier [C-S]. En [CLO-2] está disponible además la lista de los seiscientos sesenta y un primos que son ineficaces para $n=7$, un cálculo que teóricamente es posible también a partir de R_7 por el procedimiento descrito en 5.4.$[n=7]$ pero que no he completado porque el cómputo excede la capacidad del programa DERIVE.

En la sección 5.4 los cálculos dejan claro que el esquema R_n es muy adecuado para calcular los primos eficaces para valores pequeños de n. En efecto, como el lector observará, los cálculos en 5.4 son, para $n=3, n=4$, extremadamente elementales, mientras que para $n=5,6,7$ son susceptibles de ser abordados computacionalmente con mínimas casuísticas. En el ejemplo previo al final de la Memoria se muestra que $S_{n,J}$ también resulta ser un esquema muy adecuado para este tipo de cálculos. De hecho, un cálculo en tres etapas elementales permite calcular el entero D_5, cuyos divisores primos son exactamente los nueve ineficaces para $n=5$.

Los cálculos de 4.4 disponen de una ventaja adicional sobre los de 5.4, y es que permiten clasificar a los primos por *niveles de ineficacia* respecto de un n fijado, entendiendo que el nivel cero lo ocupan los primos eficaces, el nivel uno aquellos que son ineficaces para una I-conjetura en grado n con cardinal de I igual a 1 y, en general, son de nivel k aquellos que son ineficaces para una I-conjetura en grado n con cardinal de I igual a k pero que no están en los niveles de ineficacia previos. Para $n=4$, 5 y 6, los primos ineficaces aparecen

clasificados por niveles en la Memoria debido a los resultados obtenidos en 4.4. En general, los primos en los niveles de ineficacia 1 y 2 son calculables usando solo aritmética, a través de 3.5.3 y 3.5.5 respectivamente; en la Memoria se ofrece una tabla de dichos niveles hasta $n=12$, que permite observar cómo el volumen y el tamaño de los primos que contienen van aumentando a ritmo creciente cuando lo hace el valor de n.

Las observaciones 5.2.3 y 5.5.3 muestran que, igual que sucedía en el caso total, los diversos esquemas parciales que tienen sentido para una I-conjetura parcial —$Z_{n,I}$, $X_{n,I}$, $S_{n,I}$— poseen exactamente los mismos primos eficaces; se desprende de ello que, no solo el conjunto de los primos ineficaces con n, sino su distribución por los distintos niveles de ineficacia, es independiente del esquema parcial que se considere.

El desarrollo de los esquemas sintéticos en la sección 5.5 ha permitido descubrir un método aritmético similar para determinar computacionalmente, en la práctica, los primos en el nivel de ineficacia 3. Si se considera un I-problema parcial con cardinal de I mayor que 2, e $i<j$ son los dos enteros más pequeños de I, y si consideramos el abierto afín de contraejemplos a la I-conjetura con $a_{n\text{-}i}$ diferente de cero, entonces la proposición 5.5.4 muestra que la inexistencia de tales contraejemplos es equivalente a que el sistema de ecuaciones algebraicas con $q=\mathrm{card}(I)-2$ incógnitas $s_1,\ldots,s_q$ y $q+1$ ecuaciones dado en (5.21) no posea solución, siendo esta equivalencia válida tanto sobre el cuerpo $\mathbb{C}$ como sobre los cuerpos $\overline{\mathbb{F}}_p$.

La intersección del ideal principal generado por los $q+1$ polinomios que definen dichas ecuaciones con el anillo $\mathbb{Z}$ es un ideal principal cuyo generador $\Delta(n,I)$, bien definido salvo el signo, lo denominamos en la Memoria *discriminante para la I-conjetura en grado n*. El teorema 5.6.2 muestra que la inexistencia de los mencionados contraejemplos también equivale a la no anulación de $\Delta(n,I)$. Para $I=\{i\}$, se define $\Delta(n,I)=a-1$, donde $a=\binom{n}{i}$, por convenio. En el caso $I=\{i,j\}$ el teorema 5.6.8 proporciona la igualdad

$$\Delta(n,I)=(a-1)^i\,(e-1)^{n\text{-}j}\,\Delta^d,\quad \text{donde}\ \ e=\tbinom{j}{i},\quad d=\text{m.c.d.}\big(n-j,j-i\big)$$

de modo que el discriminante difiere del entero Δ en un factor consecuente con la singularización de los enteros $i<j$ dentro de I que han permitido obtener las ecuaciones (5.21).

El discriminante puede verse, a todos los efectos, como una generalización del entero Δ ligado al $\{i,j\}$-problema para los I-problemas con cardinal de I mayor que 2. Si ahora tomamos I de cardinal 3 se tiene $q=1$ y, por tanto, una sola variable y dos ecuaciones en (5.21), siendo la resultante entre ambas un nuevo valor $\delta(n,I)$ cuya no anulación equivale a la del discriminante $\Delta(n,I)$ y a la inexistencia de soluciones para (5.21). Salvo que p divida al entero μ igual al máximo común divisor de los coeficientes líder de ambas ecuaciones, la no anulación módulo p de la resultante $\delta(n,I)$ caracteriza asimismo la inexistencia de

solución sobre $\overline{\mathbb{F}}_p$ del mismo sistema (5.21). Más aún, con la única posible excepción de los primos que dividen a μ, los divisores primos de $\Delta(n,I)$ y de $\delta(n,I)$ son los mismos, según 5.6.11, siendo $\delta(n,I)$ un entero —posiblemente enorme— dado explícitamente por la fórmula de la resultante, que es una fórmula aritmética en los datos (n,I).

Como aplicaciones, y entre otras, se tiene que el problema de Casas-Alvero con cuatro monomios se puede enfocar con las tres etapas comentadas al inicio de la introducción; que la resolución por elevación dispone de un método aritmético viable para la I-conjetura cuando I_p tiene cardinal 3 y que, para valores pequeños del grado, los primos en el nivel 3 de ineficiencia son calculables.

La Memoria concluye mostrando que, para todo valor de n, la conjetura de Casas-Alvero de grado n admite formulaciones aritméticas, al enunciarla como la imposibilidad de determinada igualdad numérica. Con este fin, se define el *superdiscriminante para el grado n* como el entero dado por

$$D_n = \prod_{i=1}^{n-2} \Delta(n, I_i), \qquad \text{donde } \; I_i = \{i, i+1, \ldots, n-2\}, \;\; 0 < i < n-1,$$

y, como alternativa, el *superdiscriminante dinámico* como

$$\widetilde{D}_n = \prod_{i \in A} \Delta(n, I_i), \quad \text{siendo } A = \left\{ i \in \{1, \ldots, n-2\} \,\middle|\, \text{aún se ignora si } \Delta(n, I_i) \text{ es nulo o no} \right\}$$

—así por ejemplo, $\widetilde{D}_n = D(n, I_1)$ si es $n = p^r + 1$ o $2p^r + 1$, en caso de que la conjetura no se haya probado previamente para el valor n en cuestión—. Por construcción, el superdiscriminante permite resumir la conjetura de Casas-Alvero en grado n en que se verifique $D_n \neq 0$; no-igualdad que, dinámicamente, puede traducirse en su equivalente más simple, $\widetilde{D}_n \neq 0$. Los enteros D_n y $\widetilde{D}_n$ no tienen, sin embargo, el mismo alcance: como muestra el teorema 5.6.13, disponer de primo p que no divida a $\widetilde{D}_n$ equivale a saber que la conjetura de Casas-Alvero es cierta en grado n, pero disponer de un primo p que no divida a D_n garantiza que p es un primo eficaz para n y por tanto demuestra que la conjetura de Casas-Alvero es cierta para todos los grados de la forma np^r.

Se concluye del párrafo anterior que todos los primos ineficaces con n se encuentran en la factorización de D_n. Para $n = 3, 4, 5$, el conjunto de divisores primos de D_n coincide exactamente con el de los primos ineficaces con n; no está sin embargo descartado que, en otros grados, pueda darse una contención estricta.

Capítulo 1

El enunciado del problema

El *Problema* de Casas-Alvero consiste en averiguar si la llamada *Conjetura de Casas-Alvero* es cierta o no.

Conjetura de Casas-Alvero. *Sea $P_n(X)$ un polinomio mónico de grado n con coeficientes en el cuerpo $\mathbb{C}$ de los números complejos. Si $P_n(X)$ comparte una raíz con cada una de sus $n-1$ primeras derivadas $P_n'(X), P_n''(X), \ldots, P_n^{(n-1)}(X)$ —esto es, si para cada $i=1,\ldots,n-1$, existe $\alpha_i \in \mathbb{C}$ tal que $P_n(\alpha_i) = P_n^{(i)}(\alpha_i) = 0$— entonces existe $\alpha \in \mathbb{C}$ tal que $P_n(X) = \big(X-\alpha\big)^n$.*

Conviene remarcar que la hipótesis de este enunciado se compone exactamente de $n-1$ afirmaciones independientes acerca de $P_n(X)$ en cada una de las cuales aparece involucrada una sola de sus sucesivas derivadas; ninguna relación se conoce a priori entre dos derivadas de diferente orden.

En cuanto a las raíces α_1, $\alpha_2, \ldots, \alpha_{n-1}$ que $P_n(X)$ comparte respectivamente con su derivada primera, segunda, etc, en ningún momento se dice que hayan de ser distintas (situación que por otro lado, de poder darse, sería incompatible con la tesis del enunciado). Tampoco se presupone que todas ellas sean iguales: bajo esa suposición el enunciado sería una completa obviedad, pues se estaría diciendo que $P_n(X)$ posee una raíz de multiplicidad n que entonces, por cuestión de grados, habrá de ser única. Así pues, en el enunciado de la conjetura las hipótesis establecen la mera existencia de los $n-1$ números α_i sin ocuparse de si puede haber o no coincidencias entre ellos, mientras que la tesis equivale a que esos $n-1$ números sean iguales. Se concluye entonces que la conjetura puede reescribirse en la siguiente forma:

Conjetura de Casas-Alvero. *Sea $P_n(X)$ un polinomio mónico de grado n con coeficientes complejos. Si para cada $i=1,\ldots,n-1$ existe $\alpha_i \in \mathbb{C}$ tal que $P_n(\alpha_i) = P_n^{(i)}(\alpha_i) = 0$ entonces $\alpha_1 = \alpha_2 = \ldots = \alpha_{n-1}$.*

En la formulación de la conjetura de Casas-Alvero, la condición de ser mónico $P_n(X)$ puede suprimirse sin más peaje que sustituir, en la tesis del enunciado, el que sea $P_n(X) = (X-\alpha)^n$ por que sea $P_n(X) = (\lambda X - \mu)^n$ para ciertos $\lambda, \mu \in \mathbb{C}$, ya que $\mathbb{C}$ es algebraicamente cerrado. Al reescribir la conjetura en términos de las α_i no hay ya ninguna distinción entre el caso mónico y el general, luego es innecesario considerar este aspecto.

1.1. Preparación de Tschirnhausen

Tratando de normalizar de un modo conveniente este problema, se va a fijar el valor de la raíz α_{n-1} que $P_n(X)$ comparte con $P_n^{(n-1)}(X)$ haciendo que sea igual a 0. Veremos que esta condición sobre el polinomio no supondrá pérdida de generalidad en la conjetura de Casas-Alvero.

Observación 1.1.1. $P_n^{(n-1)}(X)$ tiene a 0 como única raíz si y solo si el polinomio $P_n(X)$ carece de término de grado $n-1$ (término *vicelíder*).

En efecto, si $P_n(X) = X^n + a_1 X^{n-1} + \cdots + a_n$, entonces su derivada $(n-1)$-ésima es $P_n^{(n-1)}(X) = n!\, X + (n-1)!\, a_1$, cuya raíz, $\alpha = -\frac{a_1}{n}$, es nula si y solo si es $a_1 = 0$.

Proposición 1.1.2. *La conjetura de Casas-Alvero es verdadera si y solo si es verdadera cuando se refiere exclusivamente a los polinomios que tienen nulo el coeficiente del término vicelíder.*

Demostración. En el caso de ser $a_1 \neq 0$, se puede hacer en $P_n(X)$ el cambio de variable $X = Y - \frac{a_1}{n}$, obteniendo:

$$P_n(X) = Y^n + \left[-\binom{n}{1}\frac{a_1}{n} + a_1\binom{n-1}{0}\right] Y^{n-1} + (\text{términos de menor grado}) = Q(Y)$$

El paso de $P_n(X)$ a $Q(Y)$ se conoce como *transformación de Tschirnhausen*; observemos que provoca la cancelación del término vicelíder en $Q(Y)$. Supongamos ahora que $P_n(X)$ satisface las hipótesis de Casas-Alvero, de modo que para cada $i = 1, \ldots, n-1$ se tiene: $P_n(\alpha_i) = P_n^{(i)}(\alpha_i) = 0$ para cierto $\alpha_i \in \mathbb{C}$. Tomando, para cada i, $\beta_i = \alpha_i + \frac{a_1}{n}$, se tendrá:

$$Q(\beta_i) = P_n\big(\beta_i - \tfrac{a_1}{n}\big) = P_n(\alpha_i) = 0$$

y además, según la regla de la cadena, se cumplirá

$$Q^{(i)}(\beta_i) = P_n^{(i)}\big(\beta_i - \tfrac{a_1}{n}\big) = P_n^{(i)}(\alpha_i) = 0.$$

Si nos constara que la conjetura de Casas-Alvero es verdadera cuando se refiere a polinomios sin término vicelíder, entonces podríamos aplicársela a $Q(Y)$, ya que cumple todos los requisitos, obteniendo

$$Q(Y) = (Y-\beta)^n \quad \text{y, en consecuencia,} \quad P_n(X) = Q(Y) = \Big[X-\big(\beta-\tfrac{a_1}{n}\big)\Big]^n.$$

Hemos demostrado que, de ser verdadera esta versión *débil* de la conjetura, lo sería también la versión ordinaria. El recíproco es obvio. □

En lo sucesivo, pues, $P_n(X) = X^n + \sum_{i=1}^{n} a_i\, X^{n-i}$ será un polinomio carente de término vicelíder (esto es, con $a_1 = 0$) y que cumple las hipótesis de Casas-Alvero. Según la observación 1.1.1, $P_n{}^{(n-1)}(X)$ posee a 0 como única raíz; decir que la comparte con $P_n(X)$ significa que $P_n(0) = 0$, o lo que es lo mismo, que $a_n = 0$. Y, en estas condiciones, un valor de α para el cual sea $P_n(X) = \big(X-\alpha\big)^n$ no puede ser otro que $\alpha = 0$. Todo ello, junto con la proposición 1.1.2, permite reescribir la conjetura de Casas-Alvero de la siguiente manera:

Conjetura de Casas-Alvero. *Sea* $P_n(X) = X^n + a_2\, X^{n-2} + \cdots + a_{n-1}X \in \mathbb{C}[X]$. *Si* $P_n(X)$ *comparte una raíz con cada uno de los polinomios* $P_n{}'(X)$, $P_n{}''(X)$, …, $P_n{}^{(n-2)}(X)$, *entonces* $P_n(X) = X^n$.

Como podemos apreciar, fijar $\alpha_{n-1} = 0$ nos libra de las indeterminadas a_1 y a_n, y nos ahorra un ítem en el listado de hipótesis —el referente a $P_n{}^{(n-1)}(X)$, que ya ha rendido su servicio—; además, da una forma mucho más manejable a la tesis de la conjetura, que deja de ser existencial y queda reducida a la verificación de una igualdad.

1.2. Presentación binómica del polinomio. La derivada neta

Poniendo $a_k = \binom{n}{k} b_k$, el polinomio mónico de grado n y coeficientes complejos genérico, $P(X)$, adopta la forma

$$P(X) = X^n + \tbinom{n}{1} b_1\, X^{n-1} + \tbinom{n}{2} b_2\, X^{n-2} + \ldots + \tbinom{n}{n-i} b_{n-i}\, X^i + \ldots + \tbinom{n}{n-1} b_{n-1}\, X + \tbinom{n}{n} b_n$$

a la que denominaremos *presentación binómica* del polinomio en alusión a los coeficientes binómicos $\binom{n}{k}$ que figuran explícitamente en ella.

Cuando se deriva un polinomio se incorpora un nuevo factor a cada uno de sus términos, pero no se trata de un factor común. Empleando la presentación binómica, la elemental igualdad

$$\tbinom{n}{k} \cdot (n-k) = n \cdot \tbinom{n-1}{k}$$

permitirá captar un factor n en cada uno de los términos de $P'(X)$, pues se tiene:

$$\left[X^n + \sum_{k=1}^{n} \binom{n}{k} b_k \, X^{n-k} \right]' = n \; X^{n-1} + \sum_{k=1}^{n-1} n \binom{n-1}{k} b_k \; X^{n-k-1}.$$

Definición 1.2.1. Llamaremos *derivada neta* del polinomio $P(X) = X^n + \sum_{k=1}^{n} \binom{n}{k} b_k \, X^{n-k}$ al polinomio

$$P^{[1]}(X) := \frac{1}{n} \cdot P'(X) = \; X^{n-1} + \sum_{k=1}^{n-1} \binom{n-1}{k} b_k \; X^{n-k-1},$$

e iterando (puesto que $P^{[1]}(X)$ está dado en la presentación binómica adecuada a su grado, y podemos proceder con él del mismo modo) se define la *derivada neta de orden i* como el polinomio:

$$P^{[i]}(X) := \frac{1}{n(n-1)\cdots(n-i+1)} \cdot P^{(i)}(X) = \; X^{n-i} + \sum_{k=1}^{n-i} \binom{n-i}{k} b_k \; X^{n-k-i}.$$

Es decir, hallar la derivada neta de orden i de un polinomio presentado en forma binómica consiste simplemente en rebajar en i unidades tanto el grado de cada término como el número superior de cada coeficiente binómico.

Cada polinomio ${P_n}^{[i]}(X)$ presenta obviamente las mismas raíces sobre los complejos que $P^{(i)}(X)$, pero está descargado de factores engorrosos y tiene una expresión sencilla que es esencialmente la misma para cualquier i y que se ajusta al mismo patrón que el polinomio de partida $P(X)$. Además, conserva la *monicidad* de este. Por todas estas razones (a las que debe el nombre que ha recibido), la derivada neta será una herramienta apta y muy conveniente para el tratamiento del problema de Casas-Alvero.

No deben confundirse las derivadas netas con las derivadas de Hasse, bien conocidas y de frecuente uso en la literatura, que se definen como sigue: Dado $P(X) = X^n + \sum_{k=1}^{n} a_k \, X^{n-k}$, se denomina *derivada de Hasse de $P(X)$ de orden i* al polinomio

$$P^{<i>}(X) := \frac{1}{i\,!} \cdot P^{(i)}(X) = \binom{n}{i} X^{n-i} + \sum_{k=1}^{n-i} \binom{n-k}{i} a_k \; X^{n-k-i}.$$

Es clara la relación: $P^{<i>}(X) = \binom{n}{i} P^{[i]}(X)$.

Las derivadas netas constituyen una alternativa a las derivadas de Hasse, respecto de las cuales presentan algunos rasgos diferenciales interesantes. Obsérvese por ejemplo que $P^{[i]}(X)$ es mónico, no así $P^{<i>}(X)$. Además, contrariamente a la de Hasse, la derivada neta de orden i sí es el resultado de aplicar i veces consecutivas la derivación neta de orden 1, ya que la forma de realizar esta es intrínseca al polinomio sobre el que actúa (depende solo de su grado, y no del dato circunstancial del orden de derivación en que se

halla). Como consecuencia de ello, la derivación neta sí satisface la propiedad, ordinaria en la derivación usual pero que falta en la de Hasse, de ser

$$\Big(P^{[i]}(X)\Big)^{[j]} = P^{[i+j]}(X), \quad \forall i, j \in \mathbb{N}.$$

Para finalizar la sección veremos cómo se enuncia la conjetura de Casas-Alvero cuando se emplea la presentación binómica para el polinomio $P_n(X)$, al que se supone ya sin término vicelíder, y se habla de las derivadas netas en lugar de las ordinarias (lo cual no altera el significado de las hipótesis dado que las raíces son las mismas en uno y otro caso).

Conjetura de Casas-Alvero. *Se considera el polinomio de coeficientes complejos*

$$P_n(X) = X^n + \tbinom{n}{2} b_2 X^{n-2} + \cdots + \tbinom{n}{n-i} b_{n-i} X^i + \cdots + \tbinom{n}{n-2} b_{n-2} X^2 + \tbinom{n}{n-1} b_{n-1} X.$$

Si $P_n(X)$ comparte una raíz con cada uno de los polinomios

$$\begin{aligned}
P_n^{[1]}(X) &= X^{n-1} + \tbinom{n-1}{2} b_2 X^{n-3} + \cdots + \tbinom{n-1}{n-i} b_{n-i} X^{i-1} + \cdots + \tbinom{n-1}{n-2} b_{n-2} X + \tbinom{n-1}{n-1} b_{n-1}, \\
P_n^{[2]}(X) &= X^{n-2} + \tbinom{n-2}{2} b_2 X^{n-4} + \cdots + \tbinom{n-2}{n-i} b_{n-i} X^{i-2} + \cdots + \tbinom{n-2}{n-2} b_{n-2}, \\
&\vdots \\
P_n^{[i]}(X) &= X^{n-i} + \tbinom{n-i}{2} b_2 X^{n-2-i} + \cdots + \tbinom{n-i}{n-i} b_{n-i}, \\
&\vdots \\
P_n^{[n-2]}(X) &= X^2 + \tbinom{2}{2} b_2,
\end{aligned}$$

entonces $P_n(X) = X^n$, esto es: $b_2 = b_3 = \ldots = b_{n-1} = 0$.

Nótese que, como ya se ha indicado, los polinomios $P_n^{[i]}(X)$ no son otra cosa que los correspondientes polinomios de grado $n-i$ presentados en forma binómica; es decir, se tiene

$$P_n^{[i]}(X) = P_{n-i}(X);$$

en el enunciado anterior, por tanto, se puede sustituir $P_n^{[i]}(X)$ por $P_{n-i}(X)$ cuando resulte conveniente.

1.3. Formulación mediante resultantes

Dados dos polinomios $P(X) = \sum_{i=0}^{n} a_i X^{n-i}$, $Q(X) = \sum_{i=0}^{m} b_i X^{m-i}$ con coeficientes en un cuerpo $\mathbb{K}$, la *resultante* de $P(X)$ y $Q(X)$, que se denota $\mathrm{Res}\big(P, Q\big)$, es el valor del deter-

minante

$$\left|\begin{array}{ccccccccccc}
a_0 & a_1 & \ldots & \ldots & a_n & & & & & & \\
 & a_0 & a_1 & \ldots & \ldots & a_n & & & & & \\
 & & \cdots\cdots\cdots\cdots\cdots & & & & & & & & \\
 & & & \cdots\cdots\cdots\cdots\cdots & & & & & & & \\
 & & & & \cdots\cdots\cdots\cdots\cdots & & & & & & \\
 & & & & & a_0 & a_1 & \ldots & \ldots & a_n & \\
b_0 & b_1 & \ldots & \ldots & \ldots & \ldots & b_m & & & & \\
 & b_0 & b_1 & \ldots & \ldots & \ldots & \ldots & b_m & & & \\
 & & \cdots\cdots\cdots\cdots\cdots\cdots\cdots & & & & & & & & \\
 & & & b_0 & b_1 & \ldots & \ldots & \ldots & \ldots & b_m &
\end{array}\right| \begin{array}{l} \left.\vphantom{\begin{array}{c}a\\a\\a\\a\\a\end{array}}\right\} m \\ \left.\vphantom{\begin{array}{c}a\\a\\a\\a\\a\end{array}}\right\} n \end{array} \tag{1.1}$$

(los espacios en blanco se suponen ocupados por ceros).

En caso de ser $a_0 = b_0 = 0$, esto es, si ambos polinomios poseen grados estrictamente inferiores a los que formalmente se les ha supuesto en la construcción descrita, la resultante será nula pues la primera columna del determinante no contendrá más que ceros.

Si es solamente uno de los polinomios el que está en ese supuesto (por ejemplo, si $b_0 = 0$ pero $a_0 \neq 0$) entonces el desarrollo del determinante por su primera columna, iterado tantas veces como sea la diferencia $m-r$ entre el grado m atribuido a $Q(X)$ y su verdadero grado r, conduce a un resultado idéntico, salvo por la aparición del factor no nulo ${a_0}^{m-r}$, al que se hubiera obtenido con una atribución correcta de grado a $Q(X)$.

Y, para el caso en que es $a_0 \cdot b_0 \neq 0$, es bien conocido lo siguiente: La búsqueda de polinomios $A(X)$ y $B(X)$ tales que

$$\operatorname{gr}\big(A(X)\big) < m, \quad \operatorname{gr}\big(B(X)\big) < n, \quad \text{y se cumpla:} \quad A(X) \cdot P(X) - B(X) \cdot Q(X) = 0$$

produce un sistema de ecuaciones lineales con $n+m$ ecuaciones y $n+m$ incógnitas (los coeficientes de los polinomios buscados) que es homogéneo y cuya matriz de coeficientes es —salvo trasposición y el cambio de signo de algunas líneas— la que se muestra en (1.1). Por el teorema de Cramer, la resultante se anula si y solo si existe una solución no trivial de dicho sistema, esto es, si es posible escribir

$$\frac{P(X)}{Q(X)} = \frac{B(X)}{A(X)},$$

siendo los polinomios que forman la segunda fracción de grado estrictamente menor que los de la primera. Pero este hecho equivale a que $P(X)$ y $Q(X)$ tengan un divisor común no trivial, lo cual a su vez es equivalente a que $P(X)$ y $Q(X)$ posean en el cuerpo $\overline{\mathbb{K}}$ (cierre algebraico de $\mathbb{K}$) alguna raíz en común.

En definitiva, el hecho de que dos polinomios $P(X)$ y $Q(X)$ pertenecientes a $\mathbb{K}[X]$ compartan una raíz en el cierre algebraico de $\mathbb{K}$ encuentra su traducción exacta, bien explícita y concisa, en que se cumpla la igualdad

$$\operatorname{Res}\big(P, Q\big) = 0.$$

Cuando los coeficientes a_i, b_i de los polinomios $P(X)$ y $Q(X)$ vienen dados en forma paramétrica se obtienen generalizaciones de estos hechos. Así por ejemplo, si los diferentes a_i, b_i son elementos de un anillo de polinomios $\mathbb{K}[t_1,\ldots,t_s]$ entonces $\mathrm{Res}\big(P,Q\big)$ es igualmente un polinomio en las indeterminadas $t_1,\ldots,t_s$ y coeficientes en $\mathbb{K}$, y $\mathrm{Res}\big(P,Q\big)=0$ es una ecuación con s incógnitas cada una de cuyas soluciones $\alpha=(\alpha_1,\ldots,\alpha_s)$ proporciona dos polinomios, $P_\alpha(X)$ y $Q_\alpha(X)$, tales que

- O bien $P_\alpha(X)$ o $Q_\alpha(X)$ son el polinomio cero.
- O bien son polinomios de grado estrictamente menor que n y que m, respectivamente,
- O bien $P_\alpha(X)$ y $Q_\alpha(X)$ comparten una raíz en el cuerpo $\overline{\mathbb{K}}$,

sin que las dos últimas posibilidades se excluyan mutuamente.

Como caso particular, si los coeficientes a_i, b_i se toman como indeterminadas a las que se asigna pesos iguales a su subíndice entonces $\mathrm{Res}\big(P,Q\big)$ es un polinomio del anillo graduado $\mathbb{K}[a_0,\ldots,a_n,b_0,\ldots,b_m]$ en el que $\mathrm{gr}\big(a_k\big)=k$, $\mathrm{gr}\big(b_k\big)=k$. En estas condiciones, es bien conocido que la resultante $\mathrm{Res}\big(P,Q\big)$ es, de hecho, un polinomio homogéneo pesado de grado $n\cdot m$; ello se debe a que el grado de un producto elemental no nulo surgido en el desarrollo del determinante (1.1) que tome, por orden de filas, los elementos ubicados en las columnas i_1, i_2,...,i_{n+m} respectivamente, claramente vale

$$\begin{aligned}\big(i_1-1\big)+\big(i_2-2\big)+\cdots+\big(i_m-m\big)+\big(i_{m+1}-1\big)+\cdots+\big(i_{m+n}-n\big)=\\ =\big(i_1+\cdots+i_{m+n}\big)-\big(1+2+\cdots+m\big)-\big(1+2+\cdots+n\big),\end{aligned}\tag{1.2}$$

y esta suma tiene valor fijo e igual a $n\cdot m$ pues, independientemente de qué permutación $(i_1,\ldots,i_{m+n})$ se considere, el primer paréntesis de (1.2) acoge a los $n+m$ primeros números naturales.

Nota 1.3.1. En general, los coeficientes de los polinomios $P(X)$ y $Q(X)$ serán elementos de un anillo conmutativo (y con elemento unidad) A. Entonces, la resultante $R=\mathrm{Res}\big(P,Q\big)$ definida por la expresión (1.1) es un elemento de A.

Si M es la matriz cuadrada de (1.1) y si $\bar v,\bar w$ son las $(n+m)$-uplas del anillo de polinomios $A[X]$ dadas respectivamente por

$$\bar v=\big(X^{m-1}P(X),\ldots,XP(X),P(X),X^{n-1}Q(X),\ldots,XQ(X),Q(X)\big),\quad \bar w=\big(X^{n+m-1},\ldots,X,1\big),$$

entonces se verifica la igualdad matricial

$$M\,\bar w^{\,T}=\bar v^{\,T}$$

donde el superíndice T significa traspuesta. Si interpretamos esta igualdad como un sistema lineal y tenemos en cuenta que la última coordenada de $\bar w$ es 1, se deduce de la regla de Cramer que

$$R=R\cdot 1=\det(M'),$$

donde M' es la matriz que se obtiene sustituyendo la última columna de M por $\bar{v}^{\,T}$. Desarrollando el determinante de M' por los menores de los elementos de dicha última columna se demuestra que R pertenece al ideal de A dado por $\langle P(X), Q(X)\rangle \cap A$, siendo $\langle P(X), Q(X)\rangle$ el ideal de $A[X]$ generado por los polinomios $P(X)$ y $Q(X)$.

Otra propiedad de las resultantes que nos será de utilidad —aparte de la obvia igualdad $\mathrm{Res}\big(P,Q\big) = (-1)^{nm}\mathrm{Res}\big(Q,P\big)$— es la que describe su comportamiento frente al producto de polinomios: $\mathrm{Res}\big(P_1\cdot P_2, Q\big) = \mathrm{Res}\big(P_1,Q\big)\cdot\mathrm{Res}\big(P_2,Q\big)$ (véase [Lan]).

1.3.1. Expresión en términos de variedades algebraicas

Gracias a la utilidad de la resultante para caracterizar la existencia de una raíz común a dos polinomios, el enunciado de Casas-Alvero tal como aparecía en la página 5 puede ser reescrito en la siguiente forma:

Conjetura de Casas-Alvero. *Se considera el polinomio con coeficientes complejos*

$$P_n(X) \;= X^n + \tbinom{n}{2} b_2\, X^{n-2} + \cdots + \tbinom{n}{n-i} b_{n-i}\, X^i + \cdots + \tbinom{n}{n-2} b_{n-2}\, X^2 + \tbinom{n}{n-1} b_{n-1}\, X$$

y, para cada $i = 1,\ldots,n-2$, *se considera* $H^{[i]} := \mathrm{Res}\big(P_n, P_n^{[i]}\big)$, *según definiciones previas. En estas condiciones, si se tiene* $H^{[1]} = H^{[2]} = \cdots = H^{[n-2]} = 0$, *entonces se cumple* $b_2 = b_3 = \cdots = b_{n-1} = 0$.

Si, haciendo un salto cualitativo, pasamos a considerar los coeficientes b_i del polinomio $P_n(X)$ como indeterminadas afectadas de pesos iguales a su subíndice, entonces

- Cada resultante $H^{[i]}$ es un polinomio homogéneo pesado de grado $n\cdot(n-i)$ en las variables $b_2,\ldots,b_{n-1}$ y con coeficientes enteros; con las $n-2$ resultantes que figuran en el enunciado se genera un ideal de $\mathbb{C}[b_2,\ldots,b_{n-1}]$ al cual denotaremos por $\mathcal{I}$.
- El conjunto de soluciones del sistema $H^{[1]} = H^{[2]} = \cdots = H^{[n-2]} = 0$ constituye una variedad algebraica en el espacio afín complejo $(n-2)$-dimensional; se trata concretamente de la variedad $V(\mathcal{I}) = \big\{\beta = (\beta_2,\ldots,\beta_{n-1}) \in \mathbb{C}^{n-2} \mid \quad f(\beta) = 0 \;\; \forall f \in \mathcal{I}\big\}$.
- Las condiciones $b_2 = b_3 = \cdots = b_{n-1} = 0$ definen la variedad algebraica $V\big(\langle b_2,\ldots,b_{n-1}\rangle\big)$, formada por un único punto —precisamente, el origen— del espacio afín $\mathbb{C}^{n-2}$.

De este modo, el enunciado anterior pasa a expresarse como sigue:

Conjetura de Casas-Alvero. *Sea* $P_n(X) = X^n + \tbinom{n}{2} b_2\, X^{n-2} + \cdots + \tbinom{n}{n-1} b_{n-1}\, X$, *y sea, para cada* $i = 1,\ldots,n-2$, *el polinomio* $H^{[i]} := \mathrm{Res}\big(P_n, P_n^{[i]}\big) \in \mathbb{C}\big[b_2,\ldots,b_{n-1}\big]$. *Entonces, en el espacio afín* $\mathbb{C}^{n-2}$, *la variedad asociada al ideal* $\mathcal{I} = \big\langle H^{[1]}, H^{[2]}, \ldots, H^{[n-2]}\big\rangle$ *no contiene más puntos que el origen; esto es, se tiene:* $V(\mathcal{I}) = V\big(\langle b_2,\ldots,b_{n-1}\rangle\big)$.

Observación 1.3.2. Es claro que el ideal $\mathcal{I}$ es distinto del ideal maximal $\mathcal{J}=\langle b_2,\ldots,b_{n\text{-}1}\rangle$, en el cual está estrictamente contenido. En efecto, $\mathcal{I}$ está generado por $n-2$ polinomios homogéneos pesados de grado $n\cdot(n-1)$, $n\cdot(n-2)$, $\ldots$, $3n$ y $2n$, respectivamente; no puede por tanto contener polinomios de grado inferior a $2n$. Cada b_i tiene grado i, con $i\leq n-1$, así que, de hecho, ninguno de los b_i se encuentra en $\mathcal{I}$.

1.3.2. Expresión en términos de ideales

La tesis del enunciado de Casas-Alvero se ha reducido a la igualdad entre dos variedades algebraicas:

$$V\big(\langle H^{[1]},H^{[2]},\ldots,H^{[n\text{-}2]}\rangle\big)=V\big(\langle b_2,\ldots,b_{n\text{-}1}\rangle\big). \tag{1.3}$$

Dado que el problema está planteado sobre el cuerpo algebraicamente cerrado de los números complejos, es aplicable el teorema de los Ceros de Hilbert, según el cual la igualdad (1.3) entre las dos variedades es equivalente a la igualdad entre los *radicales* de los respectivos ideales $\mathcal{I}=\langle H^{[1]},H^{[2]},\ldots,H^{[n\text{-}2]}\rangle$ y $\mathcal{J}=\langle b_2,\ldots,b_{n\text{-}1}\rangle$. Y, puesto que $\mathcal{J}$, por ser primo, coincide con su propio radical, el problema de Casas-Alvero se transforma en verificar la verdad o falsedad del siguiente enunciado:

Conjetura de Casas-Alvero. *Sea $\mathcal{I}$ el ideal de $\mathbb{C}\big[b_2,\ldots,b_{n\text{-}1}\big]$ definido en la forma antedicha. Se verifica la igualdad:* $\operatorname{Rad}\big(\mathcal{I}\big)=\langle b_2,\ldots,b_{n\text{-}1}\rangle$.

Observación 1.3.3. Ningún polinomio $f\in\mathbb{C}\big[b_2,\ldots,b_{n\text{-}1}\big]\smallsetminus\mathcal{J}$ pertenece al radical de $\mathcal{I}$, pues un término independiente no nulo en f no desaparece por más que f se eleve a la r-ésima potencia, con lo cual es imposible que f^r se halle en el ideal homogéneo $\mathcal{I}$, sea cual sea el exponente r. Esto prueba la inclusión de $\operatorname{Rad}\big(\mathcal{I}\big)$ en el ideal $\mathcal{J}$, así que la dificultad real del problema de Casas-Alvero reside en la inclusión contraria. Es decir, la cuestión pendiente es determinar la pertenencia o no de los elementos $b_2,\ldots,b_{n\text{-}1}$ al ideal $\operatorname{Rad}\big(\mathcal{I}\big)$.

Es bien conocido el siguiente criterio:

Proposición 1.3.4 (Criterio de pertenencia al radical). *Sea $\mathbb{K}$ un cuerpo arbitrario, sea $I=\langle f_1,\ldots,f_s\rangle$ un ideal del anillo $R=\mathbb{K}[x_1,\ldots,x_n]$ y sea $f\in R$. Entonces f pertenece al ideal $\operatorname{Rad}\big(I\big)$ si y solo si el polinomio 1 pertenece al ideal $\tilde{I}=\big\langle f_1,\ldots,f_s,1-zf\big\rangle$ del anillo $\widetilde{R}=\mathbb{K}[x_1,\ldots,x_n,z]$ (en cuyo caso, $\tilde{I}=\widetilde{R}$).*

Demostración. Ver [CLS], página 177. □

Aparece así una nueva formulación de la conjetura de Casas-Alvero, consistente en postular la pertenencia de los b_i al radical de $\mathcal{I}$ en la forma equivalente dada por 1.3.4:

Conjetura de Casas-Alvero. *Sea* $\mathcal{I}=\langle H^{[1]}, H^{[2]}, \ldots, H^{[n-2]}\rangle \subset \mathbb{C}[b_2, \ldots, b_{n-1}]$. *Entonces, para cada* $i=2, \ldots, n-1$, *el ideal* $\widetilde{\mathcal{I}}_i=\langle H^{[1]}, H^{[2]}, \ldots, H^{[n-2]}, 1-zb_i\rangle$ *del anillo* $\widetilde{R}=\mathbb{C}[b_2, \ldots, b_{n-1}, z]$ *contiene al elemento unidad de dicho anillo (y se cumple, por tanto,* $\widetilde{\mathcal{I}}_i=\widetilde{R}$*).*

1.3.3. Empleo de bases de Gröbner

En el anillo $\mathbb{K}[x]$ de los polinomios en una variable con coeficientes en un cuerpo $\mathbb{K}$, el problema de averiguar si un polinomio f pertenece o no a un ideal dado, $I=\langle g\rangle$ —en $\mathbb{K}[x]$ todos los ideales son principales— se resuelve sin más que dividir f entre g según el algoritmo clásico, y observar si el resto obtenido es o no nulo. Esta estrategia se extiende al anillo de los polinomios en varias variables, pero para lograrlo ha sido preciso crear herramientas específicas capaces de superar ciertas obstrucciones que no se producen en el caso de una variable.

En el anillo $\mathbb{K}[x_1, \ldots, x_n]$ los ideales ya no son genéricamente principales, aunque sí finitamente generados (teorema de la Base de Hilbert), es decir, de la forma $I=\langle f_1, f_2, \ldots, f_s\rangle$. Cualquier algoritmo de división destinado a calcular, para un polinomio dado f, los *cocientes* $a_1, \ldots, a_s$ y el *resto* r que, bajo ciertas especificaciones, cumplan

$$f=a_1f_1+a_2f_2+\cdots+a_sf_s+r,$$

necesita apoyarse en la previa ordenación de los monomios que permita identificar al *término líder* tanto en el *dividendo* f como en los *divisores* $f_1, \ldots, f_s$. No hay una forma única de satisfacer este requerimiento; es preciso elegir un *orden monomial* entre un abanico de ellos entre los cuales no hay ninguno que sea canónico o más natural que los otros.

Una vez fijado un orden monomial, el algoritmo de división consiste en cancelar de forma sistemática el término líder del dividendo (que se actualiza cada vez) mediante la sustracción de algún producto de la forma $c_{ij}m_{ij}f_i$ (siendo $c_{ij}\in\mathbb{K}$ y siendo m_{ij} un monomio); cuando el término líder no sea cancelable por este procedimiento se le transfiere al resto, que se constituye por acumulación. El proceso se termina cuando se hace nulo el dividendo, y entonces, para cada $i=1, \ldots s$, se tiene $a_i=\sum c_{ij}m_{ij}$. El problema, no menor, es que el uso de los divisores f_i está priorizado según el orden en que han sido listados; si se hace una permutación en la lista $(f_1, \ldots, f_s)$ entonces el mismo algoritmo producirá resultados posiblemente diferentes de los anteriores; y no solo pueden obtenerse cocientes distintos sino que incluso puede ser distinto el resto que se obtenga. En particular, puede ocurrir que al aplicar el algoritmo de división a un polinomio $f=\sum b_if_i\in I$ resulte $f=a_1f_1+a_2f_2+\cdots+a_sf_s+r$ con $r\neq 0$. Esto es, el test de pertenencia al ideal I tal como lo habíamos imaginado puede producir "falsos negativos". Esta patología es la que vienen a resolver las llamadas *bases de Gröbner*.

Una base de Gröbner es un sistema de generadores $G=\{g_1,\dots g_t\}$ para el ideal I cumpliendo la propiedad adicional de que para todo elemento $f\in I$, $f\neq 0$, el término líder de f sea múltiplo del término líder de algún $g_i\in G$; por este motivo, será imposible que el algoritmo de división de un elemento de I entre los elementos de G produzca resto no nulo. Es notable el hecho de que la propiedad calificada aquí como *adicional* constituye en realidad una condición *suficiente* para que un subconjunto G de I genere al ideal I.

A partir de un sistema de generadores ordinario $B=\{f_1,\dots,f_s\}$ puede construirse una base de Gröbner para I mediante el algoritmo de Buchberger, que básicamente consiste en ir generando e incorporando a B nuevos polinomios del ideal, en un modo tal que cada polinomio recién llegado aporte un término líder que no sea múltiplo de ninguno de los términos líderes preexistentes en B. Un polinomio así, se obtiene a partir de una pareja f_i, f_j cuyo S-polinomio deje resto no nulo al ser dividido por la totalidad de los elementos de B; justamente ese resto se tomará para ser un nuevo f_k añadido a B. (El S-polinomio de f_i y f_j se calcula como sigue:

$$S(f_i,f_j)=u\,f_i-v\,f_j,$$

donde u y v están elegidos de modo que los respectivos términos líder de uf_i y de vf_j sean del mínimo grado posible que permita su cancelación mutua.)

Cuando los emparejamientos se hacen en forma sistemática (incluyendo en cada etapa a los recién llegados) termina alcanzándose un status en que ya ningún S-polinomio deja resto no nulo; exactamente este comportamiento caracteriza a una base de Gröbner, luego B se ha convertido en una de ellas.

Esta base de Gröbner puede tener gran cantidad de elementos superfluos: todos aquellos elementos de B cuyo término líder sea múltiplo del término líder de algún otro compañero pueden suprimirse sin que el conjunto deje de ser una base de Gröbner para I; se habrá obtenido así una base de Gröbner *minimal* para dicho ideal. No hay unicidad para las bases de Gröbner minimales; sin embargo, partiendo de una cualquiera de ellas y mediante un proceso de sustracción para eliminar de cada polinomio todos aquellos términos que sean múltiplos de algún término líder, se llega a una base de Gröbner *reducida*. Cada ideal I posee una única base de Gröbner reducida; este hecho proporciona un criterio de igualdad para ideales: I y J son el mismo ideal si y solo si al calcular sendas bases de Gröbner reducidas se obtiene el mismo resultado.

Regresando al problema de Casas-Alvero, para estudiar si es o no cierta la igualdad

$$\mathrm{Rad}\big(\mathcal{I}\big)=\big\langle b_2,\dots,b_{n\text{-}1}\big\rangle$$

no podemos recurrir al criterio de comparar las respectivas bases de Gröbner reducidas puesto que no disponemos de un sistema de generadores para $\mathrm{Rad}\big(\mathcal{I}\big)$ desde el cual iniciar

los cálculos. Ahora bien: tras la última reformulación del enunciado (página 10), el objetivo es comprobar si se cumplen o no las $n-2$ igualdades ($i=2,\ldots,n-1$):

$$\widetilde{\mathcal{I}}_i := \langle H^{[1]}, H^{[2]}, \ldots, H^{[n\text{-}2]}, 1-z\,b_i\rangle \;=\; \mathbb{C}\big[b_2,\ldots,b_{n\text{-}1},z\big] := \widetilde{R},$$

cada una de las cuales toma en consideración un ideal, $\widetilde{\mathcal{I}}_i$, del que se conoce de forma explícita un sistema de generadores, $B_i = \{H^{[1]}, H^{[2]}, \ldots, H^{[n\text{-}2]}, 1-z\,b_i\}$. Debido al carácter singular del ideal total $\widetilde{R}$ (cuya base de Gröebner reducida es, evidentemente, $\{1\}$), cada una de estas igualdades será cierta si y solo si al aplicarle a B_i el algoritmo de Buchberger aparece en algún momento un polinomio unidad.

Estas reflexiones conducen a la siguiente formulación para el problema de Casas-Alvero en grado n.

Conjetura de Casas-Alvero. *Se consideran los polinomios $H^{[1]}, H^{[2]}, \ldots, H^{[n-2]}$ anteriormente construidos y, para cada $i=2,\ldots,n-1$, el ideal $\widetilde{\mathcal{I}}_i = \langle H^{[1]}, H^{[2]}, \ldots, H^{[n\text{-}2]}, 1-z\,b_i\rangle$ del anillo $\widetilde{R} = \mathbb{C}\big[b_2,\ldots,b_{n\text{-}1},z\big]$, en el que se ha fijado un orden monomial cualquiera. Entonces, para todo $i=2,\ldots,n-1$, la base de Gröbner reducida de $\widetilde{\mathcal{I}}_i$ es $\{1\}$.*

Ejemplo. Para $n=4$, se tiene:
$$P_4(X) = X^4 + 6\,b_2\,X^2 + 4\,b_3\,X;$$
$$H^{[1]} = 27\big(b_3^{\,4} + 2\,b_2^{\,3}\,b_3^{\,2}\big),$$
$$H^{[2]} = 25\,b_2^{\,4} + 16\,b_2\,b_3^{\,2}.$$

La proposición 1.3.4 proporciona las siguientes equivalencias:

$$b_2 \in \mathrm{Rad}\langle H^{[1]}, H^{[2]}\rangle \iff 1 \in \widetilde{\mathcal{I}}_2 = \langle H^{[1]}, H^{[2]}, 1-b_2 z\rangle$$
$$b_3 \in \mathrm{Rad}\langle H^{[1]}, H^{[2]}\rangle \iff 1 \in \widetilde{\mathcal{I}}_3 = \langle H^{[1]}, H^{[2]}, 1-b_3 z\rangle;$$

mientras que la pertenencia del elemento unidad a un ideal queda caracterizada por la aparición de dicho elemento en una base de Gröbner del ideal.

Trabajando con el orden monomial GRLEX (graduado lexicográfico) se ha aplicado el algoritmo de Buchberger para hallar una base de Gröbner de $\widetilde{\mathcal{I}}_2$ (resp. $\widetilde{\mathcal{I}}_3$), con los resultados que se recogen en el cuadro 1.1; de este modo se ha obtenido una demostración para la conjetura de Casas-Alvero en grado $n=4$.

Los cálculos anteriores se han realizado por medio del programa DERIVE de cálculo simbólico, de extendido empleo en ámbitos docentes. Dadas las muy limitadas capacidades del DERIVE como lenguaje de programación, el algoritmo de Buchberger se ha ejecutado introduciendo una a una las órdenes para la ejecución de los sucesivos pasos, llevando enteramente el control desde fuera del programa. Esto supone, en particular, determinar por inspección la expresión precisa para generar un nuevo S-polinomio, así como localizar al divisor adecuado (y determinar su factor acompañante) para ordenar cada una de

Para $\widetilde{\mathcal{I}}_2$, se obtiene:		Para $\widetilde{\mathcal{I}}_3$, se obtiene:	
	$f_1 = \frac{1}{27} H^{[1]}$		$g_1 = \frac{1}{27} H^{[1]}$
	$f_2 = H^{[2]}$		$g_2 = H^{[2]}$
	$f_3 = b_2\, z - 1$		$g_3 = b_3\, z - 1$
$S(f_1, f_2) \rightarrow$	$f_4 = b_2\, b_3^4$	$S(g_1, g_2) \rightarrow$	$g_4 = b_2\, b_3^4$
$S(f_1, f_3) \rightarrow$	$f_5 = b_3^4\, z + 2\, b_2^2\, b_3^2$	$S(g_1, g_3) \rightarrow$	$g_5 = 2\, b_2^3\, b_3 + b_3^3$
$S(f_2, f_3) \rightarrow$	$f_6 = 25\, b_2^3 + 16\, b_3^2$	$S(g_2, g_5) \rightarrow$	$g_6 = b_2\, b_3^3$
$S(f_1, f_4) \rightarrow$	$f_7 = b_3^6$	$S(g_3, g_5) \rightarrow$	$g_7 = 2\, b_2^3 + b_3^2$
$S(f_1, f_6) \rightarrow$	$f_8 = b_3^4$	$S(g_2, g_7) \rightarrow$	$g_8 = b_2\, b_3^2$
$S(f_3, f_6) \rightarrow$	$f_9 = 16\, b_3^2\, z + 25\, b_2^2$	$S(g_3, g_8) \rightarrow$	$g_9 = b_2\, b_3$
$S(f_1, f_9) \rightarrow$	$f_{10} = b_2^2\, b_3^2$	$S(g_3, g_9) \rightarrow$	$g_{10} = b_2$
$S(f_3, f_{10}) \rightarrow$	$f_{11} = b_2\, b_3^2$	$S(g_7, g_{10}) \rightarrow$	$g_{11} = b_3^2$
$S(f_3, f_{11}) \rightarrow$	$f_{12} = b_3^2$	$S(g_3, g_{11}) \rightarrow$	$g_{12} = b_3$
$S(f_9, f_{12}) \rightarrow$	$f_{13} = b_2^2$	$S(g_3, g_{12}) \rightarrow$	$g_{13} = 1$
$S(f_3, f_{13}) \rightarrow$	$f_{14} = b_2$		
$S(f_3, f_{14}) \rightarrow$	$f_{15} = 1$		

Cuadro 1.1: Elementos generados sucesivamente mediante el algoritmo de Buchberger aplicado a los ideales $\widetilde{\mathcal{I}}_2$ y $\widetilde{\mathcal{I}}_3$

las sustracciones requeridas por el algoritmo de división. El modo de proceder adoptado (manejando siempre los polinomios mediante su nombre, asignado en el mismo momento de su obtención) garantiza que, incluso una ejecución imperfecta del algoritmo (por ejemplo, por omitir una sustracción o identificar incorrectamente un término líder) proporciona resultados válidos, pues no se da opción a que se introduzcan polinomios que no sean pertenecientes al ideal.

Se ha realizado una tentativa de aplicar la misma técnica del ejemplo anterior para el caso $n = 5$; pero enseguida resulta evidente que con cuatro indeterminadas la tarea se vuelve enormemente más penosa, no solo por el aumento en la magnitud de la combinatoria sino también por razones prácticas, como el modo en que DERIVE presenta por pantalla los resultados, y las manipulaciones requeridas para poder analizarlos. Queda por tanto de manifiesto que la herramienta que se emplea no es la más adecuada. Ahora bien:

aunque usar programas más específicos de cálculo simbólico permitiría resolver el caso $n=5$, y posiblemente algunos casos particulares más, se muestra más adelante que el caso general ofrece una obstrucción esencial a ser resuelto por este procedimiento. La obstrucción consiste en la dificultad de saber si el coeficiente del término supuestamente líder de un S-polinomio es en verdad no nulo. Como podrá apreciarse en la sección 2.4, comprobar si dicho coeficiente (dado genéricamente) es o no distinto de cero puede ser una tarea con un grado de dificultad equiparable a la de la propia conjetura.

Capítulo 2

Problemas parciales (y primeras respuestas)

En el capítulo precedente hemos fijado, para el polinomio de grado n sin término vicelíder ni término independiente y con coeficientes en $\mathbb{C}$ genérico, la que hemos llamado su presentación binómica,

$$P_n(X) = X^n + \tbinom{n}{2} b_2 X^{n-2} + \ldots + \tbinom{n}{n-i} b_{n-i} X^i + \ldots + \tbinom{n}{n-1} b_{n-1} X \tag{2.1}$$

y hemos definido la derivada neta i-ésima de $P_n(X)$ como el polinomio

$$P_n{}^{[i]}(X) = \frac{1}{n(n-1)\cdots(n-i+1)} \cdot P^{(i)}(X) = X^{n-i} + \tbinom{n-i}{2} b_2 X^{n-2-i} + \ldots + \tbinom{n-i}{n-i} b_{n-i}\,. \tag{2.2}$$

Asímismo hemos introducido la notación: $H^{[i]} = \mathrm{Res}\big(P_n(X), P_n{}^{[i]}(X)\big)$.

Como hemos visto, el problema de Casas-Alvero para grado n consiste exactamente en averiguar si X^n es el único polinomio de la forma (2.1) que comparte una raíz con cada una de sus derivadas de orden $i = 1, \ldots, n-2$ o, equivalentemente, si

$$b_2 = 0, \quad b_3 = 0, \quad \ldots \quad b_{n-1} = 0$$

es la única solución del sistema

$$\left.\begin{array}{rcl} H^{[1]} & = & 0 \\ & \vdots & \\ H^{[n-2]} & = & 0. \end{array}\right\} \tag{2.3}$$

Abordaremos este problema estableciendo versiones débiles del mismo, en las cuales no se contemplen todos los posibles polinomios de la forma (2.1) sino únicamente los que se ajusten a una particular configuración, la cual vendrá dada por el conjunto de los grados $i_1, i_2, \ldots, i_r$ de aquellos términos que tienen opción a estar efectivamente presentes (esto

es, a aparecer con coeficiente no nulo). Habrá, por consiguiente, tantos problemas débiles (o *parciales*) como subconjuntos propios admite el conjunto formado por los grados de los términos de $P_n(X)$ distintos del líder.

2.1. El problema parcial con conjunto I de exponentes

A pesar de su sencillez, el siguiente hecho será enormemente útil.

Observación 2.1.1. Si $b_{n\text{-}i}=0$, entonces la ecuación $H^{[i]}=0$ se verifica *a fortiori*.

En efecto, puesto que el término independiente de ${P_n}^{[i]}(X)$ coincide con la variable $b_{n\text{-}i}$, es evidente que si ésta se anula entonces $P_n(X)$ y ${P_n}^{[i]}(X)$ tendrán en común la raíz $\alpha=0$ y por tanto la resultante entre ambos, $H^{[i]}$, será nula. Este comportamiento significa que la indeterminada $b_{n\text{-}i}$ divide al polinomio $H^{[i]}$; a la misma conclusión se llega independientemente sin más que observar que el determinante en que por definición consiste $H^{[i]}$ lleva a $b_{n\text{-}i}$ como el único elemento diferente de cero de la última columna.

En lo sucesivo, consideraremos que se ha fijado el grado n con que se trabaja.

Definición 2.1.2. Sea $J=\{1,2,\ldots,n-2\}$, y sea $I=\{i_1<i_2<\cdots<i_r\}\subset J$. Llamaremos *$I$-polinomio* de grado n al que, aparte del término líder X^n, no lleva otros términos que no sean los de grado i_1, $i_2,\ldots,i_r$, esto es, que se ajusta a la forma

$$P_n(X)=X^n+\tbinom{n}{n\text{-}i_r}b_{n\text{-}i_r}X^{i_r}+\ldots+\tbinom{n}{n\text{-}i_2}b_{n\text{-}i_2}X^{i_2}+\tbinom{n}{n\text{-}i_1}b_{n\text{-}i_1}X^{i_1}, \tag{2.4}$$

sin que los coeficientes que aquí figuran se supongan necesariamente distintos de cero.

Restringir el campo de trabajo al de los I-polinomios equivale a imponer de antemano las $n-2-r$ condiciones de ser $b_{n\text{-}j}=0$ para todo $j\in J\smallsetminus I$; en virtud de la observación 2.1.1, para todo I-polinomio se satisfacen trivialmente las ecuaciones $H^{[j]}=0$ correspondientes a los $n-2-r$ subíndices $j\in J\smallsetminus I$. En consecuencia, el I-polinomio $P_n(X)$ que aparece en (2.4) es un contraejemplo a la conjetura de Casas-Alvero si y solo si la r-upla de números complejos $(b_{n\text{-}i_r},\ldots,b_{n\text{-}i_1})$ es una solución no trivial del sistema

$$H^{[i_1]}=0,\quad H^{[i_2]}=0,\quad \ldots\quad H^{[i_r]}=0, \tag{2.5}$$

puesto que al completar dicha r-upla con $n-2-r$ ceros ubicados en las posiciones adecuadas se tendría una solución no trivial del sistema (2.3).

Un contraejemplo de esta naturaleza será llamado un *I-contraejemplo*.

Observación 2.1.3. En rigor, dado $i\in I$, habría que distinguir entre la ecuación $H^{[i]}=0$ del sistema (2.3), en la cual aún figuran como incógnitas las $b_{n\text{-}j}$ con $j\in J\smallsetminus I$, y la ecuación

$H_*^{[i]} = 0$ donde ya esas incógnitas $b_{n\text{-}j}$ han sido sustituidas por ceros, y solo permanecen *vivas* las r incógnitas $b_{n\text{-}i_r}, \ldots, b_{n\text{-}i_1}$; entonces, desde luego, en (2.5) deberían escribirse las formas con asterisco. Sin embargo, obviaremos esta distinción ya que en la práctica no hay ningún riesgo de confundirlas, y mantendremos la notación $H^{[i]}$ aún después de haber sustituido por ceros las variables $b_{n\text{-}j}$ en cuestión. Dicho sea de paso, lo que por supuesto sí que resulta del todo indiferente es que esta sustitución —un homomorfismo de anillos de $\mathbb{C}[b_2, \ldots, b_{n\text{-}1}]$ en $\mathbb{C}[b_{n\text{-}i_r}, \ldots, b_{n\text{-}i_1}]$— se realice *antes* o *después* de haber calculado la resultante entre los polinomios $P_n(X)$ y $P_n{}^{[i]}(X)$.

Definición 2.1.4. Para cada conjunto $I = \{i_1 < i_2 < \cdots < i_r\} \subset J = \{1, 2, \ldots, n-2\}$ se define el *problema parcial de Casas-Alvero en grado n y con conjunto de exponentes I* (o, brevemente, el *I-problema* de Casas-Alvero) como aquel que consiste en averiguar si el sistema (2.5) posee únicamente la solución trivial (en cuyo caso diremos que el I-problema tiene *respuesta afirmativa*) o si, por el contrario, existe alguna solución no trivial del mismo; esto es, si existe algún I-contraejemplo al problema (total) de Casas-Alvero en grado n.

2.2. El monomio puro de una resultante, y el $\{i\}$-problema parcial

Tomando para $P_n(X)$ y $P_n{}^{[i]}(X)$ las expresiones dadas en (2.1) y (2.2) respectivamente, su resultante adopta la forma que se muestra en la figura 2.1. La disposición de los elementos en la matriz invita a visualizarla partida en 9 cajas, de las cuales, las 4 situadas en la zona superior izquierda, **A**, **B**, **C** y **D**, son cuadradas de orden $n-i$.

Proposición 2.2.1. *Se tiene:* $H^{[i]} = b_{n\text{-}i}^{\,n}\Big[1-\binom{n}{n\text{-}i}\Big]^{n\text{-}i} + b_{n\text{-}i}\,Q_i$, *donde* Q_i *es un polinomio cuyos monomios contienen todos al menos una variable* b_j *diferente de* $b_{n\text{-}i}$.

Demostración. Como ya se ha señalado en la observación 2.1.1, es claro que $H^{[i]}$ es un múltiplo de $b_{n\text{-}i}$. En particular, si aparece en $H^{[i]}$ algún monomio *puro*, esto es, que solamente involucre una indeterminada, esta habrá de ser necesariamente $b_{n\text{-}i}$, así que, por cuestión de grados, el monomio no puede ser otro que $b_{n\text{-}i}^{\,n}$. En $H^{[i]}$ hay, en total, 2^{n-i} productos elementales que contienen $b_{n\text{-}i}^{\,n}$: obviamente, el producto $\mathcal{P}$ de todos los elementos de la diagonal principal, pero también, para cada $j = 1, \ldots, n-i$, los $\binom{n\text{-}i}{j}$ productos elementales iguales a $\binom{n}{n\text{-}i}^j b_{n\text{-}i}^{\,n}$ que resultan de sustituir en $\mathcal{P}$ a j de los $n-i$ factores —de valor $b_{n\text{-}i}$ — procedentes de la diagonal de **D**, por los correspondientes factores —de valor $\binom{n}{n\text{-}i}\,b_{n\text{-}i}$ — que se encuentran en su misma vertical, en la diagonal de **B** (ver figura 2.1). A cambio, j factores de valor 1 tomados de **A** son sustituidos por otros, idénticos,

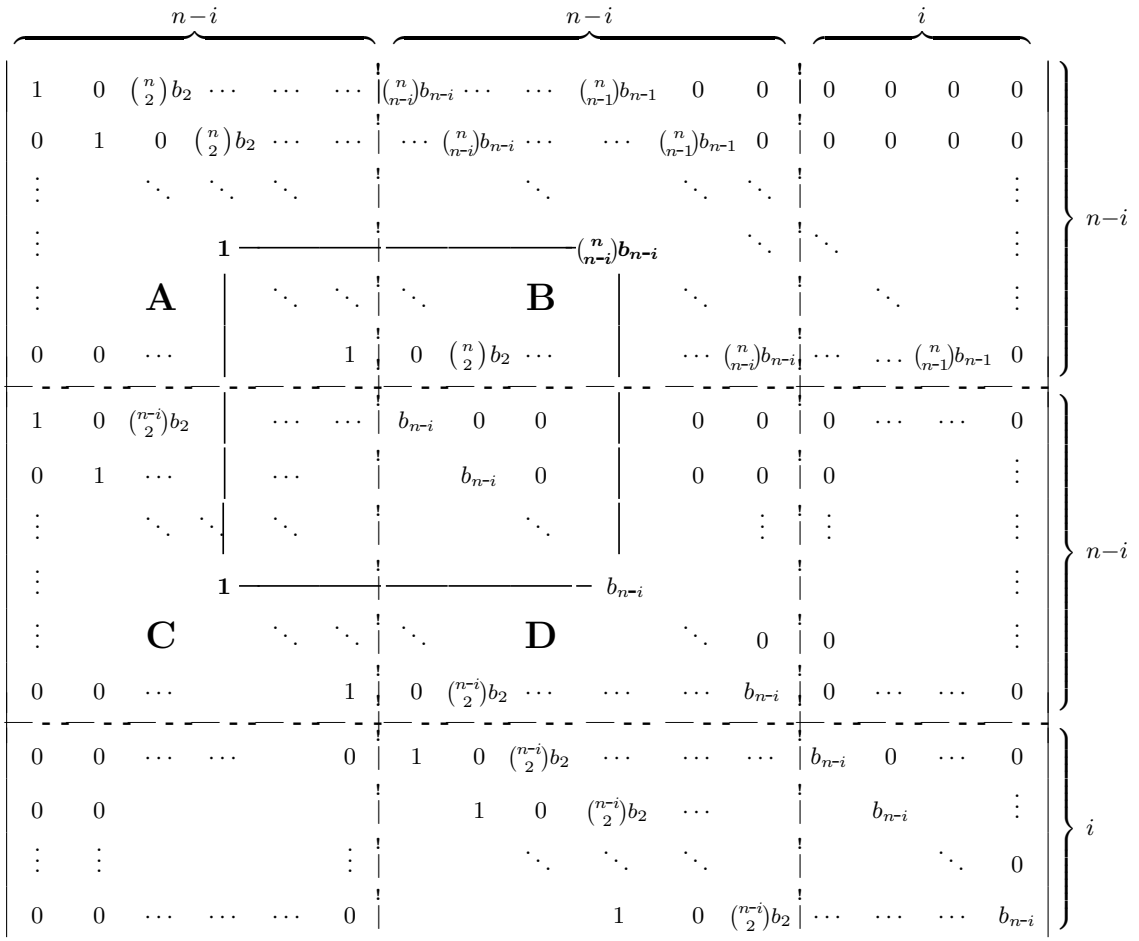


Figura 2.1: Resultante de $P_n(X)$ y $P_n{}^{[i]}(X)$.

de **C**. Estas maniobras cambian j veces la paridad del número de inversiones, por lo que los productos elementales se afectan del signo $(-1)^j$.

Asociando todos los términos de este tipo aparece el factor común $b_{n\text{-}i}^{\,n}$ que multiplica a cada término de la siguiente suma:

$$\binom{n\text{-}i}{0} - \binom{n\text{-}i}{1}\binom{n}{n\text{-}i} + \binom{n\text{-}i}{2}\binom{n}{n\text{-}i}^2 - \cdots + (-1)^j\binom{n\text{-}i}{j}\binom{n}{n\text{-}i}^j + \\ + \cdots + (-1)^{n\text{-}i}\binom{n\text{-}i}{n\text{-}i}\binom{n}{n\text{-}i}^{n\text{-}i} = \left[1 - \binom{n}{n\text{-}i}\right]^{n\text{-}i};$$

los restantes términos llevan a $b_{n\text{-}i}$ como factor común y, al menos, otra indeterminada diferente; entre todos constituyen el producto $b_{n\text{-}i}\,Q_i$. □

Proposición 2.2.2 (Caso $I=\{i\}$). *Cuando se considera el $\{i\}$-polinomio de grado n, $P_n(X) = X^n + \binom{n}{n\text{-}i} b_{n\text{-}i}\,X^i$, la única resultante no trivial es $H^{[i]} = b_{n\text{-}i}^{\,n}\left[1-\binom{n}{n\text{-}i}\right]^{n\text{-}i}$.*

Demostración. Es una consecuencia inmediata de la proposición 2.2.1, ya que todos los sumandos de Q_i contienen al menos un factor $b_{n\text{-}j}$, con $j \neq i$, que de antemano está sustituido por un cero puesto que $P_n(X)$ es un $\{i\}$-polinomio; así pues, Q_i queda anulado.

Alternativamente, si el hecho de ser nulas todas las variables $b_{n\text{-}j}$ con $j \neq i$ se traslada a la matriz mostrada en la figura 2.1, entonces el cálculo del determinante carece de dificultad. Restando cada una de las $n-i$ filas del primer bloque a su correspondiente homóloga del segundo bloque, y desarrollando por las n columnas con un único elemento no nulo que entonces presenta la matriz, solo queda calcular un determinante triangular (de hecho, diagonal) de orden n; el resultado es inmediato y, naturalmente, coincidente con el del enunciado. □

Corolario 2.2.3. *En cualquier grado, y para todo i, el $\{i\}$-problema de Casas-Alvero de grado n tiene respuesta afirmativa, esto es:*

No existen $\{i\}$-contraejemplos a la conjetura de Casas-Alvero.

Demostración. Al ser $1 \leq i \leq n-2$, el número combinatorio $\binom{n}{n\text{-}i}$ es distinto de 1; por tanto, la ecuación $H^{[i]} = 0$ que, en virtud de la proposición 2.2.2 es

$$b_{n\text{-}i}^{n}\left[1-\binom{n}{n\text{-}i}\right]^{n\text{-}i} = 0$$

no tiene en el conjunto $\mathbb{C}$ otra solución que $b_{n\text{-}i} = 0$.

2.3. El $\{i,j\}$-problema parcial

Ahora que sabemos que no existen, en ningún grado $n \in \mathbb{N}$, contraejemplos a la conjetura de Casas-Alvero que cuenten con un único término adicional al líder, es natural preguntarse si existirá algún contraejemplo con dos términos adicionales.

La respuesta a esta pregunta se descubre en esta sección. Para ello, nos será de utilidad el siguiente lema técnico.

Lema 2.3.1. *Sea M la matriz cuadrada de orden $r+s$ que se muestra en la figura 2.2, en la cual todos los elementos distintos de los indicados mediante letras o elipsis son iguales a cero. Entonces, el valor de su determinante viene dado por*

$$\det\left(M\right) = \left[A^{\rho}D^{\sigma} + (-1)^{\rho\sigma}B^{\rho}C^{\sigma}\right]^{d},$$

siendo $d = \text{m.c.d.}\left(r,s\right)$, y siendo $\rho = \frac{r}{d}$, $\sigma = \frac{s}{d}$.

Demostración. Es preciso tratar por separado los dos casos siguientes:

Caso 1: r y s primos entre sí. Los únicos elementos distintos de cero de la matriz M se encuentran dispuestos en tres líneas diagonales, que son

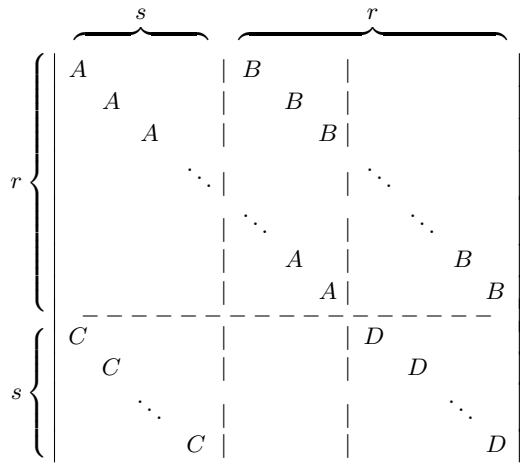


Figura 2.2: Matriz M

- La *diagonal principal*, con los elementos $m_{i,i} = \begin{cases} A, & \text{si } 1 \le i \le r \\ D, & \text{si } r+1 \le i \le r+s \end{cases}$
- La *paralela superior*, con los elementos $m_{i,i+s} = B$, para $1 \le i \le r$.
- La *paralela inferior*, con los $m_{i,i\text{-}r} = C$, para $r+1 \le i \le r+s$.

Es claro que los productos elementales $A^r D^s$ y $B^r C^s$ se encuentran en el desarrollo de $\det(M)$, yendo el segundo afectado del signo $(-1)^{rs}$, ya que la permutación de índices de columnas que le corresponde es $(s+1, s+2, \ldots, s+r, 1, 2, \ldots, s)$, sin más inversiones que las que presenta cada uno de los r primeros elementos con cada uno de los s últimos. Falta solo comprobar que todos los demás productos elementales son nulos. La táctica para ello consistirá en mostrar que la construcción de un producto elemental partiendo de un elemento de la diagonal principal, y bajo la condición de no tomar ningún elemento distinto de A, B, C o D, conduce inevitablemente al primero de los dos productos ya conocidos, $A^r D^s$, concluyéndose que no hay más productos elementales diferentes de cero que este (formado por *todos* los elementos de la diagonal principal), y $B^r C^s$, que no contiene *ningún* elemento de dicha línea.

Dado $i \le r$, en la fila del elemento $m_{i,i} = A$ ubicado en la diagonal principal solo hay otro elemento no nulo, que está situado s puestos a su derecha y es $m_{i,i+s} = B$. A su vez, en la columna de este último solamente hay otro elemento no nulo, situado s puestos más abajo, y que, por tanto, es $m_{i+s,i+s}$. En consecuencia, para formar un producto elemental $\mathcal{P}$ que evite los ceros y que contenga al factor $m_{i,i}$, dado que no podemos tomar a $m_{i,i+s}$ (pues repetiríamos fila) y que hemos de incluir un factor extraído de la columna $i+s$, necesariamente ha de tomarse para $\mathcal{P}$ el elemento $m_{i+s,i+s}$. Este elemento puede valer A

o valer D, lo cual nos es indiferente; lo significativo aquí es que se encuentra también en la diagonal principal.

Dado ahora $i > r$, razonando del mismo modo vemos que si $\mathcal{P}$ incorpora a $m_{i,i} = D$ entonces queda excluida la posibilidad de poner a $m_{i,i\text{-}r} = C$, pero eso obliga a tomar al otro elemento no nulo de la columna $i-r$, que es $m_{i\text{-}r,i\text{-}r}$, perteneciente asimismo a la diagonal principal.

Así pues, basta saber que $\mathcal{P}$ contiene *un* elemento de la diagonal principal para poder afirmar que también contiene a otro, al que se llega —según el caso— o bien avanzando s lugares o bien retrocediendo r lugares a lo largo de la diagonal. Estas dos procedimientos alternativos entre los cuales ha de elegirse el que corresponda al caso no son, sin embargo, distintos más que en apariencia: recorriendo *cíclicamente* los $r+s$ elementos de la diagonal, da lo mismo avanzar s que retroceder r lugares a partir de la posición i; comportamiento que queda descrito por la expresión $i+s \equiv i-r \mod r+s$.

En definitiva, si $m_{i,i}$ se encuentra en $\mathcal{P}$, al iterar el argumento anterior se genera una secuencia del tipo siguiente (los primeros términos son, aquí, supuestos)

$$i, \quad i+s, \quad i+2s, \quad i+2s-r, \quad i+3s-r, \quad \ldots \quad , \quad i+ks-tr, \quad \ldots \tag{2.6}$$

que proporciona —mediante la aritmética ordinaria— los índices simples (comprendidos entre 1 y $r+s$) de aquellos elementos de la diagonal principal cuya presencia en $\mathcal{P}$ se va deduciendo en pasos sucesivos a partir del dato inicial, i. De forma equivalente, empleando la aritmética modular (módulo $r+s$) obtenemos la misma secuencia de índices bajo la forma

$$i, \qquad i+s, \qquad i+2s, \qquad i+3s, \qquad i+4s, \quad \ldots \quad , \quad i+(k+t)s, \quad \ldots \tag{2.7}$$

cuando para cada uno de estos números, que son clases de equivalencia, se elige el representante comprendido entre 1 y $r+s$. En el grupo aditivo $\mathbb{Z}/_{(r+s)}$, el elemento s tiene orden igual al cardinal del grupo, $r+s$, puesto que, al ser s primo con r, lo es también con $r+s$. Esto significa que en $\mathbb{Z}/_{(r+s)}$ los $r+s$ elementos s, $2s$, $3s$, $4s$, $\ldots$, $(r+s)s$ son todos ellos distintos (y el último, igual a cero), pero entonces la secuencia dada en (2.7) es, exactamente,

$$i, \qquad i+s, \qquad i+2s, \qquad i+3s, \qquad i+4s, \quad \ldots \quad , \quad i+(r+s-1)s;$$

está formada por $r+s$ elementos *distintos* y contiene, por tanto, todas las posiciones de la diagonal principal. Queda así probado que $\mathcal{P}$ es, necesariamente, $A^r D^s$, de modo que, en definitiva, es $\det(M) = A^r D^s + (-1)^{rs} B^r C^s$. Este resultado es conforme con el enunciado del lema pues, en el caso actual, es $d = \text{m.c.d.}(r,s) = 1$, $\rho = r$, $\sigma = s$.

Caso 2: m.c.d.$(\mathbf{r},\mathbf{s}) = \mathbf{d} > 1$. A diferencia del caso anterior, en este caso sí van a existir productos elementales mixtos, esto es, que combinen factores tomados de la diagonal principal con otros procedentes de las paralelas.

Respecto del caso anterior se mantiene la validez tanto de la descripción de M como, consecuentemente, de los razonamientos para deducir que todo producto elemental $\mathcal{P}$ de M que no tome ningún cero y en el que se encuentre $m_{i,i}$ ha de contener también a los elementos de la diagonal principal cuya posición en la misma venga dada por la secuencia (2.6) en aritmética ordinaria o, equivalentemente, por la secuencia (2.7) en aritmética modular (módulo $r+s$). Sin embargo, del análisis de dichas secuencias se desprenderán esta vez conclusiones bien diferentes.

En efecto, siendo $r=\rho\, d$ y $s=\sigma d$ con ρ y σ primos entre sí, en el grupo cíclico $\mathbb{Z}/_{(r+s)}$ el elemento s tiene orden $\rho+\sigma$, dado que ks solo es divisible entre $r+s$ si $k\sigma$ lo es entre $\rho+\sigma$, y esto ocurre por primera vez para $k=\rho+\sigma$ pues m.c.d.$(\sigma,\rho+\sigma)=1$. Quiere esto decir que los $\rho+\sigma$ elementos $s,\ 2s,\ 3s,\ 4s,\ \ldots\ ,\ (\rho+\sigma)s$ son todos distintos (siendo el último, nulo) y, por lo tanto, en la secuencia (2.7), los $\rho+\sigma$ primeros términos

$$i, \qquad i+s, \qquad i+2s, \qquad i+3s, \qquad i+4s, \quad \ldots \quad , \quad i+(\rho+\sigma-1)s$$

también son todos distintos, mientras que la prolongación de dicha secuencia no hace sino replicar una y otra vez este fragmento. En particular, el término que sigue a los ya dados es, de nuevo, i.

Trasladando las anteriores conclusiones a 2.6, se tiene que sus $\rho+\sigma$ primeros términos son distintos pero a partir de ese momento todo se repite; en particular, el primer término en repetirse será de la forma $i+ks-tr$ con $k+t=\rho+\sigma$ (pues ése es el número de pasos necesarios para llegar hasta él) y, además, $i+ks-tr=i$, pues después de $\rho+\sigma$ pasos recaemos en el valor inicial. Gráficamente, tras $\rho+\sigma$ pasos se cierra el ciclo de los elementos de la diagonal principal que se visitan al iterar el razonamiento sobre los factores obligadamente presentes en $\mathcal{P}$ cuando se sabe que $m_{i,i}$ está presente. Interesa determinar el conjunto I_i que forman los índices de los elementos involucrados en dicho ciclo.

Si j pertenece a I_i, entonces j es congruente con i módulo d puesto que

$$j = i + ks - tr = i + d(k\sigma - t\rho);$$

ahora bien, en el conjunto $I=\{1,2,\ldots,r+s\}$ hay exactamente $\frac{r+s}{d}=\rho+\sigma$ números que sean congruentes módulo d con el elemento i en cuestión, luego I_i es justamente el conjunto formado por todos ellos, esto es, I_i coincide con uno de los siguientes subconjuntos de I:

$$\begin{aligned}
I_1 &= \{\ 1\ ,\ 1+d\ ,\ 1+2d\ ,\ \ \ldots\ ,1+(\rho+\sigma-1)d\ \}\\
I_2 &= \{\ 2\ ,\ 2+d\ ,\ 2+2d\ ,\ \ \ldots\ ,2+(\rho+\sigma-1)d\ \}\\
&\ \ \vdots\\
I_{d-1} &= \{d-1,\ 2d-1\ ,\ \ 3d-1\ \ ,\ \ \ldots\ \ ,\ \ (\rho+\sigma)d-1\ \}\\
I_d &= \{\ \ d\ \ ,\ \ \ 2\,d\ \ ,\ \ \ 3\,d\ \ ,\ \ \ldots\ \ ,\ \ \ (\rho+\sigma)\,d\ \};
\end{aligned}$$

(obsérvese que, si $i\equiv j \mod d$, entonces $I_i=I_j$; basta por tanto usar $i=1,\ldots,d$).

Tenemos, en definitiva, que si $m_{i,i}$ está en $\mathcal{P}$, entonces el producto *parcial* $\mathcal{P}_i = \prod_{j\in I_i} m_{j,j}$ en bloque forma parte de $\mathcal{P}$.

Por otra parte, si $m_{i,i}$ no está en $\mathcal{P}$, entonces ha de estar el otro elemento no nulo de la fila i-ésima (situado en una de las dos paralelas), al cual denotaremos m_i^*; y otro tanto sucederá para los restantes $j\in I_i$, con lo cual esta vez será el producto parcial $\mathcal{P}_i^* = \prod_{j\in I_i} m_j^*$ el que forme parte de $\mathcal{P}$.

Así pues: Fijado un producto elemental $\mathcal{P}$ que no incluya ceros, sabemos que, para cada $i=1,\dots,d$, la contribución al mismo de las filas i, $i+d$, $i+2d\dots$ es, o bien $\mathcal{P}_i$, o bien $\mathcal{P}_i^*$. Nada impide que coexistan productos parciales de uno y otro tipo. Hay, por tanto, 2^d diferentes configuraciones posibles para $\mathcal{P}$, tantas como formas de elegir cuántos y cuáles de los d productos parciales se toman del segundo tipo, esto es, tantas como subconjuntos tiene un conjunto de cardinal d.

Precisando más: De las $\rho+\sigma$ filas indicadas por los elementos de I_i, ρ se encuentran entre las r primeras filas y σ entre las s últimas, de modo que será $\mathcal{P}_i = A^\rho D^\sigma$ y $\mathcal{P}_i^* = B^\rho C^\sigma$, expresiones ambas que ya no dependen de i. Por tanto, para cada $k=0,\dots,d$, los $\binom{d}{k}$ productos elementales que toman exactamente k productos parciales del tipo segundo tienen un mismo valor, que es $\left(A^\rho D^\sigma\right)^{d-k}\left(B^\rho C^\sigma\right)^k$.

Más arduo sería analizar el signo aparejado a cada uno de estos productos elementales; puede eludirse esa tarea aplicando propiedades básicas de los determinantes para calcular $\det(M)$ de otro modo.

Observemos qué sucede si, sobre la matriz M, efectuamos intercambios de filas que coloquen en las $\rho+\sigma$ primeras posiciones a las filas F_1, F_{1+d}, $F_{1+2d}\dots$, $F_{1+(\rho+\sigma-1)d}$ y, seguidamente, intercambios de columnas que pongan en las $\rho+\sigma$ primeras posiciones a las columnas C_1, C_{1+d}, $C_{1+2d}\dots$, $C_{1+(\rho+\sigma-1)d}$. El signo del determinante se modifica cierto número de veces debido a las operaciones en filas, y otras tantas veces debido a las operaciones en columnas (pues unas y otras son nominalmente coincidentes) así que, en definitiva, tras un número par de cambios, queda como estaba. Pero todos estos movimientos colocan a las antiguas $m_{j,j}$ con $j\in I_1$ en las $\rho+\sigma$ primeras posiciones de la diagonal principal y traen, acompañándolas, a los elementos B y C que compartían fila o columna con ellas. Pero, como solo se toma una de cada d filas y una de cada d columnas, las distancias r o s que originalmente existían entre ellos quedan convertidas en distancias ρ o σ, respectivamente. Esto es, se concentran en una caja de tamaño $(\rho+\sigma)\times(\rho+\sigma)$ situada en la esquina superior derecha todos los elementos no nulos de las filas y columnas de número $j\in I_1$. Esa caja —que llamaremos matriz M_1— contiene a los elementos A, B, C, D dispuestos en tres diagonales según el esquema mostrado en la figura (2.2), solo que los números r y s se ven sustituidos por ρ y σ respectivamente.

Repitiendo el mismo tipo de proceso afectando esta vez a las filas y columnas de número $j \in I_2$ se logra una caja M_2 colocada como intersección de las $\rho+\sigma$ filas con las $\rho+\sigma$ columnas que siguen a las que contienen a M_1. La forma y el contenido de M_2 son idénticos a los de M_1.

Procediendo así sucesivamente con I_3, ..., I_d, se recolocan los elementos de M sin haber alterado el valor del determinante. La matriz que resulta está dividida en $d \times d$ cajas cuadradas de tamaño $(\rho+\sigma) \times (\rho+\sigma)$, todas las cuales son nulas excepto las cajas colocadas en la diagonal, que son $M_1, M_2, \ldots, M_d$, todas ellas iguales entre sí y que ya han sido descritas al terminar el proceso que dio lugar a M_1.

Así pues,

$$\det(M) = \det(M_1) \cdot \det(M_2) \cdot \ \cdots \ \cdot \det(M_d) = \Big[\det(M_1)\Big]^d. \tag{2.8}$$

Aplicando a M_1 el presente lema 2.3.1 en el caso previamente demostrado (pues ρ y σ sí son primos entre sí) se obtiene

$$\det\big(M_1\big) = A^{\rho} D^{\sigma} + (-1)^{\rho\sigma} B^{\rho} C^{\sigma}. \tag{2.9}$$

La igualdad (2.8), junto con (2.9), establecen la validez de la fórmula dada en el enunciado de este lema. □

Proposición 2.3.2 (Caso $I = \{i, j\}$). *Cuando se considera el $\{i, j\}$-polinomio de grado n,*

$$P_n(X) = X^n + \tbinom{n}{n\text{-}j} b_{n\text{-}j}\, X^j + \tbinom{n}{n\text{-}i} b_{n\text{-}i}\, X^i,$$

las dos únicas resultantes asociadas al problema de Casas-Alvero que no son trivialmente nulas son

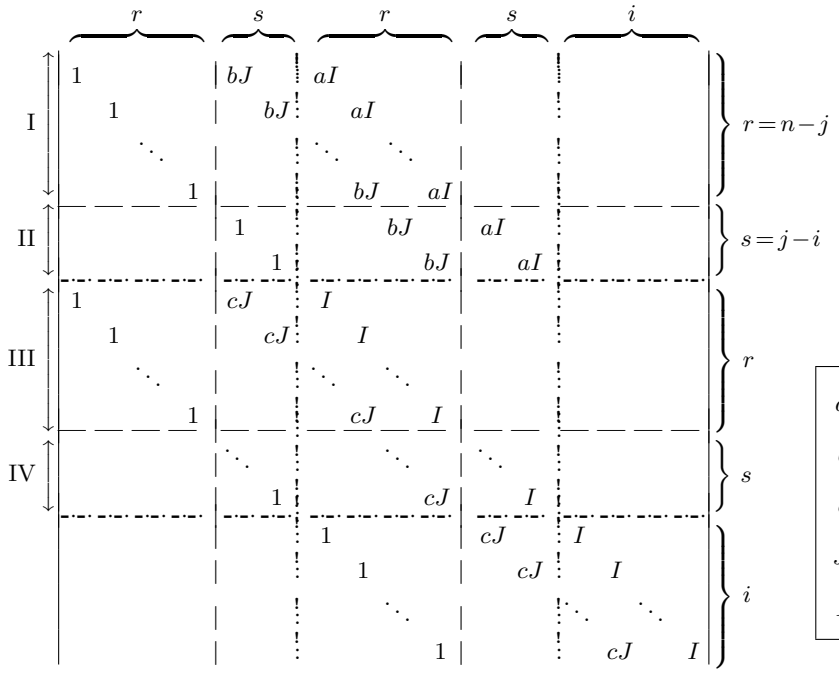
$$H^{[i]} = \ (-1)^{sr+r} \ \ b_{n\text{-}i}^{\,j} \ \Big[\, \alpha^{\rho} \beta^{\sigma} \ b_{n\text{-}j}^{\rho+\sigma} + (-1)^{\rho\sigma+\sigma} \ \gamma^{\rho+\sigma} \ \ b_{n\text{-}i}^{\rho} \,\Big]^d$$

$$H^{[j]} = \quad (-1)^{r} \quad\ b_{n\text{-}j}^{\,i} \ \Big[\quad \delta^{\rho} \ \ b_{n\text{-}j}^{\rho+\sigma} + (-1)^{\rho\sigma} \ (1+\gamma)^{\rho} \ \ b_{n\text{-}i}^{\rho} \,\Big]^d$$

donde: $r = n-j$, $s = j-i$, $d = \text{m.c.d.}(r, s)$, $\rho = \frac{r}{d}$, $\sigma = \frac{s}{d}$, *y donde*

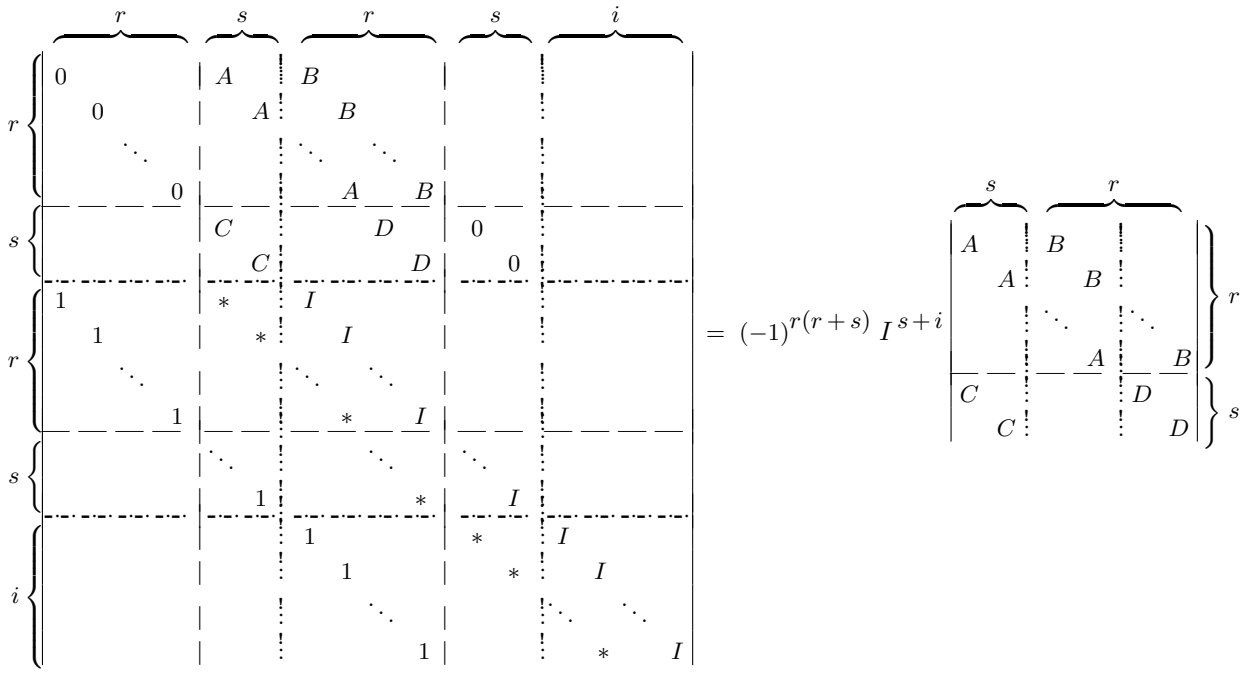
$\alpha = \binom{n}{j} - \binom{n\text{-}i}{n\text{-}j}$; $\beta = \binom{n}{j} - \binom{n\text{-}i}{n\text{-}j}\binom{n}{i}$; $\gamma = \binom{n}{i} - 1$; $\delta = \binom{n}{j} - 1$.

Demostración. El proceso para obtener la expresión de $H^{[i]}$ puede seguirse en el cuadro 2.1. Para mayor claridad, se han introducido los literales a, b, c, I, J, con el significado que allí se expresa, y que se mantendrá en el resto del capítulo —obsérvese el uso tácito de las identidades $\binom{n}{n\text{-}i} = \binom{n}{i}$, $\binom{n}{n\text{-}j} = \binom{n}{j}$—. Los elementos de la matriz que no aparecen visibles son todos ellos iguales a cero.

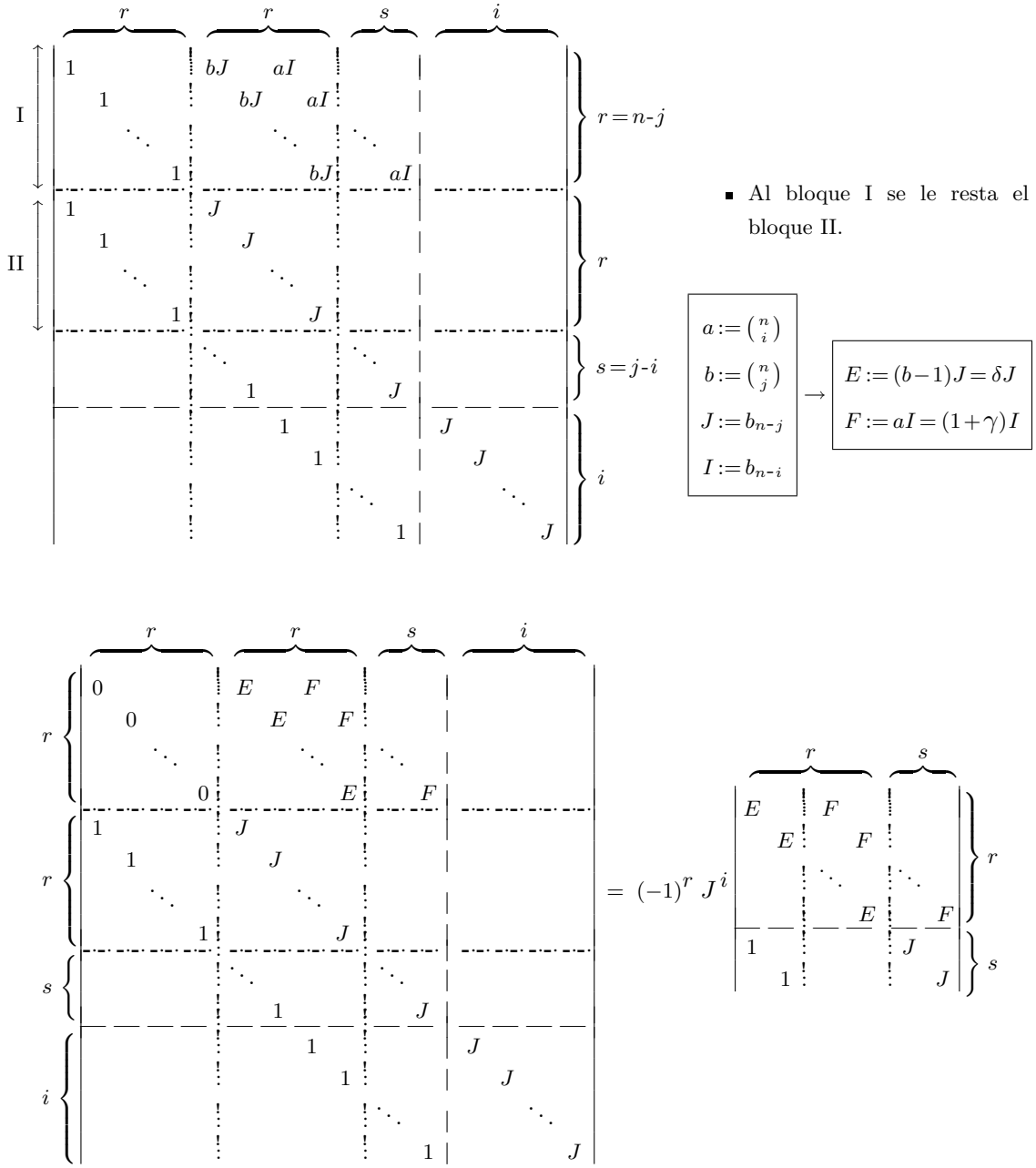


- Al bloque I se le resta el bloque III.
- Al bloque II se le resta el bloque IV multiplicado por a.

$$a := \binom{n}{i} \quad b := \binom{n}{j} \quad c := \binom{n-i}{n-j} \quad J := b_{n-j} \quad I := b_{n-i} \quad \rightarrow \quad A := (b-c)J = \alpha J \quad B := (a-1)I = \gamma I \quad C := 1-a = -\gamma \quad D := (b-ac)J = \beta J$$



Cuadro 2.1: Cálculo de $H^{[i]}$ en el $\{i,j\}$-problema.



Cuadro 2.2: Cálculo de $H^{[j]}$ en el $\{i,j\}$-problema.

A las líneas separadoras que ya se utilizaron en la figura 2.1 para la demostración de la proposición 2.2.1, se han superpuesto otras (a trazos largos) que, junto con las anteriores, subdividen la matriz en 5×5 cajas; esta partición permite apreciar cómo las $r+s=n-i$ sustracciones de filas que se indican producen la matriz que se encuentra en la parte inferior izquierda del cuadro 2.1. A partir de esta matriz, se desarrolla el determinante $s+i$ veces por la última columna —aparece así el factor $I^{s+i}=I^{j}$— y luego, r veces seguidas por la primera columna, por lo que surge r veces el factor $(-1)^{r+s+2}=(-1)^{r+s}$; obsérvese que, al tener siempre r y r^2 la misma paridad, es $(-1)^{r(r+s)}=(-1)^{r+sr}$. El determinante de orden $n-i$ que todavía queda pendiente de cálculo tiene la configuración adecuada para poder aplicar el lema 2.3.1, según el cual, dicho determinante vale

$$\Big[A^{\rho}D^{\sigma}+(-1)^{\rho\sigma}B^{\rho}C^{\sigma}\Big]^{d}=\Big[(\alpha J)^{\rho}(\beta J)^{\sigma}+(-1)^{\rho\sigma}(\gamma I)^{\rho}(-\gamma)^{\sigma}\Big]^{d};$$

operando y sustituyendo se obtiene para $H^{[i]}$ el resultado esperado.

El cálculo de la otra resultante, $H^{[j]}$, se muestra en el cuadro 2.2, y sigue un procedimiento análogo. Una vez hechas las sustracciones de filas que generan los ceros en la diagonal de la primera caja, se desarrolla el determinante por sus últimas i columnas y luego, por cada una de sus r primeras columnas. Aparecen de ese modo los factores J^{i} y $(-1)^{(r+2)r}=(-1)^{r}$, junto con un determinante de orden $n-i$ que, de nuevo por aplicación del lema 2.3.1, vale

$$\Big[E^{\rho}J^{\sigma}+(-1)^{\rho\sigma}F^{\rho}1^{\sigma}\Big]^{d}=\Big[(\delta J)^{\rho}J^{\sigma}+(-1)^{\rho\sigma}\big((1+\gamma)I\big)^{\rho}\Big]^{d};$$

basta ahora operar y sustituir para obtener la conclusión. □

Estamos ya en condiciones de caracterizar cuándo un $\{i,j\}$-problema tiene respuesta afirmativa, y cuándo no la tiene:

Teorema 2.3.3. *El sistema de ecuaciones asociado al $\{i,j\}$-problema de grado n,*

$$H^{[i]}=0,\qquad H^{[j]}=0,\qquad b_{n-k}=0\ \ \forall k\neq i,j$$

posee soluciones diferentes de la trivial si y solo si se verifica la igualdad

$$a^{\rho}\big(b-c\big)^{\rho}\big(b-ac\big)^{\sigma}\ =\ (-1)^{\sigma}\big(a-1\big)^{\rho+\sigma}\big(b-1\big)^{\rho},$$

donde $a=\binom{n}{i}$, $b=\binom{n}{j}$, $c=\binom{n-i}{n-j}$ *y* $\rho=\frac{n-j}{d}$, $\sigma=\frac{j-i}{d}$, *con* $d=\text{m.c.d.}\big(n-j,j-i\big)$.

Demostración. Una eventual solución $(p,q)\neq(0,0)$ para el sistema de ecuaciones $H^{[i]}=H^{[j]}=0$ en las dos incógnitas b_{n-j} y b_{n-i} ha de tener sus dos componentes diferentes de cero ya que, en caso contrario, el $\{i,j\}$-polinomio correspondiente,

$$P_n(X)=X^n+\tbinom{n}{n-j}\,p\,X^{j}+\tbinom{n}{n-i}\,q\,X^{i},$$

sería en realidad un $\{j\}$-polinomio (si $q=0$), o un $\{i\}$-polinomio (si $p=0$) que sirve como contraejemplo a la conjetura de Casas-Alvero; y esto, según el corolario 2.2.3, es imposible.

Al sustituir dicha solución (p,q) en la expresión que para el sistema $H^{[i]}=0,\ H^{[j]}=0$ suministra la proposición 2.3.2, se obtiene:

$$(-1)^{sr+r}\ \ q^j\ \Big[\,\alpha^{\rho}\beta^{\sigma}\ p^{\rho+\sigma}+(-1)^{\rho\sigma+\sigma}\ \gamma^{\rho+\sigma}\ \ q^{\rho}\,\Big]^d=0$$
$$(-1)^{r}\quad p^i\ \Big[\quad \delta^{\rho}\ \ p^{\rho+\sigma}+(-1)^{\rho\sigma}\ (1+\gamma)^{\rho}\ \ q^{\rho}\,\Big]^d=0$$

lo cual, siendo $p\cdot q\neq 0$, se verifica si y solo si se cumple

$$\alpha^{\rho}\beta^{\sigma}\ p^{\rho+\sigma}+(-1)^{\rho\sigma+\sigma}\ \gamma^{\rho+\sigma}\ \ q^{\rho}\ =0$$
$$\delta^{\rho}\ \ p^{\rho+\sigma}+(-1)^{\rho\sigma}\ (1+\gamma)^{\rho}\ \ q^{\rho}\ =0;$$

pero esto significa que el par $\big(p^{\rho+\sigma},q^{\rho}\big)$ es una solución no trivial del sistema lineal homogéneo, en las incógnitas u y v,

$$\begin{aligned}\alpha^{\rho}\beta^{\sigma}\ \mathrm{u}\ +\ (-1)^{\rho\sigma+\sigma}\ \gamma^{\rho+\sigma}\ \ \mathrm{v}\ &=\ 0\\ \delta^{\rho}\ \ \mathrm{u}\ +\ (-1)^{\rho\sigma}\ (1+\gamma)^{\rho}\ \ \mathrm{v}\ &=\ 0,\end{aligned}\tag{2.10}$$

cuya matriz de coeficientes tiene determinante Δ dado por

$$\Delta=(-1)^{\rho\sigma}\Big[a^{\,\rho}\,\big(b-c\big)^{\rho}\big(b-ac\big)^{\sigma}-(-1)^{\sigma}\big(a-1\big)^{\rho+\sigma}\big(b-1\big)^{\rho}\Big],\tag{2.11}$$

puesto que es: $\alpha=b-c,\ \beta=b-ac,\ \gamma=a-1$ y $\delta=b-1$.

En resumen, se tiene:

$$(p,q)\neq(0,0)\ \text{ es solución de }\ H^{[i]}=H^{[j]}=0\iff$$
$$\iff (p,q),\ \text{con}\ \ p\cdot q\neq 0,\ \ \text{es solución de } H^{[i]}=H^{[j]}=0\iff$$
$$\iff \big(p^{\rho+\sigma},q^{\rho}\big),\ \text{con}\ \ p^{\rho+\sigma}\cdot q^{\rho}\neq 0,\ \ \text{es solución no trivial de (2.10)},$$

para lo cual es condición necesaria la anulación del determinante Δ.

Por otra parte, el que se anule Δ garantiza la existencia de una solución no trivial para (2.10) de la forma (u_0,v_0), aunque no excluye que sea $u_0\cdot v_0=0$; quien sí excluye esta posibilidad es el hecho de ser manifiestamente no nulos tanto $\delta=\binom{n}{j}-1$ como $1+\gamma=\binom{n}{i}$, con lo cual, la igualdad

$$\delta^{\rho}\,u_0+(-1)^{\rho\sigma}\ (1+\gamma)^{\rho}\,v_0=0,$$

que se obtiene al sustituir dicha solución en la segunda ecuación del sistema (2.10), no puede verificarse si *solo una* componente de (u_0,v_0) es distinta de cero. Finalmente, el que sea $\mathbb{C}$ un cuerpo algebraicamente cerrado permite escribir $u_0=p^{\rho+\sigma},\ \ v_0=q^{\rho}$ para ciertos $p,q\in\mathbb{C}$, quedando demostrado que $\Delta=0$ es condición también suficiente para que el sistema $H^{[i]}=H^{[j]}=0$ admita una solución $(p,q)\neq(0,0)$. $\square$

Corolario 2.3.4. *En cualquier grado, y para cualesquiera i, j, el $\{i,j\}$-problema de Casas-Alvero tiene respuesta afirmativa, esto es:*

No existen $\{i,j\}$-contraejemplos a la conjetura de Casas-Alvero.

Demostración. En aplicación del teorema anterior, basta comprobar que, cualesquiera que sean n, i, $j \in \mathbb{N}$, con $1 \leq i < j \leq n-2$, y siendo $a = \binom{n}{i}$, $b = \binom{n}{j}$, $c = \binom{n\text{-}i}{n\text{-}j}$, se verifica

$$a^{\rho}\,(b-c)^{\rho}(b-ac)^{\sigma} \;\neq\; (-1)^{\sigma}(a-1)^{\rho+\sigma}(b-1)^{\rho} \tag{2.12}$$

siempre que ρ y σ sean enteros positivos.

Si los dos miembros de (2.12) fueran iguales, se tendría que a divide a $b-1$ y es, por tanto, primo con b. Pero, bajo las condiciones dadas, $a = \binom{n}{i}$ y $b = \binom{n}{j}$ nunca pueden ser primos entre sí, como muestra la igualdad

$$\binom{n}{i}\binom{n-i}{n-j} = \binom{n}{j}\binom{j}{i} \tag{2.13}$$

(ver comentario 2.3.5). El número $a = \binom{n}{i}$ divide, obviamente, al producto de la derecha en (2.13); y es estrictamente mayor que el factor $\binom{j}{i}$ dado que es $n > j$. Así pues, necesariamente alguno de los factores primos de a debe encontrarse alojado en $\binom{n}{j}$. Esto prueba (2.12), y concluye la demostración. □

Notemos que la demostración anterior admite el siguiente enfoque: Se concluye que la desigualdad (2.12) es cierta porque dicha desigualdad se verifica módulo p, siendo p el factor primo común de a y b antes aludido.

Comentario 2.3.5. La igualdad (2.13) puede comprobarse fácilmente desarrollando ambos miembros; sin embargo resulta más sencillo e interesante establecerla mediante un razonamiento de tipo combinatorio.

Consideremos un conjunto A de cardinal n en el que se quiere formar un subconjunto B de cardinal j, dentro del cual se desea destacar un *subsubconjunto* C de cardinal i (recuérdese que es $n > j > i \geq 1$). Al imaginar que dentro del diagrama de Euler-Venn de A incluimos el de B y en este el de C, a modo de diana, se visualiza inmediatamente que esta acción equivale a partir al conjunto A en los tres subconjuntos disjuntos $A \setminus B$, $B \setminus C$ y C, de cardinales respectivos $n-j$, $j-i$, i. Para el recuento de las configuraciones distintas que pueden obtenerse, se presentan dos alternativas:

- Multiplicar el número de subconjuntos $C \subset A$ diferentes, por el número de particiones en dos piezas de tamaño $j-i$ y $n-j$, respectivamente, que pueden hacerse en $A \setminus C$.

o bien, simplemente,

- Multiplicar el número de posibles subconjuntos $B \subset A$ por el número de posibles sub-subconjuntos $C \subset B$.

Al igualar los dos resultados se obtiene justamente (2.13), expresión que, de hecho, admite 2^4 variantes puramente formales, como por ejemplo

$$\binom{n}{n-i}\binom{n-i}{n-j} = \binom{n}{n-j}\binom{j}{i}. \tag{2.14}$$

Bajo una u otra forma, esta igualdad será utilizada reiteradamente en la demostración de resultados que son clave en el desarrollo de esta Memoria; así ocurre en la proposición 3.3.4, el lema 4.1.3 y el teorema 5.2.2.

2.4. Viabilidad del empleo de bases de Gröbner

En la sección 1.3.2 quedó expuesto cómo el problema total de Casas-Alvero de grado n se transforma en el problema de averiguar si es falsa o verdadera la afirmación

$$\text{Para cada } \; k=2,\ldots,n-1, \quad b_k \in \operatorname{Rad}\Big(\big\langle H^{[1]}, H^{[2]}, \ldots, H^{[n-2]}\big\rangle\Big) \subset \mathbb{C}\big[b_2,\ldots,b_{n-1}\big],$$

o, equivalentemente, si es falsa o verdadera la afirmación

$$\text{Para cada } k=2,\ldots,n-1, \quad 1 \in \widetilde{\mathcal{I}}_k := \Big\langle H^{[1]}, H^{[2]}, \ldots, H^{[n-2]}, 1-zb_k \Big\rangle \subset \mathbb{C}\big[b_2,\ldots,b_{n-1},z\big]. \tag{2.15}$$

Posteriormente, en la sección 1.3.3, se muestra cómo la obtención para cada ideal $\widetilde{\mathcal{I}}_k$ de una base de Gröbner $\mathcal{B}_k$ zanja la cuestión acerca de (2.15) —y, en consecuencia, el problema de Casas-Alvero de grado n— puesto que

$$1 \in \widetilde{\mathcal{I}}_k \quad \Longleftrightarrow \quad \text{El elemento 1 se encuentra en } \mathcal{B}_k.$$

Previa elección de un orden monomial para $\mathbb{C}\big[b_2,\ldots,b_{n-1},z\big]$, la búsqueda de la base de Gröbner $\mathcal{B}_k$ consiste en aplicar el algoritmo de Buchberger al sistema de generadores $\big\{H^{[1]}, H^{[2]}, \ldots, H^{[n-2]}, 1-zb_k\big\}$; empleando software específico para esta tarea puede procederse con valores sucesivos $n=4$, $n=5$, etc. mientras no se rebase la capacidad del sistema informático, cosa que con los medios actuales sucede con valores de n muy pequeños.[1]

Pero, más allá de cuantos casos particulares permita solventar, interesa valorar si este procedimiento ofrece alguna posibilidad de avance en el caso general, esto es, con n genérico. Como piedra de toque para el procedimiento nos sirve el $\{i,j\}$-problema parcial de grado n, de dificultad acotada y cuya respuesta ya conocemos.

[1] En el momento de redactar esta Memoria, los primeros valores de n para los que no se conoce una prueba conceptual de la conjetura son $n=12$ y $n=20$. Recientemente en 2012 la conjetura ha sido establecida para $n=12$ a través de una computación que, utilizando medios de altas prestaciones, ha consumido varias semanas en la realización de los cálculos, similares aunque alternativos al algoritmo de Buchberger, precedidos de diversas reducciones o simplificaciones. Para $n=20$ el cálculo requerido parece actualmente inabordable.

Todo lo dicho al inicio de esta sección se adapta de forma obvia a un $\{i,j\}$-problema de grado n, que, en consecuencia, se reduce a determinar si es verdadero o falso lo siguiente:

$$b_{n\text{-}j}, b_{n\text{-}i} \in \mathrm{Rad}\Big(\big\langle H^{[i]}, H^{[j]}\big\rangle\Big) \subset \mathbb{C}\big[b_{n-j}, b_{n\text{-}i}\big], \tag{2.16}$$

o, equivalentemente, lo siguiente:

$$1 \in \widetilde{\mathcal{I}}_{n\text{-}j} := \Big\langle H^{[i]}, H^{[j]}, 1 - z\, b_{n\text{-}j}\Big\rangle, \qquad 1 \in \widetilde{\mathcal{I}}_{n\text{-}i} := \Big\langle H^{[i]}, H^{[j]}, 1 - z\, b_{n\text{-}i}\Big\rangle, \tag{2.17}$$

bien entendido que los ideales $\widetilde{\mathcal{I}}_{n\text{-}j}$, $\widetilde{\mathcal{I}}_{n\text{-}i}$, lo son del anillo $\mathbb{C}\big[b_{n\text{-}j}, b_{n\text{-}i}, z\big]$ dado que, como venimos haciendo, prescindimos de las indeterminadas b_k con $k \neq n-j, n-i$, nulas por definición en todo $\{i,j\}$-polinomio.

Ahora bien, al demostrar el teorema 2.3.3 se razonó suficientemente que el sistema $H^{[i]} = 0,\ H^{[j]} = 0$ en las incógnitas $b_{n\text{-}j}, b_{n\text{-}i}$ posee alguna solución (p,q) distinta de la trivial si y solo si (p,q) es una solución no trivial del sistema

$$\begin{aligned} \alpha^{\rho}\beta^{\sigma}\ b_{n\text{-}j}^{\rho+\sigma} + (-1)^{\rho\sigma+\sigma}\ \gamma^{\rho+\sigma}\ b_{n\text{-}i}^{\rho} &= 0 \\ \delta^{\rho}\ b_{n\text{-}j}^{\rho+\sigma} + (-1)^{\rho\sigma}\ (1+\gamma)^{\rho}\ b_{n\text{-}i}^{\rho} &= 0. \end{aligned} \tag{2.18}$$

Si llamamos $G^{[i]}$ y $G^{[j]}$, respectivamente, a los primeros miembros de las igualdades en (2.18) —que, observemos, aparecían (con exponente d) en las expresiones de $H^{[i]}$ y $H^{[j]}$ dadas por la proposición 2.3.2—, entonces tenemos que

$$V\big(\langle H^{[i]}, H^{[j]}\rangle\big) = V\big(\langle G^{[i]}, G^{[j]}\rangle\big),$$

de modo que el sistema $G^{[i]} = G^{[j]} = 0$ puede reemplazar, a todos los efectos —en particular, en la reducción de la conjetura de Casas-Alvero a los enunciados (2.16) y (2.17)— al inicial sistema $H^{[i]} = H^{[j]} = 0$. Concluimos que el $\{i,j\}$-problema se reduce a averiguar si es o no cierta la siguiente afirmación:

$$1 \in \widetilde{\mathcal{J}}_{n\text{-}j} := \Big\langle G^{[i]}, G^{[j]}, 1 - z\, b_{n\text{-}j}\Big\rangle, \qquad 1 \in \widetilde{\mathcal{J}}_{n\text{-}i} := \Big\langle G^{[i]}, G^{[j]}, 1 - z\, b_{n\text{-}i}\Big\rangle, \tag{2.19}$$

la cual sustituye ventajosamente a (2.17) por la mayor simplicidad de los polinomios que intervienen.

Se trata ahora de comprobar si las bases de Gröbner de estos dos ideales contienen al polinomio unidad.

Fijamos, pues, un orden monomial en $\mathbb{C}\big[b_{n\text{-}j}, b_{n\text{-}i}, z\big]$, que supondremos otorga mayor orden a $b_{n\text{-}j}^{\rho+\sigma}$ que a $b_{n\text{-}i}^{\rho}$. En aplicación del algoritmo de Buchberger, será necesario (en ambos casos) calcular el S-polinomio de $G^{[i]}$ y $G^{[j]}$, pero

$$S(G^{[i]}, G^{[j]}) = \ (-1)^{\rho\sigma}\ \Big[(-1)^{\sigma}\ \delta^{\rho}\ \gamma^{\rho+\sigma} - (1+\gamma)^{\rho}\ \alpha^{\rho}\ \beta^{\sigma}\Big]\ b_{n\text{-}i}^{\rho}$$

$$\begin{aligned} &= -(-1)^{\rho\sigma}\left[a^{\,\rho}\,(b-c)^{\rho}\,(b-ac)^{\sigma}-(-1)^{\sigma}\,(a-1)^{\rho+\sigma}\,(b-1)^{\rho}\right]b_{n\text{-}i}^{\rho}\\ &= -\Delta\,b_{n\text{-}i}^{\rho}\end{aligned}$$

(se ha utilizado aquí la notación del teorema 2.3.3). En particular, Δ, introducido en (2.11), es el valor del determinante cuya anulación equivale a la existencia de $\{i,j\}$-contraejemplos a la conjetura de Casas-Alvero, y cuyo análisis (con la conclusión final de que Δ nunca es nulo) constituye la demostración del corolario 2.3.4, que da la respuesta (afirmativa) de todo $\{i,j\}$-problema.

La cuestión de si Δ es o no distinto de cero, que fue clave en la resolución directa del $\{i,j\}$-problema, aparece como un obstáculo que es necesario superar para continuar con el algoritmo de Buchberger. (Dicho sea de paso, una vez establecido que es $\Delta\neq 0$, resulta inmediato que tanto $b_{n\text{-}i}^{\rho}$ como $G^{[i]}-(-1)^{\rho\sigma+\sigma}\,\gamma^{\rho+\sigma}\,b_{n\text{-}i}^{\rho}=\alpha^{\rho}\,\beta^{\sigma}b_{n\text{-}j}^{\rho+\sigma}$ pertenecen al ideal $\langle G^{[i]},G^{[j]}\rangle$ y, por tanto, $b_{n\text{-}i},\ b_{n\text{-}j}\in\mathrm{Rad}\big(\langle G^{[i]},G^{[j]}\rangle\big)$, afirmación equivalente a (2.19)).

Probar con otro orden monomial diferente que esta vez diera prioridad al monomio $b_{n\text{-}i}^{\rho}$ no permitiría soslayar dicha cuestión, pues en ese caso se obtendría

$$S(G^{[i]},G^{[j]})=\,\Delta\,b_{n\text{-}j}^{\rho+\sigma}.$$

Cabe preguntarse, por último, si la presencia del factor Δ (y la obstrucción que supone) no será consecuencia de haber empleado los polinomios $G^{[i]}$ y $G^{[j]}$ en lugar de los debidos $H^{[i]}$ y $H^{[j]}$. Pero, si escribimos (en notación simplificada)

$$G^{[i]}=A\,b_{n\text{-}j}^{\rho+\sigma}+\,B\,b_{n\text{-}i}^{\rho}\,,\qquad\qquad G^{[j]}=C\,b_{n\text{-}j}^{\rho+\sigma}+\,D\,b_{n\text{-}i}^{\rho}\,,$$

entonces se tiene que

$$H^{[i]}=M\big(A\,b_{n\text{-}j}^{\rho+\sigma}+\,B\,b_{n\text{-}i}^{\rho}\big)^{\,d}\,,\qquad\qquad H^{[j]}=N\big(C\,b_{n\text{-}j}^{\rho+\sigma}+\,D\,b_{n\text{-}i}^{\rho}\big)^{\,d}\,,$$

y puede comprobarse que el S-polinomio de $H^{[i]}$ y $H^{[j]}$, mucho más aparatoso que el de $G^{[i]}$ y $G^{[j]}$, lleva como supuesto término líder al monomio $(b_{n\text{-}j}^{\rho+\sigma})^{d\text{-}1}\cdot b_{n\text{-}i}^{\rho}$ precedido del coeficiente

$$d\,MNA^{d\text{-}1}C^{d\text{-}1}\big(CB-AD\big)=-d\,MNA^{d\text{-}1}C^{d\text{-}1}\Delta,$$

de modo que el persistente obstáculo que Δ origina no es atribuible a la preparación anterior.

La conclusión de todo ello es, por tanto, que el método de las bases de Gröbner se encuentra bloqueado por dificultades de índole no computacional sino aritmética, cuya resolución equivale a la del propio problema de Casas-Alvero.

Capítulo 3

Usando esquemas proyectivos

Se considera el anillo de polinomios $\mathbb{Z}[z_1,\ldots,z_m]$ graduado mediante la asignación de pesos enteros $w_1, w_2, \ldots, w_m$ a sus indeterminadas, y se toman $F_1, F_2, \ldots, F_r \in \mathbb{Z}[z_1,\ldots,z_m]$, polinomios homogéneos respecto de dichos pesos. En tales condiciones, el sistema de ecuaciones

$$\left.\begin{array}{c} F_1(z_1,\ldots,z_m)=0 \\ \vdots \\ F_r(z_1,\ldots,z_m)=0 \end{array}\right\} \tag{3.1}$$

tiene la particularidad siguiente: cualquiera que sea el cuerpo $\mathbb{K}$, si $\alpha=(\alpha_1,\ldots,\alpha_m)\in\mathbb{K}^m$ es una solución del sistema, entonces la m-upla $\lambda\alpha=(\lambda^{w_1}\alpha_1, \lambda^{w_2}\alpha_2,\ldots,\lambda^{w_m}\alpha_m)$ es igualmente solución del mismo sistema, para todo $\lambda\in\mathbb{K}-\{0\}$. Identificando entre sí todas las m-uplas de la forma $\lambda\alpha$ se constituye un punto $[\alpha]$ del espacio proyectivo pesado $\mathbb{P}^{m-1}_{w_1,\ldots,w_m}(\mathbb{K})=\big(\mathbb{K}^m-\{\bar{0}\}\big)/\!\sim$. Tiene, por tanto, sentido construir un funtor asociado al sistema (3.1), concretamente, el funtor

$$Y : \big\{\text{Cuerpos conmutativos}\big\} \rightsquigarrow \big\{\text{Conjuntos}\big\}$$

que sobre los objetos viene dado por

$$Y(\mathbb{K}) = \Big\{\, [\alpha]\in \mathbb{P}^{m-1}_{w_1,\ldots,w_m}(\mathbb{K}) \,|\quad F_1(\alpha)=F_2(\alpha)=\ldots=F_r(\alpha)=0\Big\};$$

esto es, $Y\big(\mathbb{K}\big)$ recoge aquellos puntos $[\alpha]$ del correspondiente espacio proyectivo pesado tales que cada uno de sus representantes $\lambda\alpha$ es una solución del sistema de ecuaciones.

En esta Memoria (y por abuso de lenguaje) llamaremos *esquema proyectivo pesado* al funtor Y, si bien a lo que ese nombre propiamente designa es a una determinada extensión —que se define también a partir del sistema (3.1)— del funtor Y a la categoría de anillos conmutativos; el motivo por el que obviamos dicha extensión es que únicamente necesitaremos manejar los conjuntos $Y\big(\mathbb{K}\big)$ —y, aun esto, solo para ciertos cuerpos $\mathbb{K}$—.

Más precisamente, los cuerpos que habremos de considerar en este trabajo son, además del cuerpo $\mathbb{C}$, la clausura algebraica $\overline{\mathbb{Q}}$ del cuerpo $\mathbb{Q}$ y, para cada primo p, la clausura algebraica del cuerpo $\mathbb{F}_p = \mathbb{Z}/_{(p)}$, a la cual denotaremos por $\overline{\mathbb{F}}_p$. La clausura algebraica de un cuerpo $\mathbb{K}$ se define como un cuerpo $\overline{\mathbb{K}}$ que es a la vez algebraicamente cerrado y extensión algebraica de $\mathbb{K}$, significando lo primero que todo polinomio de $\overline{\mathbb{K}}[X]$ encuentra alguna raíz en $\overline{\mathbb{K}}$, y lo segundo, que todo elemento de $\overline{\mathbb{K}}$ es algebraico sobre $\mathbb{K}$, esto es, raíz de algún polinomio perteneciente a $\mathbb{K}[X]$. Aunque para un cuerpo general cuanto se sabe de su clausura algebraica es que existe y es única salvo isomorfismo, en los casos mencionados de $\mathbb{K} = \mathbb{Q}$ y de $\mathbb{K} = \mathbb{F}_p$ se dispone de un conocimiento más específico de la misma.

En el caso de $\mathbb{Q}$, el hecho de disponer de $\mathbb{C}$, que es un *supracuerpo* para $\overline{\mathbb{Q}}$ con el que estamos largamente familiarizados, facilita la comprensión de $\overline{\mathbb{Q}}$ como el subconjunto de $\mathbb{C}$ formado por los elementos que son algebraicos sobre $\mathbb{Q}$. El cuerpo $\overline{\mathbb{Q}}$ se puede también visualizar como la unión de todos los *cuerpos de números*, es decir, de los subcuerpos $\mathbb{K}$ de $\mathbb{C}$ que son extensiones finitas sobre $\mathbb{Q}$. Decir que el cuerpo $\mathbb{K} \subset \mathbb{C}$ es una extensión *finita* de $\mathbb{Q}$ significa que $\mathbb{K}$ es un espacio vectorial de dimensión finita sobre $\mathbb{Q}$ (cuerpo al que contiene); a dicha dimensión, usualmente denotada por $[\mathbb{K} : \mathbb{Q}]$, se la denomina *grado* de la extensión. En general, una extensión de un cuerpo es finita si y solo si tal extensión está finitamente generada por elementos algebraicos, siendo, en consecuencia, algebraica.

En el caso de $\mathbb{F}_p$, fijando —en principio, de forma abstracta— una clausura algebraica, $\overline{\mathbb{F}}_p$, podemos luego visualizarla como la unión de todos los cuerpos finitos de característica p. Tales cuerpos contienen un subcuerpo isomorfo a $\mathbb{Z}/_{(p)} = \mathbb{F}_p$, y son $\mathbb{F}_p$-espacios vectoriales de dimensión necesariamente finita; por tanto, su cardinal es la potencia p^r para algún entero $r \geq 1$. El —salvo isomorfismo— único cuerpo existente con p^r elementos, denotado $\mathbb{F}_{p^r}$, puede interpretarse como el subcuerpo de $\overline{\mathbb{F}}_p$ formado por las raíces del polinomio $X^{p^r} - X \in \mathbb{F}_p[X]$, que todos sus elementos no nulos satisfacen en virtud del teorema de Lagrange (y el nulo también, trivialmente). Recíprocamente, cada $\alpha \in \overline{\mathbb{F}}_p$ se encuentra en el subcuerpo $\mathbb{F}_p[\alpha]$ que, por ser finitamente generado por un elemento algebraico, es una extensión finita de $\mathbb{F}_p$, de modo que es un cuerpo finito y de característica p.

Observación 3.0.1. Retornando al esquema proyectivo Y definido a partir del sistema homogéneo pesado (3.1): Puesto que la m-upla $\bar{0} \in \mathbb{K}^m$ no proporciona ningún punto del espacio proyectivo, la expresión $Y\big(\mathbb{K}\big) = \emptyset$ equivale a decir que sobre el cuerpo $\mathbb{K}$ el sistema en cuestión *únicamente* posee la solución trivial.

Lema 3.0.2. *Para el esquema proyectivo Y dado por (3.1) se tiene que la condición $Y(\mathbb{C}) = \emptyset$ es equivalente a la condición $Y\big(\overline{\mathbb{Q}}\big) = \emptyset$.*

Demostración. Puesto que toda solución no trivial que el sistema (3.1) encuentre sobre el cuerpo $\overline{\mathbb{Q}}$ es, obviamente, una solución no trivial sobre $\mathbb{C}$, la implicación "*si* $Y(\mathbb{C})=\emptyset$ *entonces* $Y(\overline{\mathbb{Q}})=\emptyset$" es inmediata.

Para probar la recíproca, consideremos las parejas de ideales $\mathcal{H}_{\mathbb{C}}$, $\mathcal{J}_{\mathbb{C}}$ de $\mathbb{C}[z_1,\ldots,z_m]$ y $\mathcal{H}_{\overline{\mathbb{Q}}}$, $\mathcal{J}_{\overline{\mathbb{Q}}}$ de $\overline{\mathbb{Q}}[z_1,\ldots,z_m]$, donde $\mathcal{H}_{\mathbb{C}}$ y $\mathcal{H}_{\overline{\mathbb{Q}}}$ están generados por $F_1,\ldots,F_r$ y $\mathcal{J}_{\mathbb{C}}$ y $\mathcal{J}_{\overline{\mathbb{Q}}}$ están generados por $z_1,\ldots,z_m$. Puesto que tanto $\mathbb{C}$ como $\overline{\mathbb{Q}}$ son cuerpos algebraicamente cerrados, el teorema de los ceros de Hilbert asegura que la condición $Y(\mathbb{C})=\emptyset$ equivale a que sea $\mathrm{Rad}(\mathcal{H}_{\mathbb{C}})=\mathrm{Rad}(\mathcal{J}_{\mathbb{C}})$ y que la condición $Y(\overline{\mathbb{Q}})=\emptyset$ es equivalente a que sea $\mathrm{Rad}(\mathcal{H}_{\overline{\mathbb{Q}}})=\mathrm{Rad}(\mathcal{J}_{\overline{\mathbb{Q}}})$ —en cada caso, en el anillo de polinomios que corresponde—. Como $\mathcal{J}_{\mathbb{C}}$ y $\mathcal{J}_{\overline{\mathbb{Q}}}$ son ideales radicales, y como —por ser los polinomios F_i homogéneos pesados— se tienen las inclusiones $\mathcal{H}_{\mathbb{C}}\subset\mathcal{J}_{\mathbb{C}}$ y $\mathcal{H}_{\overline{\mathbb{Q}}}\subset\mathcal{J}_{\overline{\mathbb{Q}}}$, las condiciones $Y(\mathbb{C})=\emptyset$ y $Y(\overline{\mathbb{Q}})=\emptyset$ son equivalentes simplemente a que sea $\mathcal{J}_{\mathbb{C}}\subset\mathrm{Rad}(\mathcal{H}_{\mathbb{C}})$ y $\mathcal{J}_{\overline{\mathbb{Q}}}\subset\mathrm{Rad}(\mathcal{H}_{\overline{\mathbb{Q}}})$, respectivamente. Pero a su vez, estas inclusiones equivalen a la existencia de números enteros $d_i>0$, $i=1,\ldots,m$ tales que ${z_i}^{d_i}\in\mathcal{H}_{\mathbb{C}}$ y que ${z_i}^{d_i}\in\mathcal{H}_{\overline{\mathbb{Q}}}$, respectivamente. Ahora bien, al ser $\mathcal{H}_{\overline{\mathbb{Q}}}\subset\mathcal{H}_{\mathbb{C}}$, es claro que ${z_i}^{d_i}\in\mathcal{H}_{\overline{\mathbb{Q}}}$ implica ${z_i}^{d_i}\in\mathcal{H}_{\mathbb{C}}$, y por tanto, que $Y(\overline{\mathbb{Q}})=\emptyset$ implica $Y(\mathbb{C})=\emptyset$. □

La siguiente propiedad de los esquemas proyectivos nos resultará de extraordinaria utilidad:

Proposición 3.0.3 (Schicho, Graf von Bothmer, Labs, Van de Woestijne). *Sea Y el esquema proyectivo dado por (3.1). Entonces, las siguientes condiciones son equivalentes:*

(*i*) *Para todos los primos p, excepto para un número finito de ellos, $Y(\overline{\mathbb{F}}_p)$ es vacío.*

(*ii*) *Existe un primo p tal que $Y(\overline{\mathbb{F}}_p)$ es vacío.*

(*iii*) *$Y(\mathbb{C})$ es vacío.*

Demostración. Como $(i)\Rightarrow(ii)$ es trivial, demostraremos las implicaciones $(ii)\Rightarrow(iii)$ y $(iii)\Rightarrow(i)$.

Para demostrar $(iii)\Rightarrow(i)$ consideraremos los cuerpos $\mathbb{C}$ y $\overline{\mathbb{F}}_p$, y los ideales $\mathcal{H}_{\mathbb{C}}$ y $\mathcal{H}_p$ generados por $F_1,\ldots,F_r$ en los anillos $\mathbb{C}[z_1,\ldots,z_m]$ y $\overline{\mathbb{F}}_p[z_1,\ldots,z_m]$ respectivamente. Si (iii) es cierto, entonces (ver demostración del lema 3.0.2) podemos tomar enteros $d_i>0$ tales que $z_i^{d_i}\in\mathcal{H}_{\mathbb{C}}$, esto es, tales que

$$z_i^{d_i}=G_1F_1+G_2F_2+\cdots+G_rF_r,\qquad \text{para ciertos } G_j\in\mathbb{C}[z_1,\ldots,z_m]. \tag{3.2}$$

Tomemos ahora un subespacio vectorial T suplementario del subespacio $\mathbb{Q}$ en el $\mathbb{Q}$-espacio vectorial $\mathbb{C}$, de modo que sea $\mathbb{C}=\mathbb{Q}\oplus T$. Escribiendo $G_j=G_j'+G_j''$ (donde el primer sumando tiene todos sus coeficientes en $\mathbb{Q}$ y el segundo en T) la expresión (3.2) queda

$$z_i^{d_i} = \sum_{j=1}^{r} G'_j F_j + \sum_{j=1}^{r} G''_j F_j,$$

siendo esta la única manera de descomponer $z_i^{d_i} \in \mathbb{Q}[z_1, \ldots, z_r]$ en suma de dos polinomios con coeficientes, respectivamente, en $\mathbb{Q}$ y en T —recuérdese que los F_j tienen sus coeficientes en $\mathbb{Z}$—. La unicidad obliga a que sea nulo $\sum G''_j F_j$ y, por tanto, a que sea $z_i^{d_i} = \sum G'_j F_j$. Lo notable en esta igualdad es el hecho de saber que en la expresión (3.2) los polinomios G_j no son otros que los G'_j, y tienen coeficientes racionales. Tomemos los primos p que sean mayores que todos los denominadores de los coeficientes de todos los G_j, cuando se hace variar $j = 1, \ldots r$ y también se hace variar $i = 1, \ldots, m$ (índice que, por simplicidad de notación, no se refleja aquí). Entonces, no solamente los coeficientes de los F_j —que son enteros— sino también los coeficientes de los G_j, alcanzan a tener en $\mathbb{F}_p$ una imagen mediante la reducción módulo p (dada, en este caso, por $\varphi(a/b) := \varphi(a) \cdot \big[\varphi(b)\big]^{-1}$, siendo $\varphi : \mathbb{Z} \to \mathbb{Z}/_{(p)} = \mathbb{F}_p$ la aplicación característica), ya que sus denominadores no pueden ser múltiplo de p. De este modo obtenemos polinomios $\overline{F}_j$, $\overline{G}_j$ sobre $\mathbb{F}_p$, para los que se conserva la igualdad

$$z_i^{d_i} = \overline{G}_1 \overline{F}_1 + \overline{G}_2 \overline{F}_2 + \cdots + \overline{G}_r \overline{F}_r, \qquad \text{para ciertos } \overline{F}_i, \overline{G}_i \in \mathbb{F}_p[z_1, \ldots, z_m]. \tag{3.3}$$

Esta igualdad tiene lugar, de hecho, en el anillo $\overline{\mathbb{F}}_p[z_1, \ldots, z_m]$, e informa de que z_i pertenece al radical de $\mathcal{H}_p$. Dado que ello es así para cada $i = 1, \ldots, r$, se deduce, por el teorema de los ceros de Hilbert sobre $\overline{\mathbb{F}}_p$, que es $Y\big(\overline{\mathbb{F}}_p\big) = \emptyset$. Este resultado se ha obtenido para todos los primos excepto una cantidad finita, ya que los polinomios G_j reunían entre todos una cantidad finita de coeficientes.

Nuestra prueba de la implicación $(ii) \Rightarrow (iii)$ será más técnica, y requiere el uso de anillos de enteros de cuerpos de números, así como la aplicación de conocidas propiedades que a continuación se describen de forma escueta, a fin de que la redacción de la prueba resulte autocontenida. La justificación de estas propiedades es no trivial, y puede encontrarse, por ejemplo, en [Ser] o [Sam].

Tomemos un cuerpo de números $\mathbb{K} \subset \mathbb{C}$. Los elementos de $\mathbb{K}$ que son raíces de algún polinomio mónico con coeficientes en $\mathbb{Z}$ forman un subanillo $\mathcal{O}_{\mathbb{K}}$ de $\mathbb{K}$ que se denomina *anillo de enteros* de $\mathbb{K}$. El cuerpo de fracciones de $\mathcal{O}_{\mathbb{K}}$ es el propio $\mathbb{K}$, y $\mathcal{O}_{\mathbb{K}}$ contiene a $\mathbb{Z}$. Como $\mathbb{Z}$-módulo, $\mathcal{O}_{\mathbb{K}}$ es libre y de rango igual al grado $[\mathbb{K} : \mathbb{Q}]$. Todos los ideales primos de $\mathcal{O}_{\mathbb{K}}$ a excepción del ideal (0) son ideales maximales del anillo. Si $\mathfrak{p}$ es un ideal maximal, entonces $\mathfrak{p} \cap \mathbb{Z} = (p)$ para algún número primo p, y se tiene que el anillo cociente $\mathcal{O}_{\mathbb{K}}/\mathfrak{p}$ es un cuerpo finito con p^r elementos para cierto $r > 0$. Recíprocamente, dado un primo p, existe algún ideal maximal $\mathfrak{p}$ (de hecho, un número finito de ellos) tal que $\mathfrak{p} \cap \mathbb{Z} = (p)$. A partir de un isomorfismo entre los cuerpos finitos $\mathcal{O}_{\mathbb{K}}/\mathfrak{p}$ y $\mathbb{F}_{p^r}$ —el cual existe, pues se trata de dos cuerpos con igual número de elementos— se deduce un

homomorfismo de anillos $\phi_{\mathfrak{p}} : \mathcal{O}_{\mathbb{K}} \to \overline{\mathbb{F}}_p$ cuyo núcleo es $\mathfrak{p}$ y cuya imagen es $\mathbb{F}_{p^r}$; este homomorfismo será utilizado como herramienta para reducir módulo $\mathfrak{p}$ las coordenadas de los puntos contenidos en $Y\big(\mathbb{K}\big)$. Como caso particular relevante, para $\mathbb{K}=\mathbb{Q}$ se tiene $\mathcal{O}_{\mathbb{Q}}=\mathbb{Z}$; los ideales maximales de este anillo son los del tipo $\big(p\big)$, siendo p un número primo, y la aplicación $\phi_{(p)} : \mathbb{Z} \to \overline{\mathbb{F}}_p$ es la composición de las de reducción módulo p usual, $\varphi : \mathbb{Z} \to \mathbb{Z}/_{(p)} = \mathbb{F}_p$, con la de inclusión de $\mathbb{F}_p$ en $\overline{\mathbb{F}}_p$.

De gran utilidad resulta la existencia de una valoración $\mathfrak{v}_{\mathfrak{p}} : \mathbb{K}\setminus\{0\} \to \mathbb{Z}$ asociada a cada ideal maximal $\mathfrak{p}$ de $\mathcal{O}_{\mathbb{K}}$. Se define en primer lugar sobre los elementos del anillo de enteros:

$$\text{Dado } \alpha \in \mathcal{O}_{\mathbb{K}}\setminus\{0\}, \qquad \mathfrak{v}_{\mathfrak{p}}(\alpha) := l \quad \text{ si } \ \alpha \in \mathfrak{p}^l \ \text{ pero } \ \alpha \notin \mathfrak{p}^{l+1},$$

y luego se extiende a los elementos no nulos de $\mathbb{K}$:

$$\text{Si } \ \alpha, \beta \in \mathcal{O}_{\mathbb{K}}\setminus\{0\}, \qquad \mathfrak{v}_{\mathfrak{p}}\big(\frac{\alpha}{\beta}\big) := \mathfrak{v}_{\mathfrak{p}}(\alpha) - \mathfrak{v}_{\mathfrak{p}}(\beta).$$

Es usual ampliar $\mathfrak{v}_{\mathfrak{p}}$ a todo $\mathbb{K}$ definiendo $\mathfrak{v}_{\mathfrak{p}}(0) := \infty$. Para cualesquiera $\alpha, \beta \in \mathbb{K}$, se satisfacen las dos propiedades siguientes:

(1) $\mathfrak{v}_{\mathfrak{p}}(\alpha+\beta) \geq \text{mín}\big\{\mathfrak{v}_{\mathfrak{p}}(\alpha), \mathfrak{v}_{\mathfrak{p}}(\beta)\big\}$.

(2) $\mathfrak{v}_{\mathfrak{p}}(\alpha\cdot\beta) = \mathfrak{v}_{\mathfrak{p}}(\alpha) + \mathfrak{v}_{\mathfrak{p}}(\beta)$

Los elementos $\tau \in \mathcal{O}_{\mathbb{K}}$ con $\mathfrak{v}_{\mathfrak{p}}(\tau)=1$, que siempre existen, reciben el nombre de *uniformizantes*. Es de destacar también el conjunto de los elementos a los que la valoración les asigna una imagen no negativa, y que coincide con el localizado de $\mathcal{O}_{\mathbb{K}}$ mediante el ideal $\mathfrak{p}$. Esto es,

$$\mathcal{O}_{\mathbb{K},\mathfrak{p}} = \big\{\alpha \in \mathbb{K} \,|\quad \mathfrak{v}_{\mathfrak{p}}(\alpha) \geq 0\big\}.$$

El homomorfismo $\phi_{\mathfrak{p}}$ de reducción módulo $\mathfrak{p}$ se hace extensivo al anillo local $\mathcal{O}_{\mathbb{K},\mathfrak{p}}$; el núcleo de este homomorfismo lo forman justamente los elementos α cuya valoración es estrictamente positiva.

Finalmente, si $\mathbb{K}$ y $\mathbb{L}$ son cuerpos de números con $\mathbb{K}\subset\mathbb{L}$, y si $\mathfrak{p}$ es un ideal maximal de $\mathcal{O}_{\mathbb{K}}$, entonces se tiene $\mathfrak{p}=\mathfrak{q}\cap\mathcal{O}_{\mathbb{K}}$ para algún ideal maximal $\mathfrak{q}$ del anillo $\mathcal{O}_{\mathbb{L}}$.

Probaremos ahora la implicación $(ii)\Rightarrow(iii)$ mostrando que si $Y\big(\overline{\mathbb{Q}}\big) \neq \emptyset$ entonces se tiene $Y\big(\overline{\mathbb{F}}_p\big) \neq \emptyset$ para todo primo p; hecho que, a la vista del lema 3.0.2, deja zanjada la cuestión.

Si $Y\big(\overline{\mathbb{Q}}\big) \neq \emptyset$ entonces existe alguna solución $\alpha=(\alpha_1,\ldots,\alpha_m) \in \overline{\mathbb{Q}}^m$ del sistema (3.1) tal que $\alpha_j \neq 0$ para al menos un índice j. Como cada componente α_i es algebraica sobre $\mathbb{Q}$, existen cuerpos de números que contienen a $\alpha_1,\ldots,\alpha_m$ simultáneamente. Tomemos uno de ellos, $\mathbb{K}$, y consideremos en su anillo de enteros $\mathcal{O}_{\mathbb{K}}$ un ideal maximal $\mathfrak{p}$ tal que sea $\mathfrak{p}\cap\mathbb{Z}=(p)$. Escribiendo cada α_i como cociente de dos elementos de $\mathcal{O}_{\mathbb{K}}$ y tomando

como λ el producto de los denominadores obtenidos, se consigue una nueva solución del sistema (3.1), $\lambda\alpha=(\lambda^{w_1}\alpha_1,\ldots,\lambda^{w_m}\alpha_m)$, que define el mismo punto $[\alpha]$ del espacio proyectivo $\mathbb{P}^{m-1}_{w_1,\ldots,w_m}(\overline{\mathbb{Q}})$ pero cuyas coordenadas $\lambda^{w_i}\alpha_i$ se encuentran en $\mathcal{O}_{\mathbb{K}}$. Así, sin pérdida de generalidad, podemos suponer directamente que $\alpha_i\in\mathcal{O}_{\mathbb{K}}$ para todo i.

Ahora, si se tuviese $\mathfrak{v}_{\mathfrak{p}}(\alpha_i)=0$ (es decir, $\alpha\notin\mathfrak{p}$) para algún i, entonces, por reducción módulo $\mathfrak{p}$ se tendría que $\big(\phi_{\mathfrak{p}}(\alpha_1),\ldots,\phi_{\mathfrak{p}}(\alpha_m)\big)$ sería una solución de (3.1) sobre $\overline{\mathbb{F}}_p$ con $\phi_{\mathfrak{p}}(\alpha_i)\neq 0$ para ese mismo i, y por tanto $Y\big(\overline{\mathbb{F}}_p\big)$ sería no vacío. Sin embargo, como pudiera suceder que fuera $\mathfrak{v}_{\mathfrak{p}}(\alpha_i)>0$ para todo i, necesitamos pasar a otro cuerpo de números mayor que $\mathbb{K}$ sobre el que poder elegir un nuevo representante del punto $[\alpha]$ que ya no presente ese tipo de problema.

A tal propósito, definimos el número racional

$$x=\text{mín}\left\{\frac{\mathfrak{v}_{\mathfrak{p}}(\alpha_1)}{w_1}\,,\ \frac{\mathfrak{v}_{\mathfrak{p}}(\alpha_2)}{w_2}\,,\ \ldots\ ,\ \frac{\mathfrak{v}_{\mathfrak{p}}(\alpha_m)}{w_m}\right\} \tag{3.4}$$

(x es siempre finito: algún $\mathfrak{v}_{\mathfrak{p}}(\alpha_i)$ pudiera ser ∞, pero todos, no, ya que hay un $\alpha_j\neq 0$), y escribimos $x=\frac{c}{d}$ con c, d enteros y $d>0$. Tomamos un uniformizante $\tau\in\mathcal{O}_{\mathbb{K}}$ y un número complejo μ tal que $\mu^d=\tau$. Puesto que μ es algebraico sobre $\mathbb{K}$, podemos tomar un nuevo cuerpo de números $\mathbb{L}$ que contenga a $\mathbb{K}$ y a μ. Tomemos ahora un ideal maximal $\mathfrak{q}$ del anillo de enteros $\mathcal{O}_{\mathbb{L}}$ verificando la igualdad $\mathfrak{q}\cap\mathcal{O}_{\mathbb{K}}=\mathfrak{p}$. Es fácil comprobar que se cumple

$$\text{Si } \alpha\in\mathbb{K},\ \ \alpha\neq 0,\ \ \text{entonces}\quad \mathfrak{v}_{\mathfrak{q}}(\alpha)=d\cdot\mathfrak{v}_{\mathfrak{p}}(\alpha)\cdot\mathfrak{v}_{\mathfrak{q}}(\mu);$$

ello es consecuencia del hecho siguiente: Si $\mathfrak{v}_{\mathfrak{p}}(\alpha)=v$, $\alpha\neq 0$, entonces α se puede escribir en la forma

$$\alpha\ =\ \tau^v\cdot\frac{\beta}{\gamma},\quad \text{con}\ \ \beta,\gamma\in\mathcal{O}_{\mathbb{K}}\ \ \text{y}\ \ \beta,\gamma\notin\mathfrak{p}.$$

esto es,

$$\alpha\ =\ \mu^{d\cdot v}\cdot\frac{\beta}{\gamma},\quad \text{con}\ \ \beta,\gamma\in\mathcal{O}_{\mathbb{L}}\ \ \text{y}\ \ \beta,\gamma\notin\mathfrak{q}.$$

Consideramos ahora la solución de (3.1) dada por $\lambda\alpha=(\lambda^{w_1}\alpha_1,\ldots,\lambda^{w_m}\alpha_m)$ cuando se toma $\lambda=\mu^{-c}\in\mathbb{L}$. Las componentes de esta m-upla se encuentran, de hecho, en el anillo local $\mathcal{O}_{\mathbb{L},\mathfrak{q}}$, pues, en efecto,

$$\mathfrak{v}_{\mathfrak{q}}(\lambda^{w_i}\alpha_i)=\mathfrak{v}_{\mathfrak{q}}(\mu)\cdot\big(-w_i\cdot c+\mathfrak{v}_{\mathfrak{p}}(\alpha_i)\cdot d\big)\geq 0,\quad \text{para todo } i=1,\ldots m;$$

pero además sabemos con certeza que se cumple la igualdad $\mathfrak{v}_{\mathfrak{q}}(\lambda^{w_i}\alpha_i)=0$ para al menos uno de los índices(aquel o aquellos i tales que el cociente $\frac{\mathfrak{v}_{\mathfrak{p}}(\alpha_i)}{w_i}$, por ser mínimo, coincida precisamente con $x=\frac{c}{d}$ según fue definido en (3.4)). Así pues, no solamente es cierto que la reducción módulo $\mathfrak{q}$ de cada componente de esta solución está definida, sino que además alguna es no nula, de modo que la r-upla

$$\big(\,\phi_{\mathfrak{q}}(\lambda^{w_1}\alpha_1),\ \phi_{\mathfrak{q}}(\lambda^{w_2}\alpha_2),\ \ldots\ ,\ \phi_{\mathfrak{q}}(\lambda^{w_r}\alpha_r)\,\big)$$

determina en efecto un punto del espacio proyectivo $\mathbb{P}^{m-1}_{w_1,\ldots,w_m}(\overline{\mathbb{F}}_p)$ perteneciente a $Y\big(\overline{\mathbb{F}}_p\big)$. □

Nota 3.0.4. La demostración de la proposición anterior esquiva el lenguaje y la teoría abstracta de esquemas. La prueba de Schicho, Graf von Bothmer, Labs y Van de Woestijne en [BLSW] es no constructiva, y requiere formular resultados especializados de la teoría de esquemas que se ha considerado innecesario introducir en esta Memoria. Nuestra prueba, por su parte, requiere utilizar las propiedades de los anillos de enteros de cuerpos de números —teoría también especializada, pero más apropiada para un público general—, y presenta además la particularidad de ser constructiva.

Nota 3.0.5. Cuando para cada cuerpo $\mathbb{K}$ se tenga que $Y\big(\mathbb{K}\big)$ es vacío, diremos que el esquema Y *carece de entidad geométrica*. Un ejemplo de esta situación se obtiene si en (3.1) se toma $r=m\geq 1$ y $F_j=z_j^{l_j}$ siendo $l_j>0$ un entero para cada $j=1,\ldots,m$. Otro ejemplo se obtiene si se toma $m=0$, es decir, si no se considera ninguna variable, ya que entonces $Y\big(\mathbb{K}\big)$ es vacío por serlo formalmente el espacio proyectivo (-1)-dimensional (razón por la que ese espacio no se define en geometría).

La demostración del lema 3.0.2 puede adaptarse sin ningún cambio esencial al caso de característica $p\geq 0$ para probar que si $\overline{\mathbb{K}}$ es un cuerpo algebraicamente cerrado de característica $p>0$ (resp. $p=0$) entonces $Y\big(\overline{\mathbb{K}}\big)$ es vacío si y solo si $Y\big(\overline{\mathbb{F}}_p\big)$ es vacío (resp. $Y\big(\overline{\mathbb{Q}}\big)$ es vacío). De ello se deduce que el esquema proyectivo Y carece de entidad geométrica si y solo si $Y\big(\overline{\mathbb{Q}}\big)$ es vacío e $Y\big(\overline{\mathbb{F}}_p\big)$ es vacío para todo primo p; o, equivalentemente, si $Y\big(\mathbb{C}\big)$ es vacío e $Y\big(\overline{\mathbb{F}}_p\big)$ es vacío para todo primo p. Como además el teorema 3.0.3 muestra que la condición $Y\big(\mathbb{C}\big)=\emptyset$ es aquí superflua, concluimos que el esquema proyectivo Y carece de entidad geométrica si y solo si se tiene $Y\big(\overline{\mathbb{F}}_p\big)=\emptyset$ para todo primo p.

3.1. Esquemas proyectivos asociados a los problemas de Casas-Alvero total y parcial

Sea de nuevo el polinomio $P_n(X)=X^n+\binom{n}{2}b_2\,X^{n-2}+\ldots+\binom{n}{n-i}b_{n-i}\,X^i+\ldots+\binom{n}{n-1}b_{n-1}\,X$ y, para cada $i=1,2,\ldots,n-2$, su derivada neta i-ésima, $P_n^{[i]}(X)$, así como la resultante $H^{[i]}=\mathrm{Res}\big(P_n,P_n^{[i]}\big)$. Recordemos que en el anillo $\mathbb{Z}[b_2,\ldots,b_{n-1}]$, graduado mediante la asignación de pesos dada por $\mathrm{gr}(b_k):=k$, todos los polinomios $H^{[i]}$ son homogéneos.

Denotaremos por Y_n al esquema proyectivo pesado definido por las ecuaciones

$$H^{[1]}=H^{[2]}=\ldots=H^{[n-2]}=0\,.$$

Por otra parte, para cada conjunto de exponentes $I=\{i_1,\ldots,i_r\}\subset J=\{1,2,\ldots,n{-}2\}$, denotaremos por $Z_{n,I}$ al esquema proyectivo pesado definido por las ecuaciones

$$H^{[i_1]}=H^{[i_2]}=\ldots=H^{[i_r]}=0\,;\qquad b_{n\text{-}j}=0,\quad \forall j\in J\smallsetminus I.$$

Obsérvese que se trata del sistema que define el I-problema de Casas-Alvero, bien entendido que, en este contexto, se mantiene a las $n{-}2$ indeterminadas b_k como incógnitas presentes en el sistema —sin prescindir de las $b_{n\text{-}j}$, expresamente obligadas a ser nulas—, de modo que todo $Z_{n,I}$ es un subesquema del espacio proyectivo pesado $(n\text{-}3)$-dimensional, en su acepción de esquema.

Observación 3.1.1. Cualquiera que sea el cuerpo $\mathbb{K}$, se verifica

$$I\subset I'\subset J=\{1,2,\ldots,n{-}2\}\quad\Longrightarrow\quad Z_{n,I}\big(\mathbb{K}\big)\subset Z_{n,I'}\big(\mathbb{K}\big)\subset Y_n\big(\mathbb{K}\big).$$

En efecto, basta recordar que, según se vio en la observación 2.1.1, para cada $i\in J$ se cumple: $b_{n\text{-}i}=0\;\Rightarrow\;H^{[i]}=0$ (o, equivalentemente, $b_{n\text{-}i}$ divide al polinomio $H^{[i]}$) y tener presente que, siendo $I=\{i_1,\ldots,i_r\}$, $I'\smallsetminus I=\{k_1,\ldots,k_s\}$, $J\smallsetminus I'=\{j_1,\ldots,j_t\}$, entonces

$$\bullet\ Z_{n,I}\text{ está definido por el sistema}\quad\begin{cases} H^{[i_1]}=\cdots=H^{[i_r]}=0\\ b_{n\text{-}k_1}=\cdots=b_{n\text{-}k_s}=0\\ b_{n\text{-}j_1}=\cdots=b_{n\text{-}j_t}=0,\end{cases}$$

mientras que

$$\bullet\ Z_{n,I'}\text{ está definido por el sistema}\quad\begin{cases} H^{[i_1]}=\cdots=H^{[i_r]}=0\\ H^{[k_1]}=\cdots=H^{[k_s]}=0\\ b_{n\text{-}j_1}=\cdots=b_{n\text{-}j_t}=0\end{cases}$$

y, el esquema Y_n, por el sistema $H^{[1]}=H^{[2]}=\ldots=H^{[n\text{-}2]}=0$.

Más precisamente, fijado un cuerpo $\mathbb{K}$, los conjuntos $Z_{n,I}\big(\mathbb{K}\big)$, $Z_{n,I'}\big(\mathbb{K}\big)$ y $Y_n\big(\mathbb{K}\big)$ son justamente las variedades proyectivas del espacio proyectivo pesado $\mathbb{P}^{n-3}_{2,3,\ldots,n\text{-}1}(\mathbb{K})$ determinadas, respectivamente, por los ideales

$$\begin{gathered}\big\langle H^{[i_1]},\ldots,H^{[i_r]};\,b_{n\text{-}k_1},\ldots,b_{n\text{-}k_s};\,b_{n\text{-}j_1},\ldots,b_{n\text{-}j_t}\big\rangle,\\ \big\langle H^{[i_1]},\ldots,H^{[i_r]};\,H^{[k_1]},\ldots,H^{[k_s]};\,b_{n\text{-}j_1},\ldots,b_{n\text{-}j_t}\big\rangle,\\ \big\langle H^{[1]},H^{[2]},\ldots,H^{[n\text{-}2]}\big\rangle;\end{gathered}$$

las evidentes relaciones de inclusión que se dan entre estos ideales significan que el esquema $Z_{n,I}$ es un subesquema de $Z_{n,I'}$, y que ambos lo son de Y_n.

En los problemas de Casas-Alvero, lo mismo en su forma total que en todas sus formas parciales, la tesis del enunciado podrá ser caracterizada muy nítidamente empleando los esquemas que acabamos de definir.

Proposición 3.1.2. *(a) La conjetura de Casas-Alvero es verdadera para grado n si y solo si $Y_n(\mathbb{C}) = \emptyset$, esto es, si el esquema proyectivo Y_n carece de puntos sobre $\mathbb{C}$.*

(b) El problema parcial de Casas-Alvero en grado n y con exponentes en I tiene respuesta afirmativa si y solo si $Z_{n,I}(\mathbb{C}) = \emptyset$.

Demostración. (a) Es claro, puesto que ambas cosas equivalen a que $\bar{0}=(0,\ldots,0)$ sea la única solución sobre $\mathbb{C}$ del sistema homogéneo $H^{[1]}=H^{[2]}=\ldots=H^{[n-2]}=0$; por el contrario, la eventual existencia de una solución no trivial del mismo, $\beta=(\beta_2,\ldots,\beta_{n-1})\in\mathbb{C}^{n-2}$, significaría simultáneamente que el polinomio

$$P_{n,\beta}(X)=X^n+\tbinom{n}{2}\beta_2\,X^{n-2}+\ldots+\tbinom{n}{n-i}\beta_{n-i}\,X^i+\ldots+\tbinom{n}{n-1}\beta_{n-1}\,X$$

es un contraejemplo a la conjetura de Casas-Alvero en grado n, y que $Y_n(\mathbb{C})$ contiene por lo menos al punto $[\beta]$.

(b) Este hipotético contraejemplo al problema total sería un I-contraejemplo si y solo si fueran nulas las componentes de β ubicadas en ciertas posiciones prefijadas (y esto le pasaría a $\lambda\beta$, para todo $\lambda\in\mathbb{C}$), por lo que el punto $[\beta]$ estaría de hecho en $Z_{n,I}(\mathbb{C})$. □

Observación 3.1.3. Dado que el conjunto *completo* de exponentes, $J=\{1,2,\ldots,n-2\}$, es subconjunto de sí mismo, entre los esquemas de tipo $Z_{n,I}$ se encuentra el esquema $Z_{n,J}$, que en nada se diferencia de Y_n. Podemos convenir, pues, en considerar al problema *total* de Casas-Alvero como uno más de los problemas parciales, y tratar conjuntamente todos ellos. Emplearemos la notación Y_n, específica del problema total, cuando sea preciso poner énfasis en que nos referimos a dicho caso.

Podemos ya formular una condición suficiente para que un I-problema parcial de Casas-Alvero de grado n tenga respuesta afirmativa.

Proposición 3.1.4. *Si existe un primo p tal que $Z_{n,I}\big(\overline{\mathbb{F}}_p\big)=\emptyset$, entonces la conjetura de Casas-Alvero en grado n no admite ningún I-contraejemplo. En particular, si $Y_n\big(\overline{\mathbb{F}}_p\big)=\emptyset$, entonces dicha conjetura es verdadera para el grado n.*

Demostración. Si, para determinado primo p, $Z_{n,I}\big(\overline{\mathbb{F}}_p\big)=\emptyset$ (resp. $Y_n\big(\overline{\mathbb{F}}_p\big)=\emptyset$) entonces, en virtud de la proposición 3.0.3 se tendrá que $Z_{n,I}(\mathbb{C})=\emptyset$ (resp. $Y_n(\mathbb{C})=\emptyset$); basta ahora aplicar la proposición 3.1.2. □

La anterior proposición se destaca por las posibilidades operativas que ofrece, pero sucede además que también es cierto su recíproco, como igualmente se desprende de 3.0.3. Se tiene entonces un nuevo enunciado equivalente para la conjetura de Casas-Alvero:

Conjetura de Casas-Alvero. *Sea* Y_n *el subesquema proyectivo del espacio proyectivo pesado* $\mathbb{P}^{n-3}_{2,3,\ldots,n-1}$ *definido por las ecuaciones* $H^{[1]} = H^{[2]} = \ldots = H^{[n-2]} = 0$. *Se verifica lo siguiente: Existe algún número primo* p *tal que* $Y_n\big(\overline{\mathbb{F}}_p\big) = \emptyset$.

3.2. La reducción módulo p

Habida cuenta de la relevancia que acaba de tomar el conjunto $Z_{n,I}\big(\overline{\mathbb{F}}_p\big)$, procede interesarse por la naturaleza y el significado de sus elementos.

La construcción de los esquemas $Z_{n,I}$ se ha regido por un discurso —sobre polinomios, derivadas y raíces compartidas— desarrollado siempre bajo el supuesto de encontrarnos trabajando sobre $\mathbb{C}$, y por tanto en característica cero. Así se obtienen las ecuaciones $H^{[k]}=0$ (en $n-2$ incógnitas y con coeficientes enteros); ahora bien, una vez fijadas, son ellas solas quienes definen por sí mismas el esquema.

Para ahora estudiar las soluciones sobre $\overline{\mathbb{F}}_p$ de dichas ecuaciones será muy útil recuperar, en lo posible, el significado original de las mismas. Esta es una tarea delicada que exige comprobar cuidadosamente cada detalle.

En lo que sigue, consideraremos fijados el grado n y un primo p; $I=\{i_1,\ldots,i_r\}$, por su parte, será un determinado conjunto de exponentes.

Notación. Dado $P_n(X)= X^n + \sum_{i\in I} \binom{n}{n-i} b_{n-i}\, X^i$, denotaremos como $\overline{P}_n(X)$ al polinomio reducido módulo p de $P_n(X)$, esto es,

$$\overline{P}_n(X) = X^n + \sum_{i\in I} \overline{\binom{n}{n-i}}\, b_{n-i}\, X^i,$$

donde $\overline{\binom{n}{n-i}}$ denota la imagen del número combinatorio $\binom{n}{n-i}$ mediante la aplicación característica $\varphi:\mathbb{Z}\to\mathbb{Z}/_{(p)}$. Obsérvese que las b_{n-i} permanecen como indeterminadas.

Del mismo modo, para cada $k=1,\ldots,n-2$, escribiremos

$$\overline{P}_n^{[k]}(X) = X^{n-k} + \sum_{\substack{i\in I\\ i\geq k}} \overline{\binom{n-k}{n-i}}\, b_{n-i}\, X^{i-k},$$

y también

$$\overline{H}^{[k]} = \mathrm{Res}\big(\overline{P}_n,\, \overline{P}_n^{[k]}\big) \in \mathbb{Z}/_{(p)}\big[b_2,\ldots,b_{n-1}\big].$$

Lema 3.2.1. *La ecuación* $H^{[k]}=0$ *admite como solución sobre* $\overline{\mathbb{F}}_p$ *a la* $(n-2)$*-upla* $\beta=(\beta_2,\ldots,\beta_{n-1})\in {\overline{\mathbb{F}}_p}^{n-2}$ *si y solo si los dos polinomios*

$$\overline{P}_{n,\beta}(X) = X^n + \sum_{i=1}^{n-2} \overline{\binom{n}{n-i}}\, \beta_{n-i}\, X^i \quad y \quad \overline{P}^{[k]}_{n,\beta}(X) = X^{n-k} + \sum_{i=1}^{n-2} \overline{\binom{n-k}{n-i}}\, \beta_{n-i}\, X^{i-k},$$

pertenecientes a $\overline{\mathbb{F}}_p[X]$, *comparten una raíz en* $\overline{\mathbb{F}}_p$.

Demostración. El valor $H^{[k]}(\beta) \in \overline{\mathbb{F}}_p$ es, por construcción, igual a la resultante de los polinomios

$$P_{n,\beta}(X) = X^n + \sum_{i=1}^{n-2} \tbinom{n}{n\text{-}i}\, \beta_{n\text{-}i}\, X^i \quad \text{y} \quad P_{n,\beta}^{[k]}(X) = X^{n-k} + \sum_{i=1}^{n\text{-}2} \tbinom{n\text{-}k}{n\text{-}i}\, \beta_{n\text{-}i}\, X^{i-k}$$

bajo el supuesto de que sus grados son, respectivamente, n y $n-k$. Esta suposición es, en ambos, casos, correcta (lo garantiza el hecho de ser polinomios formalmente mónicos: el coeficiente 1 no es nulo en ninguna característica). Entonces, de acuerdo con lo expuesto en la sección 1.3, la anulación de $H^{[k]}(\beta)$ es condición necesaria y también suficiente para que los polinomios $P_{n,\beta}(X)$ y $P_{n,\beta}^{[k]}(X)$ compartan alguna raíz en el cuerpo algebraicamente cerrado $\overline{\mathbb{F}}_p$.

Ahora bien, en la $\mathbb{Z}$-álgebra $\overline{\mathbb{F}}_p$, multiplicar por un factor entero h consiste justamente en multiplicar por el número $\varphi(h) \in \mathbb{Z}/_{(p)} = \mathbb{F}_p$, de modo que, desde cualquier punto de vista, $\overline{P}_{n,\beta}(X)$ es el mismo polinomio que $P_{n,\beta}(X)$, así como $\overline{P}_{n,\beta}^{[k]}(X)$ es el mismo polinomio que $P_{n,\beta}^{[k]}(X)$. Por tanto, el que $(\beta_2, \ldots, \beta_{n-1}) \in \overline{\mathbb{F}}_p{}^{n\text{-}2}$ satisfaga la ecuación $H^{[k]} = 0$ tiene exactamente el significado que le otorga el enunciado del lema. □

Observación 3.2.2. Por la misma razón, el valor $\overline{H}^{[k]}(\beta) = \mathrm{Res}\big(\overline{P}_{n,\beta}\,,\, \overline{P}_{n,\beta}^{[k]}\big) \in \overline{\mathbb{F}}_p$ es idéntico al valor $H^{[k]}(\beta) = \mathrm{Res}\big(P_{n,\beta}\,,\, P_{n,\beta}^{[k]}\big)$. Así que, tratándose de determinar el conjunto de puntos $Z_{n,I}\big(\overline{\mathbb{F}}_p\big)$, la ecuación $\overline{H}^{[k]} = 0$ es indistinguible de $H^{[k]} = 0$.

Comentario 3.2.3. Los polinomios reducidos módulo p, $\overline{P}_n(X)$ y $\overline{P}_n^{[k]}(X)$, son redundantes con $P_n(X)$ y $P_n^{[k]}(X)$; en efecto, cuando se les *especializa* en un punto $(\beta_2, \ldots, \beta_{n\text{-}1}) \in \overline{\mathbb{F}}_p{}^{n\text{-}2}$, unos y otros proporcionan iguales resultados. Ahora bien, el hecho de disponer de ellos *como objetos formales* distintos de sus análogos sin reducir aportará claridad en posteriores razonamientos.

Comentario 3.2.4. Del lema precedente se sigue que, ciertamente, el sistema de ecuaciones $H^{[i_1]} = H^{[i_2]} = \ldots = H^{[i_r]} = 0$ (siendo $b_{n\text{-}k} = 0 \ \forall j \in J \smallsetminus I$) recoge las condiciones necesarias y suficientes para que un polinomio de la forma

$$\overline{P}_n(X) = X^n + \sum_{i \in I} \overline{\tbinom{n}{n\text{-}i}}\, b_{n\text{-}i}\, X^i, \qquad \text{con } b_{n\text{-}i} \in \overline{\mathbb{F}}_p,$$

comparta en $\overline{\mathbb{F}}_p$ una raíz con cada uno de los polinomios

$$\overline{P}_n^{[1]}(X)\,, \quad \overline{P}_n^{[2]}(X)\,, \quad \ldots \quad, \ \overline{P}_n^{[n\text{-}2]}(X).$$

Sin embargo, los $\overline{P}_n^{[k]}(X)$ no admiten una interpretación obvia como derivadas sucesivas de $\overline{P}_n(X)$ (al menos, cuando $p \leq n$), pues en característica p el concepto de derivada pierde

consistencia. En efecto, con la derivada habitual, la incorporación de factores procedentes del exponente convierte en nulos algunos de los términos del resultado (de hecho, la derivada de orden p será el polinomio nulo); en el caso de las derivadas de Hasse y netas, además, la eliminación de factores producida por la división ocasiona la eventual reaparición de términos al derivar sucesivamente. El siguiente ejemplo muestra lo errático que puede ser este comportamiento:

Consideramos el polinomio $P(X) = X^6 + X^5 \in \overline{\mathbb{F}}_2[X]$. En característica 2,

$$\begin{aligned} P'(X) &= 6X^5 + 5X^4 = X^4 \\ P''(X) &= 4X^3 = 0. \end{aligned}$$

Si decidimos emplear la derivada de Hasse, entonces:

$$\begin{aligned} P^{<1>}(X) &= 6X^5 + 5X^4 = X^4 \\ P^{<2>}(X) &= 15X^4 + 10X^3 = X^4 \\ P^{<3>}(X) &= 20X^3 + 10X^2 = 0 \\ P^{<4>}(X) &= 15X^2 + 5X = X^2 + X \\ P^{<5>}(X) &= 6X + 1 = 1. \end{aligned}$$

La derivada neta, en este caso, ni siquiera puede ser utilizada ya que sería

$$P^{[1]}(X) = \frac{1}{6} \cdot (6X^5 + 5X^4) = X^5 + \frac{5}{6} X^4,$$

lo cual carece de sentido en característica 2. En realidad, la derivada neta solo está definida para aquellos polinomios que admitan ser escritos en *presentación binómica*, esto es, $P_6(X) = X^6 + \binom{6}{1} b_1 X^5 + \binom{6}{2} b_2 X^4 + \cdots$, lo cual no sucede en este ejemplo ya que en $\overline{\mathbb{F}}_2$ la igualdad $\binom{6}{1} b_1 = 1$ es imposible.

Incluso en los casos en que la derivada neta está definida, no está bien definida. Como ejemplo, en característica 5 se tiene el polinomio $P(X) = X^5$; como este polinomio coincide con $P_5(X) = X^5 + \binom{5}{1} b_1 X^4 + \binom{5}{2} b_2 X^3 + \binom{5}{3} b_3 X^2 + \binom{5}{4} b_4 X$ cualesquiera que sean los valores que se dé a las indeterminadas b_k, ocurrirá que

$$\begin{aligned} P^{[1]}(X) &= X^4 + \binom{4}{1} b_1 X^3 + \binom{4}{2} b_2 X^2 + \binom{4}{3} b_3 X + \binom{4}{4} b_4 = \\ &= X^4 + 4b_1 X^3 + b_2 X^2 + 4b_3 X + b_4, \end{aligned}$$

de modo que la derivada neta de $P(X) = X^5$ coincide con una infinidad de polinomios distintos.

Naturalmente, nada de esto ocurría en característica cero, donde la aplicación $\mathbb{K}$-lineal

$$\begin{array}{rccc} L_0 : & \mathbb{K}^n & \longrightarrow & \mathbb{K}[X]_{<n} \\ & (b_1, \ldots, b_n) & \longmapsto & \sum_{i=1}^{n} \binom{n}{i} b_i X^{n-i} \end{array}$$

es biyectiva, y por tanto todo polinomio mónico de grado n admite una presentación binómica que además es única. De ese modo, la aplicación $\mathbb{K}$-lineal que a cada polinomio de $\mathbb{K}[X]_{<n}$ le envía a su derivada neta de orden k puede factorizarse a través de $\mathbb{K}^n$ usando

$$\begin{array}{rccc} L_k: & \mathbb{K}^n & \longrightarrow & \mathbb{K}[X]_{<n-k} \\ & (b_1,\ldots,b_n) & \longmapsto & \sum_{i=1}^{n-k} \binom{n-k}{i} b_i\, X^{n-i-k}, \end{array}$$

con lo cual queda bien definida en $\mathbb{K}[X]_{<n}$.

En característica p podemos simular este buen comportamiento si, en vez de trabajar con el concepto de polinomio, lo hacemos con un nuevo concepto, al que denominaremos *polinomio presentado*. Un polinomio presentado $P_n(X)$ es un polinomio que admite presentación binómica y para el que se ha fijado (como estructura adicional a la de polinomio) una presentación binómica concreta que hace explícito el valor de cada uno de los b_i, incluso en el caso de que su correspondiente *cofactor*, $\binom{n}{i}$, sea nulo en característica p. Así, un mismo polinomio da lugar a tantos polinomios presentados como presentaciones binómicas diferentes admita. Es claro que, sobre polinomios presentados, la derivación neta y las derivaciones netas sucesivas sí que están bien definidas, y satisfacen todas las propiedades anteriormente indicadas para la derivación neta.

Observación 3.2.5. En ausencia de una forma de derivar que corresponda al significado que la derivada tiene en característica cero, no parece factible *a priori* trasladar a característica p la idea del problema de Casas-Alvero. Evidentemente, sí que puede trasladarse el problema de la existencia de polinomios que compartan una raíz en $\overline{\mathbb{F}}_p$ con determinados otros polinomios (esto lo hace el esquema basado en la anulación de las resultantes) pero, en principio, si tales *otros* polinomios no responden en aspectos muy básicos a lo que cabe entender por *derivada*, no parece razonable identificarlo como un genuino problema de Casas-Alvero. No obstante, en el capítulo 5, los teoremas 5.3.1 y 5.5.2 mostrarán que en todo caso el problema sí puede ser formulado sobre $\overline{\mathbb{F}}_p$ sin ninguna ambigüedad.

3.3. Eliminación de monomios módulo p

Hemos visto que la reducción módulo p puede provocar la *desaparición* —por ser múltiplo de p su correspondiente coeficiente binómico, $\binom{n}{n-i}$— de muchos de los términos de $P_n(X)$; en esta sección mostraremos consecuencias útiles de este hecho. Comenzamos viendo el caso extremo en que todos los términos distintos del líder quedan eliminados.

Teorema 3.3.1 (Resolución por interpretación). *Si al reducir módulo p un I-polinomio $P_n(X) = X^n + \sum_{i\in I} \binom{n}{n-i} b_{n-i}\, X^i$ se obtiene $\overline{P}_n(X) = X^n$, entonces $Z_{n,I}\big(\overline{\mathbb{F}}_p\big) = \emptyset$.*

Demostración. Para cada $k \in I$, el lema 3.2.1 permite traducir la ecuación $H^{[k]} = 0$ por la afirmación siguiente:

$$\overline{P}_n(X) = X^n \text{ comparte una raíz en } \overline{\mathbb{F}}_p \text{ con } \overline{P}_n^{[k]}(X) = X^{n-k} + \sum_{\substack{i \in I \\ i > k}} \overline{\binom{n-k}{n-i}}\, b_{n-i}\, X^{i-k} + \overline{\binom{n-k}{n-k}}\, b_{n-k}.$$

Ahora bien, dado que X^n no tiene otra raíz que $\alpha = 0$, tal afirmación significa que se cumple la igualdad

$$\overline{P}_n^{[k]}(0) = 0$$

lo cual, calculando la evaluación indicada en el primer miembro, resulta ser

$$1 \cdot b_{n-k} = 0.$$

Queda así probado que, bajo la hipótesis $\overline{P}_n(X) = X^n$, el sistema de ecuaciones que define a $Z_{n,I}\big(\overline{\mathbb{F}}_p\big)$ exige la anulación de todas las componentes y no tiene, por tanto, más solución que la trivial. □

Conviene llamar la atención sobre la potencia del lema 3.2.1 para transformar cada ecuación $H^{[k]} = 0$ (en la que posiblemente figuren varias o incluso todas las indeterminadas b_j) en una afirmación simple acerca de b_{n-k} que la deja resuelta. La mera interpretación del significado que $H^{[k]} = 0$ tiene en característica p ha hecho innecesario aplicar otras técnicas usuales en la resolución de ecuaciones.

Como primera aplicación del teorema 3.3.1 se logra ya demostrar la conjetura de Casas-Alvero para una infinidad de números: todos aquellos que sean potencia de un primo.

Corolario 3.3.2. *La conjetura de Casas-Alvero es cierta para todo número de la forma* $n = p^r$.

Demostración. Gracias a la proposición 3.1.4, es suficiente con demostrar que el esquema $Y_{p^r} = Z_{p^r,J}$ (siendo J el conjunto completo de exponentes) carece de puntos sobre $\overline{\mathbb{F}}_p$, es decir, que se cumple $Y_{p^r}\big(\overline{\mathbb{F}}_p\big) = \emptyset$. Pero esto es consecuencia inmediata del teorema 3.3.1, puesto que, como es bien conocido, se verifica:

$$\text{Para todo } i = 1, 2, \ldots, p^r - 1, \qquad \binom{p^r}{i} \equiv 0 \mod p,$$

de modo que el reducido módulo p del polinomio $P_n(X) = X^n + \sum_{i=1}^{p^r-2} \binom{p^r}{p^r - i} b_{p^r-i}\, X^i$ es justamente $\overline{P}_n(X) = X^n$. □

Notación. Dado un conjunto de exponentes $I = \{i_1, i_2, \ldots, i_r\}$ y un primo p, denotaremos por I_p al conjunto de los exponentes (diferentes de n) que se conservan cuando se reduce módulo p el I-polinomio $P_n(X) = X^n + \sum_{i \in I} \binom{n}{n-i} b_{n-i}\, X^i$. Esto es:

$$I_p = \Big\{\, i \in I \mid \ \overline{\tbinom{n}{n\text{-}i}} \neq 0 \,\Big\} \ = \ \Big\{\, i \in I \mid \ \tbinom{n}{i} \not\equiv 0 \mod p \,\Big\}$$

En consecuencia, para el polinomio reducido se tienen dos expresiones alternativas:

$$\overline{P}_n(X) = X^n + \sum_{i \in I} \overline{\tbinom{n}{n\text{-}i}}\, b_{n\text{-}i}\, X^i \ = \ X^n + \sum_{i \in I_p} \overline{\tbinom{n}{n\text{-}i}}\, b_{n\text{-}i}\, X^i,$$

dado que si $j \in I \smallsetminus I_p$ entonces el término $\overline{\tbinom{n}{n\text{-}j}}\, b_{n\text{-}j}\, X^j$ no precisa ser consignado.

Observación 3.3.3. El enunciado del teorema de resolución por interpretación (3.3.1) puede ahora reescribirse del siguiente modo: " *Si* $I_p = \emptyset$, *entonces* $Z_{n,I}\big(\overline{\mathbb{F}}_p\big) = \emptyset$ "

El hecho de que un determinado monomio $\overline{\tbinom{n}{n\text{-}j}}\, b_{n\text{-}j}\, X^j$ quede eliminado de $\overline{P}_n(X)$ a causa de la congruencia $\tbinom{n}{j} \equiv 0 \mod p$ no significa que la variable $b_{n\text{-}j}$ vaya a desaparecer del problema que nos ocupa, consistente en hallar $Z_{n,I}\big(\overline{\mathbb{F}}_p\big)$ o, lo que es igual, en resolver sobre $\overline{\mathbb{F}}_p$ el sistema de ecuaciones

$$H^{[i_1]} = H^{[i_2]} = \ldots = H^{[i_r]} = 0\,; \qquad b_{n\text{-}i} = 0 \quad \forall i \in J \smallsetminus I, \tag{3.5}$$

puesto que dicha variable $b_{n\text{-}j}$ aparecerá en los sucesivos polinomios $\overline{P}_n^{\,[k]}(X)$ acompañada del factor $\overline{\tbinom{n\text{-}k}{n\text{-}j}}$, el cual no tiene por qué ser nulo. Por tanto, todas las variables $b_{n\text{-}j}$ con $j \in I \smallsetminus I_p$ siguen tan vigentes como incógnitas del sistema (3.5) como las variables $b_{n\text{-}i}$ con $i \in I_p$, que permanecen visibles en $\overline{P}_n(X)$. Se presenta, no obstante, la siguiente peculiaridad:

Proposición 3.3.4. *Se considera el I-polinomio $P_n(X) = X^n + \sum_{i \in I} \tbinom{n}{n\text{-}i} b_{n\text{-}i}\, X^i$, así como su reducido módulo p, $\overline{P}_n(X) = X^n + \sum_{i \in I_p} \overline{\tbinom{n}{n\text{-}i}}\, b_{n\text{-}i}\, X^i$. Para cada $k \in I_p$ se cumple:*

$$\overline{P}_n^{\,[k]}(X) = X^{n\text{-}k} + \sum_{\substack{i \in I_p \\ i \geq k}} \overline{\tbinom{n\text{-}k}{n\text{-}i}}\, b_{n\text{-}i}\, X^{i\text{-}k}.$$

Es decir, para aquellas derivadas $P_n^{\,[k]}(X)$ cuyo orden de derivación pertenezca al conjunto I_p, la reducción módulo p elimina todos los términos que involucren a las indeterminadas $b_{n\text{-}j}$ con $j \in I \smallsetminus I_p$, de modo que $\overline{P}_n^{\,[k]}(X)$ solo contiene indeterminadas que estuvieran efectivamente presentes en $\overline{P}_n(X)$.

Demostración. Debemos comprobar que si el término $\tbinom{n}{n\text{-}j} b_{n\text{-}j}\, X^j$ está presente en $P_n(X)$ pero desaparece al pasar a $\overline{P}_n(X)$, entonces el término $\tbinom{n\text{-}k}{n\text{-}j} b_{n\text{-}j}\, X^{j\text{-}k}$, que está presente

en $P_n^{[k]}(X)$ para $k \leq j$, también va a desaparecer al pasar a $\overline{P}_n^{[k]}(X)$, siempre y cuando k coincida con alguno de los exponentes supervivientes en $\overline{P}_n(X)$.

Partimos, por tanto, de la siguiente situación:

$$k \in I_p, \quad j \in I \smallsetminus I_p, \quad 1 \leq k < j < n \tag{3.6}$$

(pues, obviamente, la igualdad $k = j$ es imposible), y nuestro objetivo es demostrar la congruencia $\binom{n-k}{n-j} \equiv 0 \mod p$. La clave para lograrlo se encuentra en la igualdad (2.14) establecida en el comentario 2.3.5, según la cual:

$$\binom{n}{n-k}\binom{n-k}{n-j} = \binom{n}{n-j}\binom{j}{k}. \tag{3.7}$$

En efecto, de (3.6) se desprende que p divide a $\binom{n}{n-j}$ pero no divide a $\binom{n}{n-k}$. En estas condiciones, el segundo factor del primer miembro en (3.7) debe ser, necesariamente, múltiplo de p. □

Ejemplo. Con $n = 10$, $I = \{5, 6, 7, 8\}$, $p = 5$, se tiene:

$$P_{10}(X) = X^{10} + 45\, b_2\, X^8 + 120\, b_3\, X^7 + 210\, b_4\, X^6 + 252\, b_5\, X^5.$$

Podemos observar que $\binom{10}{2} = 45$, $\binom{10}{3} = 120$ y $\binom{10}{4} = 210$ son congruentes con 0 módulo 5, mientras que $\binom{10}{5} = 252$ no lo es, de modo que

$$\overline{P}_{10}(X) = X^{10} + \overline{2}\, b_5\, X^5, \quad \text{y además} \quad I_p = \{5\}.$$

En los polinomios $\overline{P}_{10}^{[k]}(X)$ pueden encontrarse b_2, b_3, b_4 y b_5; así, por ejemplo:

$$\begin{aligned} P_{10}^{[2]}(X) &= X^8 + 28\, b_2\, X^6 + 56\, b_3\, X^5 + 70\, b_4\, X^4 + 56\, b_5\, X^3, \\ P_{10}^{[3]}(X) &= X^7 + 21\, b_2\, X^5 + 35\, b_3\, X^4 + 35\, b_4\, X^3 + 21\, b_5\, X^2 \end{aligned}$$

y por tanto

$$\begin{aligned} \overline{P}_{10}^{[2]}(X) &= X^8 + \overline{3}\, b_2\, X^6 + b_3\, X^5 + b_5\, X^3, \\ \overline{P}_{10}^{[3]}(X) &= X^7 + b_2\, X^5 + b_5\, X^2. \end{aligned}$$

Ahora bien, la proposición 3.3.4 garantiza que en $\overline{P}_{10}^{[5]}(X)$ no van a figurar b_2, b_3 ni b_4. Y, en efecto, se tiene

$$P_{10}^{[5]}(X) = X^5 + 10\, b_2\, X^3 + 10\, b_3\, X^2 + 5\, b_4\, X + b_5,$$

de modo que: $\overline{P}_{10}^{[5]}(X) = X^5 + b_5$.

Según se vio en la observación 3.1.1, al ser I_p un subconjunto de I, Z_{n,I_p} es un subesquema de $Z_{n,I}$ y, en particular, se verifica la inclusión $Z_{n,I_p}(\overline{\mathbb{F}}_p) \subset Z_{n,I}(\overline{\mathbb{F}}_p)$, de donde se sigue trivialmente la implicación

$$Z_{n,I}(\overline{\mathbb{F}}_p) = \emptyset \quad \Longrightarrow \quad Z_{n,I_p}(\overline{\mathbb{F}}_p) = \emptyset.$$

Lo que resulta llamativo (y útil) es que también es cierta la implicación recíproca.

Teorema 3.3.5 (Resolución por elevación). *Sea I el conjunto de exponentes correspondiente al I-polinomio de grado n $P_n(X) = X^n + \sum_{i\in I} \binom{n}{n-i} b_{n-i} X^i$, y sea p un número primo. Se verifica*

$$Z_{n,I_p}(\overline{\mathbb{F}}_p) = \emptyset \quad \Longleftrightarrow \quad Z_{n,I}(\overline{\mathbb{F}}_p) = \emptyset.$$

Demostración. Falta solamente demostrar la implicación hacia la derecha. Con el fin de distinguir claramente entre los esquemas $Z_{n,I}$ y Z_{n,I_p} introducimos un polinomio auxiliar, el I_p-polinomio genérico $Q_n(X) = X^n + \sum_{i\in I_p} \binom{n}{n-i} b_{n-i} X^i$, al que vamos a referir la construcción de Z_{n,I_p}.

Pongamos $I_p = \{k_1, k_2, \ldots, k_s\} \subset I = \{i_1, i_2, \ldots, i_r\}$. Sabemos que $Z_{n,I}(\overline{\mathbb{F}}_p)$ es la subvariedad proyectiva de $\mathbb{P}^{n-3}_{2,3,\ldots,n-1}(\overline{\mathbb{F}}_p)$ definida por el sistema de ecuaciones $H^{[i_1]} = H^{[i_2]} = \ldots = H^{[i_r]} = 0$; $b_{n-i} = 0 \ \forall i \in J \setminus I$ o, equivalentemente, (ver observación 3.2.2) por el sistema de ecuaciones

$$\overline{H}^{[i_1]} = \overline{H}^{[i_2]} = \ldots = \overline{H}^{[i_r]} = 0\,; \qquad b_{n-i} = 0 \ \forall i \in J \setminus I, \tag{3.8}$$

donde $\overline{H}^{[i]} = \mathrm{Res}\big(\overline{P}_n(X), \overline{P}_n^{[i]}(X)\big)$ para cada $i = i_1, \ldots, i_r$. De igual manera, $Z_{n,I_p}(\overline{\mathbb{F}}_p)$ es la subvariedad proyectiva del mismo espacio proyectivo pesado definida por el sistema de ecuaciones

$$\widehat{H}^{[k_1]} = \widehat{H}^{[k_2]} = \ldots = \widehat{H}^{[k_s]} = 0\,; \qquad b_{n-i} = 0 \ \forall i \in J \setminus I_p, \tag{3.9}$$

donde $\widehat{H}^{[i]} = \mathrm{Res}\big(\overline{Q}_n(X), \overline{Q}_n^{[i]}(X)\big)$ para cada $i = k_1, \ldots, k_s$. Cuando la inclusión $I_p \subset I$ es estricta (el caso contrario carece de interés), $Q_n(X)$ es distinto de $P_n(X)$: le faltan algunos de sus términos. Pero como se trata justo de los términos que la reducción módulo p hace desaparecer, sucede que $\overline{P}_n(X)$ y $\overline{Q}_n(X)$ son iguales.

Por otra parte, para un orden de derivación dado, $k = 1, \ldots, n-2$, los polinomios $P_n^{[k]}(X)$ y $Q_n^{[k]}(X)$ difieren en los términos de la forma $\binom{n-k}{n-i} b_{n-i} X^{i-k}$ con $i \in I \setminus I_p$, $i \geq k$; la proposición 3.3.4 garantiza que para $k \in I_p$ estos términos desaparecen al reducir módulo p, de modo que la igualdad $\overline{P}_n^{[k]}(X) = \overline{Q}_n^{[k]}(X)$, que no es en general cierta para k arbitrario, sí que es cierta para $k = k_1, k_2, \ldots, k_s$. Queda así probado que para toda $k \in I_p$

se verifica

$$\widehat{H}^{[k]} = \mathrm{Res}\big(\ \overline{Q}_n(X),\ \overline{Q}_n^{[k]}(X)\ \big) = \mathrm{Res}\big(\ \overline{P}_n(X),\ \overline{P}_n^{[k]}(X)\ \big) = \overline{H}^{[k]}.$$

Observemos que estas resultantes involucran exclusivamente a las indeterminadas $b_{n\text{-}k_1}$, $b_{n\text{-}k_2}$,..., $b_{n\text{-}k_s}$. Estamos ya en condiciones de resolver el sistema (3.8), lo cual se efectuará en dos etapas:

Etapa 1. La hipótesis $Z_{n,I_p}\big(\overline{\mathbb{F}}_p\big) = \emptyset$ significa que el sistema (3.9) únicamente posee la solución trivial; por tanto, el conjunto de condiciones $\widehat{H}^{[k_1]} = \widehat{H}^{[k_2]} = \ldots = \widehat{H}^{[k_s]} = 0$ implica que $b_{n\text{-}k_1} = b_{n\text{-}k_2} = \ldots = b_{n\text{-}k_s} = 0$. Ahora bien, como acabamos de ver, este sistema es indistinguible a todos los efectos del sistema $\overline{H}^{[k_1]} = \overline{H}^{[k_2]} = \ldots = \overline{H}^{[k_s]} = 0$; se concluye entonces que el subsistema de (3.8) formado por estas s ecuaciones obliga a que sean nulas $b_{n\text{-}k_1}, b_{n\text{-}k_2}, \ldots, b_{n\text{-}k_s}$, esto es, justo las variables presentes en $P_n(X)$ que sobreviven a la reducción módulo p de dicho polinomio.

Etapa 2. Una vez conocido que $b_{n\text{-}k_1}, b_{n\text{-}k_2}, \ldots, b_{n\text{-}k_s}$ son nulas, podemos sustituirlas por 0 en $P_n(X)$, pero entonces tenemos

$$\overline{P}_n(X) = X^n + \sum_{i\in I_p} \overline{\tbinom{n}{n\text{-}i}} \cdot 0 \cdot X^i = X^n.$$

Aplicando el teorema 3.3.1 (de resolución por interpretación) se obtiene que las $r-s$ incógnitas pendientes de despejar en el sistema (3.8) han de ser también nulas, esto es, en definitiva, que $Z_{n,I}\big(\overline{\mathbb{F}}_p\big) = \emptyset$. □

La proposición 3.1.2 caracterizaba en términos de esquemas la respuesta afirmativa a los diversos problemas de Casas-Alvero. Más adelante, la proposición 3.1.4 (basada en la proposición 3.0.3 de Schicho, Graf von Bothmer, Labs y Van de Woestijne) proporcionó una condición suficiente para tal respuesta afirmativa. El teorema 3.3.5 de resolución por elevación multiplica la potencia de dicha proposición al anteponer otra condición suficiente mucho menos exigente y más sencilla de verificar en ciertos casos. A continuación recordamos conjuntamente estas tres contribuciones, que van a confluir en un corolario de extraordinaria aplicabilidad en el futuro.

[**3.1.2**] El I-problema parcial de Casas-Alvero de grado n tiene respuesta afirmativa si y solo si $Z_{n,I}(\mathbb{C}) = \emptyset$.

[**3.1.4**] Si para el primo p se cumple $Z_{n,I}\big(\overline{\mathbb{F}}_p\big) = \emptyset$, entonces $Z_{n,I}(\mathbb{C}) = \emptyset$.

[**3.3.5**] Si para el primo p se cumple $Z_{n,I_p}\big(\overline{\mathbb{F}}_p\big) = \emptyset$, entonces $Z_{n,I}\big(\overline{\mathbb{F}}_p\big) = \emptyset$ (y además es trivialmente cierta la implicación recíproca).

Corolario 3.3.6. *Sea $n \in \mathbb{N}$, sea $J = \{1, 2, \ldots, n-2\}$, y sea $I \subset J$.*

Es condición suficiente para que el I-problema parcial de Casas-Alvero de grado n tenga respuesta afirmativa, que exista un número primo p tal que $Z_{n,I_p}(\overline{\mathbb{F}}_p) = \emptyset$.

En particular, si existe un primo p tal que $Z_{n,J_p}(\overline{\mathbb{F}}_p) = \emptyset$, entonces la conjetura de Casas-Alvero de grado n es verdadera.

Demostración. La primera afirmación resulta de considerar la cadena de implicaciones

$$Z_{n,I_p}(\overline{\mathbb{F}}_p) = \emptyset \;\Rightarrow\; Z_{n,I}(\overline{\mathbb{F}}_p) = \emptyset \;\Rightarrow\; Z_{n,I}(\mathbb{C}) = \emptyset \;\Rightarrow\; \boxed{\text{No existen } I\text{-contraejemplos a la conjetura de Casas-Alvero de grado n}}$$

Después, basta recordar que el esquema Y_n coincide con $Z_{n,J}$, y por tanto

$$Z_{n,J_p}(\overline{\mathbb{F}}_p) = \emptyset \Rightarrow Y_n(\overline{\mathbb{F}}_p) = Z_{n,J}(\overline{\mathbb{F}}_p) = \emptyset \Rightarrow Y_n(\mathbb{C}) = \emptyset \Rightarrow \boxed{\text{La conjetura de Casas-Alvero de grado } n \text{ no admite contraejemplo alguno}}$$

□

3.4. Triángulo de Tartaglia en característica positiva

Como se acaba de ver, fijado n, la conjetura de Casas-Alvero de grado n queda probada si se logra encontrar un primo p tal que $Z_{n,J_p}(\overline{\mathbb{F}}_p) = \emptyset$, lo cual equivale a que sea $Y_n(\overline{\mathbb{F}}_p) = \emptyset$ (más adelante, y debido a que zanja afirmativamente el problema total de Casas-Alvero en grado n, de un primo con esta cualidad diremos que es un *primo eficaz con* n). Dado que existen infinitos primos disponibles, se plantea la cuestión de cuáles entre ellos pueden más plausiblemente conducir a la deseada igualdad $Z_{n,J_p}(\overline{\mathbb{F}}_p) = \emptyset$, y en una primera aproximación parece conveniente que J_p sea lo más *pequeño* —en cuanto a cardinal— posible. Recordemos que J viene denotando el conjunto *completo* de exponentes a considerar en el problema de Casas-Alvero de grado n, de modo que

$$J = \{1, 2, \ldots, n-2\} \qquad \text{y} \qquad J_p = \{\, i \in J \mid \tbinom{n}{i} \not\equiv 0 \mod p \,\}.$$

Así pues,para visualizar J_p basta tomar de la línea $(n+1)$-ésima del triángulo de Tartaglia todos los elementos a excepción del primero y los dos últimos, según se muestra:

$$\tbinom{n}{0} \boxed{\tbinom{n}{1}\ \tbinom{n}{2}\ \tbinom{n}{3}\ \tbinom{n}{4}\ \cdots\ \tbinom{n}{n-3}\ \tbinom{n}{n-2}} \tbinom{n}{n-1}\ \tbinom{n}{n},$$

reduciéndolos a continuación módulo p; los elementos de J_p indican las *posiciones* en las que resulta un valor no nulo. Localizar situaciones en que J_p posee pocos elementos requiere por tanto observar en qué filas del triángulo de Tartaglia la reducción módulo p produce mayor cantidad de ceros. Para este fin será de gran utilidad la proposición siguiente.

Proposición 3.4.1. *Sea p un número primo, y sean $h, r \in \mathbb{N}$. Se verifican las siguientes congruencias:*

1. $\binom{hp^r}{kp^r} \equiv \binom{h}{k} \mod p$, para todo $k = 0, 1, 2, \ldots, h$.
2. $\binom{hp^r}{i} \equiv 0 \mod p$, para todo $i \neq 0\cdot p^r,\ 1\cdot p^r,\ 2\cdot p^r,\ \ldots,\ h\cdot p^r$.

En particular, (caso $h=1$), $\binom{p^r}{i} \equiv 0 \mod p$ para todo i diferente de 0 y de p^r.

Demostración. La fórmula del binomio de Newton junto con el evidente hecho de que el número combinatorio $\binom{p}{i}$ es múltiplo de p para todo $i = 1, \ldots, p-1$ proporcionan la identidad, válida en característica p,

$$\big(a+b\big)^p = a^p + b^p,$$

de donde resulta

$$\big(a+b\big)^{p^2} = \Big[\big(a+b\big)^p\Big]^p = \big(a^p + b^p\big)^p = a^{p^2} + b^{p^2}$$

e, iterando el procedimiento,

$$\big(a+b\big)^{p^r} = a^{p^r} + b^{p^r}.$$

Siempre en característica p, se obtiene

$$\big(a+b\big)^{hp^r} = \Big[\big(a+b\big)^{p^r}\Big]^h = \Big[a^{p^r} + b^{p^r}\Big]^h = \sum_{k=0}^{h} \binom{h}{k} a^{p^r(h-k)}\, b^{p^r k},$$

expresión que necesariamente coincide —en cuanto polinomio de $\mathbb{F}_p[a, b]$— con la dada directamente por la fórmula del binomio de Newton,

$$\big(a+b\big)^{hp^r} = \sum_{i=0}^{hp^r} \binom{hp^r}{i} a^{hp^r - i}\, b^i.$$

Identificando los coeficientes de una y otra expresión se obtienen ya las congruencias del enunciado. □

Comentario 3.4.2. El fascinante triángulo de Tartaglia en característica p (ver, en la figura 3.1, el caso $p=3$) presenta estructura fractal, y son las líneas correspondientes a las potencias de p las que delimitan las unidades de distinto orden que lo configuran; tales líneas —las que contienen a los números $\binom{p^r}{i}$ para $i = 0, 1, \ldots, p$— están formadas exclusivamente por ceros salvo, naturalmente, los elementos inicial y final, iguales a 1.

La porción del triángulo de Tartaglia que queda *por encima* de la línea p^r sería la *unidad de orden* r, $T(r)$. Para cada $h = 1, \ldots, p-1$, en la línea hp^r son nulos todos los elementos excepto los de la forma $\binom{hp^r}{kp^r}$ para $k = 0, 1, \ldots, h$, los cuales componen una réplica exacta

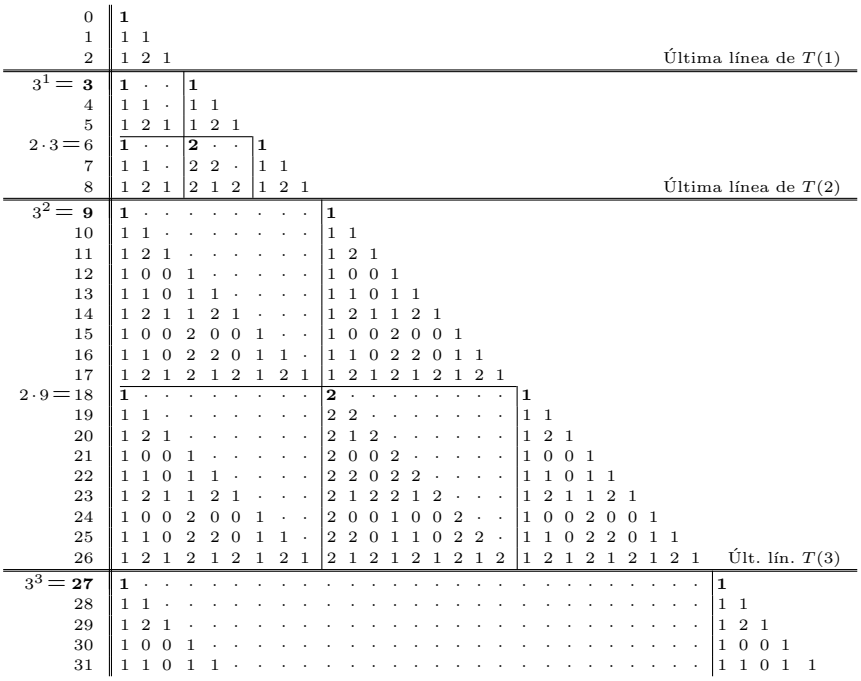


Figura 3.1: Fractal de Tartaglia en característica 3. Los puntos representan ceros

de la línea h, dado que se cumple $\binom{hp^r}{kp^r} \equiv \binom{h}{k} \mod p$. Además, cada uno de estos números resulta ser el vértice superior de un triángulo igual al triángulo unidad de orden r, $T(r)$ multiplicado por cierto factor que, lógicamente, coincide con el valor que se encuentra en dicho vértice, $\binom{h}{k}$. Esos $h+1$ triángulos *colgados* de la línea hp^r dejan libres h zonas triangulares —en posición invertida respecto de aquellos— de p^r-1 filas de altura; todos los elementos ubicados en estas áreas son iguales a cero. A fin de resaltar visualmente la estructura, en la figura 3.1 estos ceros se han representado mediante puntos.

Tenemos así que el trapecio formado por la línea hp^r junto con las p^r-1 líneas siguientes es un mosaico cuyas piezas son las $h+1$ copias del triángulo $T(r)$ multiplicadas por los respectivos $\binom{h}{k}$, y los h triángulos invertidos, totalmente llenos de ceros (puntos, en la figura 3.1) que aparecen intercalados. Agregando al triángulo $T(r)$ los $p-1$ trapecios que arrancan de las líneas hp^r con $h = 1, 2, \ldots, p-1$, respectivamente, se forma el triángulo $T(r+1)$, unidad de orden $r+1$ en el fractal. Es de destacar el hecho de que toda esta precisa construcción queda completamente explicada por la proposición 3.4.1 junto con el modo en que se propagan hacia las líneas inferiores los valores de los números combinatorios, según la propiedad fundamental $\binom{n}{i} + \binom{n}{i+1} = \binom{n+1}{i+1}$.

Observación 3.4.3. Como alternativa a la demostración que se basa en la fórmula de Newton, encontramos la justificación aritmética de las congruencias dadas en 3.4.1 obser-

vando la igualdad

$$\binom{hp^r}{kp^r}=\frac{\boxed{hp^r}\cdot(hp^r\text{-}1)\cdots\boxed{(hp^r\text{-}p)}\cdot(hp^r\text{-}p\text{-}1)\cdots\boxed{(hp^r\text{-}2p)}\cdot(hp^r\text{-}2p\text{-}1)\ \cdots\ \cdots\ \cdots\ (hp^r\text{-}kp^r+1)}{\boxed{kp^r}\cdot(kp^r\text{-}1)\cdots\boxed{(kp^r\text{-}p)}\cdot(kp^r\text{-}p\text{-}1)\cdots\boxed{(kp^r\text{-}2p)}\cdot(kp^r\text{-}2p\text{-}1)\ \cdots\ \cdots\ \cdots\ 1}$$

en la que se han recuadrado los factores que son múltiplo de p; puede apreciarse que van perfectamente emparejados en numerador y denominador. Además, los factores sin recuadrar comprendidos entre ellos van siendo congruentes módulo p con $-1,-2,\ldots,1-p$, también de forma paralela en numerador y denominador, de modo que sus respectivos cocientes valen siempre 1 módulo p. Por otra parte, considerando solo los recuadros, hay arriba $kp^{r\text{-}1}$ factores decrecientes de p en p a partir de hp^r, y lo mismo abajo, esta vez a partir de kp^r; dividiendo entre p a cada uno de ellos se conserva el valor entero de la expresión, que ahora es directamente interpretable como $\binom{hp^{r-1}}{kp^{r-1}}$. Queda así probada la cadena de congruencias $\binom{hp^r}{kp^r}\equiv\binom{hp^{r-1}}{kp^{r-1}}\equiv\binom{hp^{r-2}}{kp^{r-2}}\equiv\cdots\equiv\binom{h}{k}\mod p$.

El proceso anterior no requiere que h sea primo con p, y puede aplicarse al caso $r>s$ para demostrar que $\binom{hp^r}{kp^s}\equiv\binom{hp^{r-s}}{k}\mod p$. El caso opuesto, $r<s$, puede obviarse, pues una simple reescritura lo lleva al caso $r=s$; en el siguiente ejemplo se muestra cómo:

$$\binom{200\cdot 7^3}{3\cdot 7^5}=\binom{200\cdot 7^3}{200\cdot 7^3-3\cdot 7^5}=\binom{200\cdot 7^3}{(200-3\cdot 7^2)\,7^3},\qquad \text{y}\quad 7\nmid(200-3\cdot 7^2).$$

Según esto, para ver qué sucede con $\binom{hp^r}{i}$ cuando i no es de la forma kp^r basta considerar el caso $\binom{hp^r}{k}$ donde k es primo con p. Se tendrá, entonces, $k=c\cdot p+m$, con $0<m<p$. El número combinatorio $\binom{hp^r}{cp}$ puede ser múltiplo de p, o no serlo; este hecho no reviste importancia. Lo significativo es que $\binom{hp^r}{k}=\binom{hp^r}{cp+m}$ se obtiene a partir de $\binom{hp^r}{cp}$ incorporando los m factores que le faltan en numerador y denominador:

$$\binom{hp^r}{k}=\binom{hp^r}{cp+m}=\frac{\boxed{(hp^r-cp)}\cdot(hp^r-cp-1)\cdots(hp^r-cp-m+1)}{(cp+m)\cdot(cp+m-1)\cdots(cp+1)}\cdot\binom{hp^r}{cp}\qquad(3.10)$$

Los factores que se añaden al denominador van desde $cp+1$ hasta $cp+m$; ninguno de ellos es, por tanto, múltiplo de p. Por el contrario, al numerador le llega *seguro* un múltiplo de p (ver recuadro), hp^r-cp, junto con otros varios factores. La fracción surgida en (3.10) es, pues, un elemento nulo en $\mathbb{F}_p$, concluyéndose que también lo es $\binom{hp^r}{k}$.

3.5. Los casos de cardinal 1 y 2 para I_p

En el capítulo 2 quedó demostrado que, sea cual sea el grado n que se considere, la conjetura de Casas-Alvero no admite ningún $\{i\}$-contraejemplo ni tampoco ningún $\{i,j\}$-contraejemplo (corolarios 2.2.3 y 2.3.4, respectivamente). Naturalmente, la segunda negación incluye lo dicho por la primera; no obstante, conviene resaltar el carácter autónomo

de esta, cuya previa obtención constituyó un paso necesario para llegar hasta la segunda. En términos de esquemas proyectivos estos resultados se expresan de la siguiente manera:

$$\text{Para todo } n\in\mathbb{N},\quad \forall i,j\in\{1,2,\dots,n\text{-}2\},\quad Z_{n,\{i\}}(\mathbb{C})=\emptyset\quad \text{y}\quad Z_{n,\{i,j\}}(\mathbb{C})=\emptyset.$$

En el ámbito de la proposición 3.1.4 (*Si* $Z_{n,I}(\overline{\mathbb{F}}_p)=\emptyset$, *entonces* $Z_{n,I}(\mathbb{C})=\emptyset$), los conjuntos de la forma $Z_{n,\{i\}}(\overline{\mathbb{F}}_p)$ o $Z_{n,\{i,j\}}(\overline{\mathbb{F}}_p)$ carecen de interés pues, como acabamos de ver, aquellos resultados a los que podrían darnos acceso han sido ya establecidos con anterioridad; sin embargo, tras el teorema de resolución por elevación y su corolario 3.3.6 cobran un extraordinario valor. Identificar bajo qué condiciones resultan ser vacíos dichos conjuntos va a proporcionar conclusiones que no se limitan a los $\{i\}$ ó $\{i,j\}$-problemas, sino que se extienden a cualquier I-problema para el que pueda hallarse un primo p tal que el conjunto $I_p=\left\{\, i\in I \mid \binom{n}{i}\not\equiv 0 \mod p\right\}$ tenga, o bien cardinal 1, o bien cardinal 2.

Es precisamente el trabajo desarrollado en el capítulo 2 para establecer los preliminares de los resultados arriba reseñados el que permite dar inmediata respuesta a esta cuestión.

Teorema 3.5.1. (a) $Z_{n,\{i\}}(\overline{\mathbb{F}}_p)=\emptyset$ *si y solo si* $\binom{n}{i}\not\equiv 1 \mod p$.

(b) $Z_{n,\{i,j\}}(\overline{\mathbb{F}}_p)=\emptyset$ *si y solo si se cumplen las tres condiciones siguientes:*

(i) $a\not\equiv 1 \mod p$

(ii) $b\not\equiv 1 \mod p$

(iii) $a^{\rho}(b-c)^{\rho}(b-ac)^{\sigma}-(-1)^{\sigma}(a-1)^{\rho+\sigma}(b-1)^{\rho}\not\equiv 0 \mod p$,

siendo $a=\binom{n}{i}$, $b=\binom{n}{j}$, $c=\binom{n\text{-}i}{n\text{-}j}$ y $\rho=\frac{n\text{-}j}{d}$, $\sigma=\frac{j\text{-}i}{d}$, *con* $d=\text{m.c.d.}(n-j,j-i)$.

Demostración. (a) El esquema $Z_{n,\{i\}}$ está definido por las ecuaciones $H^{[i]}=0$; $b_{n\text{-}j}=0$ para todo $j\in J\smallsetminus\{i\}$. La proposición 2.2.2 había dejado establecido que es

$$H^{[i]}=\ b^{n}_{n\text{-}i}\Big[1-\binom{n}{n\text{-}i}\Big]^{n\text{-}i}. \tag{3.11}$$

Sobre el cuerpo $\overline{\mathbb{F}}_p$ la ecuación $H^{[i]}=0$ es equivalente a $b_{n\text{-}i}=0$ si y solo si es $\overline{1-\binom{n}{n\text{-}i}}\neq 0$, esto es, si el entero $\binom{n}{n\text{-}i}=\binom{n}{i}$ no es congruente con 1 módulo p. En caso contrario, cualquier $\lambda\in\overline{\mathbb{F}}_p$ verificará dicha ecuación y, por tanto, el punto $[\beta]=\big[(0,0,\dots,\lambda,0,\dots,0)\big]$ pertenecerá al conjunto $Z_{n,\{i\}}(\overline{\mathbb{F}}_p)$.

(b) El esquema $Z_{n,\{i,j\}}$, a su vez, responde a la ecuaciones $H^{[i]}=H^{[j]}=0$; $b_{n\text{-}k}=0$ para todo $k\in J\smallsetminus\{i,j\}$. Según la proposición 2.3.2, se tiene

$$\begin{aligned} H^{[i]}&=\ (-1)^{rs+r}\ \ b^{j}_{n\text{-}i}\ \Big[\,\alpha^{\rho}\beta^{\sigma}\ b^{\rho+\sigma}_{n\text{-}j}+(-1)^{\rho\sigma+\sigma}\ \gamma^{\rho+\sigma}\ \ b^{\rho}_{n\text{-}i}\,\Big]^{d}\\ H^{[j]}&=\quad (-1)^{r}\quad b^{i}_{n\text{-}j}\ \Big[\quad \delta^{\rho}\ \ b^{\rho+\sigma}_{n\text{-}j}+(-1)^{\rho\sigma}\ (1+\gamma)^{\rho}\ \ b^{\rho}_{n\text{-}i}\,\Big]^{d}\end{aligned} \tag{3.12}$$

donde $\alpha = b-c, \quad \beta = b-ac, \quad \gamma = a-1, \quad \delta = b-1, \quad r = n-j = \rho d, \quad s = j-i = \sigma d.$

Según el apartado (a) de la presente proposición, (i) y (ii) son las condiciones necesarias y suficientes para que sea $Z_{n,\{i\}}\big(\overline{\mathbb{F}}_p\big) = \emptyset$ y $Z_{n,\{j\}}\big(\overline{\mathbb{F}}_p\big) = \emptyset$; esto es, para que el sistema en dos incógnitas $H^{[i]} = H^{[j]} = 0$ no admita soluciones con solo una componente distinta de cero. Hemos de ver que, en esa situación, (iii) equivale a que no exista para dicho sistema ninguna solución con *ambas* componentes distintas de cero.

La demostración es muy similar a la del teorema 2.3.3; igual que allí, una solución $\big(p, q\big)$ con $p \cdot q \neq 0$ se caracteriza por anular los dos polinomios que aparecen encerrados entre corchetes en (3.12), lo cual significa que $\big(p^{\rho+\sigma},\, q^{\rho}\big)$ satisface el sistema de ecuaciones lineales en las incógnitas u y v,

$$\begin{aligned} \alpha^{\rho}\beta^{\sigma}\ \mathrm{u}\ +\ (-1)^{\rho\sigma+\sigma}\ \gamma^{\rho+\sigma}\ \mathrm{v}\ &=\ 0 \\ \delta^{\rho}\ \mathrm{u}\ +\ (-1)^{\rho\sigma}\ (1+\gamma)^{\rho}\ \mathrm{v}\ &=\ 0, \end{aligned} \tag{3.13}$$

cuya matriz de coeficientes tiene justamente determinante

$$\Delta = (-1)^{\rho\sigma}\Big[a^{\,\rho}\,\big(b-c\big)^{\rho}\big(b-ac\big)^{\sigma} - (-1)^{\sigma}\big(a-1\big)^{\rho+\sigma}\big(b-1\big)^{\rho}\Big].$$

Por tanto, la anulación (módulo p) de Δ es condición necesaria para la existencia de $\big(p, q\big)$. Para comprobar que es también suficiente, es preciso descartar la existencia de soluciones no triviales para el sistema (3.13) que sean de la forma $(u_0, 0)$ o $(0, v_0)$. Pero es que, al sustituir una solución del tipo $(u_0, 0)$ en la segunda ecuación del sistema, se tendría

$$\delta^{\rho}\, u_0 = 0, \ \text{ con } \ u_0 \neq 0 \quad \Longrightarrow \quad \delta = b-1 = 0, \quad \text{en contra de (ii)},$$

mientras que, al sustituir una solución de la forma $(0, v_0)$ en la primera ecuación, se tendría

$$(-1)^{\rho\sigma+\sigma}\ \gamma^{\rho+\sigma}\, v_0 = 0, \ \text{ con } v_0 \neq 0 \quad \Longrightarrow \quad \gamma = a-1 = 0, \quad \text{en contra de (i)},$$

luego quedan, en efecto, descartadas tales soluciones. □

Observación 3.5.2. La demostración de 3.5.1(a) ha puesto de manifiesto que, en el contexto del esquema $Z_{n,\{i\}}$, la hipótesis $\binom{n}{i} \equiv 1 \mod p$ convierte sobre $\overline{\mathbb{F}}_p$ a la ecuación $H^{[i]} = 0$ en una tautología. Es de interés precisar la razón por la que esto ocurre. Y es que

$$\left.\begin{aligned} &P_n(X) = X^n + \tbinom{n}{n-i} b_{n-i}\, X^i = X^i\Big[\, X^{n-i} + \tbinom{n}{n-i} b_{n-i}\Big] \\ &P_n{}^{[i]}(X) = X^{n-i} + 1 \cdot b_{n-i} \\ &\tbinom{n}{i} \equiv 1 \mod p \end{aligned}\right\} \ \Rightarrow\ \overline{P}_n(X) = X^i \cdot \overline{P}_n{}^{[i]}(X)$$

de modo que en tal situación, $\overline{P}_n{}^{[i]}(X)$ forzosamente comparte, no ya una, sino *todas* sus raíces con $\overline{P}_n(X)$.

Nos ocupamos ahora del caso en que I_p tiene cardinal 1.

Proposición 3.5.3. *Se considera fijado un grado n y un conjunto de exponentes $I \subset J = \{1, 2, \ldots, n-2\}$. Si existe un primo p tal que $I_p = \{i\}$ y además $\binom{n}{i} \not\equiv 1 \mod p$, entonces el I-problema de Casas-Alvero de grado n tiene respuesta afirmativa.*

Demostración. Según el teorema 3.5.1(a), de la hipótesis $\binom{n}{i} \not\equiv 1 \mod p$ se sigue que $Z_{n,\{i\}}(\overline{\mathbb{F}}_p) = \emptyset$, y dado que $I_p = \{i\}$, ello significa que $Z_{n,I_p}(\overline{\mathbb{F}}_p) = \emptyset$. Estamos, pues, en condiciones de aplicar el corolario 3.3.6 para obtener la conclusión requerida. □

Corolario 3.5.4. *La conjetura de Casas-Alvero es verdadera para los infinitos números de la forma $n = 2p^r$.*

Demostración. Sea $n = 2p^r$ para cierto primo p, siendo $r \geq 1$. Por la proposición 3.4.1 se sabe que $\binom{2p^r}{i} \equiv 0 \mod p$ para todos los valores de $i \in J = \{1, 2, \ldots, 2p^r - 2\}$ excepto para $i = p^r$, para el cual es $\binom{2p^r}{p^r} \equiv \binom{2}{1} \mod p$. Esto es,

$$J_p = \{p^r\} \quad \text{y} \quad \binom{n}{p^r} \equiv 2 \not\equiv 1 \mod p$$

(puesto que nunca $2-1$ puede ser múltiplo de p). Basta aplicar ahora la proposición 3.5.3 para obtener que el J-problema (esto es, el problema *total*) de Casas-Alvero de grado n tiene respuesta afirmativa. □

Pasamos a ocuparnos del caso en que I_p tiene cardinal 2.

Proposición 3.5.5. *Sea $n \in \mathbb{N}$ y sea $I \subset J = \{1, 2, \ldots, n-2\}$. Para que el I-problema de Casas-Alvero de grado n tenga respuesta afirmativa es condición suficiente que exista un primo p para el cual sea $I_p = \{i, j\}$ y se cumpla:*

(*i*) $a \not\equiv 1 \mod p$

(*ii*) $b \not\equiv 1 \mod p$

(*iii*) $a^{\rho}(b-c)^{\rho}(b-ac)^{\sigma} - (-1)^{\sigma}(a-1)^{\rho+\sigma}(b-1)^{\rho} \not\equiv 0 \mod p$,

siendo $a = \binom{n}{i}$, $b = \binom{n}{j}$, $c = \binom{n-i}{n-j}$ *y* $\rho = \frac{n-j}{d}$, $\sigma = \frac{j-i}{d}$, *con* $d = \text{m.c.d.}(n-j, j-i)$.

Demostración. En la situación del enunciado se tiene que $Z_{n,I_p}(\overline{\mathbb{F}}_p) = \emptyset$, de acuerdo con el teorema 3.5.1(b). Puede, por tanto, aplicarse el corolario 3.3.6, el cual concluye la prueba. □

Corolario 3.5.6. *La conjetura de Casas-Alvero es verdadera para todo número de la forma $n = 3p^r$, siendo $p \neq 2$.*

Demostración. Para el conjunto completo de exponentes, $J=\{1,\,2,\,\ldots\,,\,3p^r-2\}$ y en aplicación de la proposición 3.4.1 —relativa a las congruencias módulo p que satisfacen los números del tipo $\binom{hp^r}{i}$— se obtiene

$$J_p=\{i,\,j\},\quad \text{donde } i=p^r\,,\quad \text{y}\quad j=2p^r,$$
$$a=\tbinom{n}{i}=\tbinom{3p^r}{p^r}\equiv\tbinom{3}{1}=3\mod p,$$
$$b=\tbinom{n}{j}=\tbinom{3p^r}{2p^r}\equiv\tbinom{3}{2}=3\mod p,$$
$$c=\tbinom{n\text{-}i}{n\text{-}j}=\tbinom{2p^r}{p^r}\equiv\tbinom{2}{1}=2\mod p,$$
$$d=\text{m.c.d.}(p^r,p^r)=p^r\,,\quad \rho=\tfrac{p^r}{d}=1\,,\quad \sigma=\tfrac{p^r}{d}=1,$$

según la notación de la proposición 3.5.5. Dicha proposición garantiza, pues, la respuesta afirmativa al J-problema (o problema total) de Casas-Alvero de grado $n=3p^r$, siempre que se cumplan las condiciones

(i) y (ii) $\quad 3\not\equiv 1 \mod p$

(iii) $\quad 3(3-2)(3-6)-(-1)(3-1)^2(3-1)\not\equiv 0 \mod p$, esto es, $-1\not\equiv 0 \mod p$,

condiciones que únicamente excluyen al primo $p=2$.

3.6. Conjeturas de transmisión de hipótesis

Observación 3.6.1. Todo contraejemplo a la conjetura de Casas-Alvero de grado 12, en caso de existir, debe necesariamente cumplir la condición de que sea $b_{11}\neq 0$.

En efecto: si fuera $b_{11}=0$ entonces dicho contraejemplo sería en realidad un I-polinomio con $I=J\smallsetminus\{1\}=\{2,3,\ldots,10\}$. Pero el primo $p=11$ evidentemente divide a todos los números combinatorios de la forma $\binom{12}{i}$ con $i\neq 0,1,11$ y 12, de modo que es $I_{11}=\emptyset$.

El teorema de resolución por interpretación (3.3.1, o bien 3.3.3) nos dice que entonces se tiene $Z_{12,I}(\overline{\mathbb{F}}_{11})=\emptyset$, y la proposición 3.1.4 añade que, de hecho, es $Z_{12,I}(\mathbb{C})=\emptyset$, esto es, que no existe tal contraejemplo carente de término en X.

Teorema 3.6.2. *Si p es un número primo y $r\geq 1$, entonces la conjetura de Casas-Alvero de grado $n=p^r+1$ o $n=2p^r+1$ no admite contraejemplos cuyo término de grado 1 tenga coeficiente nulo.*

Demostración. En caso de ser $n=p^r+1$, la prueba se reduce a formalizar el razonamiento seguido en la observación anterior. Sabemos que la línea del triángulo de Tartaglia que contiene los números $\binom{p^r+1}{i}$ tiene, módulo p, la forma

$$1\quad\boxed{1\quad 0\quad 0\quad 0\quad 0\quad \ldots\quad 0\quad 0\quad 0}\quad 1\quad 1$$

(se ha recuadrado la colección de valores obtenidos cuando i recorre $J=\{1,2,,\ldots,n-2\}$). Como consecuencia de ello podemos afirmar que es $J_p=\{1\}$.

Desafortunadamente, al ser $\binom{n}{1}=p^r+1\equiv 1 \mod p$, no es posible emplear la proposición 3.5.3 con referencia al conjunto J. Tomando en cambio el conjunto de exponentes $I=J\smallsetminus\{1\}$, se cumple

$$I_p=\emptyset \implies Z_{n,I}\big(\overline{\mathbb{F}}_p\big)=\emptyset \implies Z_{n,I}(\mathbb{C})=\emptyset,$$

esto es: entre los polinomios en que está ausente el término de grado 1 no existe ninguno que sirva como contraejemplo a la conjetura.

El caso $n=2p^r+1$, $p\geq 3$ admite una prueba similar a la anterior. Reduciendo módulo p la línea del triángulo de Tartaglia que contiene los números $\binom{2p^r+1}{i}$, queda de la forma

$$1 \quad \boxed{1 \quad 0 \quad 0 \quad 0 \quad \ldots \quad 0 \quad 2 \quad 2 \quad 0 \quad 0 \quad \ldots \quad 0 \quad 0 \quad 0} \quad 1 \quad 1$$

donde el recuadro tiene el mismo significado que arriba, y los valores 2 corresponden a los índices $i=p^r$ e $i=p^r+1$. Así pues, en esta ocasión se tiene $J_p=\{1,p^r,p^r+1\}$ y no disponemos de resultados que permitan extraer conclusiones útiles referidas al conjunto completo de exponentes, J; en cambio, para $I=J\smallsetminus\{1\}$ se tiene $I_p=\{p^r,p^r+1\}$, de modo que podemos emplear la proposición 3.5.5 en relación con los conjuntos I e I_p.

Para aplicar dicha proposición 3.5.5, se considera el conjunto de exponentes I, el primo p, y los índices $i=p^r$ y $j=p^r+1$, y se obtiene:

$$a\equiv 2 \mod p, \qquad b\equiv 2 \mod p, \qquad c=\binom{p^r+1}{p^r}\equiv 1 \mod p, \qquad \rho=p^r, \qquad \sigma=1.$$

Obviamente se satisfacen las condiciones (i) y (ii) del enunciado, pues es $2\not\equiv 1 \mod p$; y también se satisface (iii), ya que se tiene $a^{\,\rho}\,(b-c)^{\rho}(b-ac)^{\sigma}\equiv 0 \mod p$, mientras que, en cambio, es $(-1)^{\sigma}(a-1)^{\rho+\sigma}(b-1)^{\rho}\equiv -1 \mod p$. Se concluye entonces, sucesivamente, que los conjuntos de puntos $Z_{n,I_p}\big(\overline{\mathbb{F}}_p\big)$, $Z_{n,I}\big(\overline{\mathbb{F}}_p\big)$ y $Z_{n,I}(\mathbb{C})$ son vacíos, y que, por tanto, el I-problema parcial de Casas-Alvero de grado n tiene respuesta afirmativa, esto es, que ningún I-polinomio (polinomio carente de término vicelíder, de término independiente y también de término lineal) puede servir como contraejemplo a la conjetura. □

Si $P(X)$ es un polinomio de grado n que, como todos los que venimos considerando a partir de la proposición 1.1.2, carece de término vicelíder y de término independiente, entonces, cualesquiera que sean los enteros $d\geq 2$, $e\geq 1$, los polinomios $[P(X)]^d$ y $X^e\cdot P(X)$ van a carecer no solo de dichos términos sino también del término de grado 1. Supongamos que sea $N=d\cdot n$, o bien $N=e+n$, y que se da una de las dos *circunstancias* siguientes

(i) $N=p^r+1$ o $N=2p^r+1$, donde p es primo y $r\geq 1$.

(*ii*) Se sabe que la conjetura de Casas-Alvero de grado N es cierta.

Entonces, si se supiera que $[P(X)]^d$ o $X^e \cdot P(X)$ verifican las hipótesis de la conjetura de Casas-Alvero en grado N, y puesto que, en virtud o bien del teorema 3.6.2 o bien de dicha conjetura —según que se dé la circunstancia (*i*) o (*ii*)—, no pueden ser contraejemplos de la misma, se tendría la seguridad de que satisfacen su tesis, esto es, que se cumple $[P(X)]^d = X^N$ o $X^e \cdot P(X) = X^N$, de donde se deduciría que es $P(X) = X^n$.

Lo anterior puede considerarse, en teoría, como una posible estrategia para probar la conjetura de Casas-Alvero de grado n para aquellos valores de n en que su validez no haya sido aún establecida. Naturalmente, ello requeriría que fuésemos capaces de demostrar que si $P(X)$ verifica las hipótesis de la conjetura entonces, para valores d, e adecuados, alguno de los polinomios $[P(X)]^d$ o $X^e \cdot P(X)$ también verifica dichas hipótesis. Tenemos así dos nuevas conjeturas: el que verdaderamente se produzca, semejante *transmisión* de las hipótesis de Casas-Alvero en el caso de $[P(X)]^d$ —que llamaremos *propagación*—, y el hecho análogo en el caso de $X^e \cdot P(X)$, que llamaremos *desplazamiento*. Ambas conjeturas, que a continuación pasamos a precisar, resultan equivalentes a la de Casas-Alvero, y nada permite suponer que vayan a mostrarse más asequibles que aquella.

3.6.1. Conjeturas de propagación

Llamaremos *propagación de hipótesis* a la transmisión del cumplimiento de las hipótesis de Casas-Alvero desde un polinomio $P_n(X)$ hasta su potencia d-ésima, $[P_n(X)]^d$. Las hipótesis de Casas-Alvero para el polinomio de partida constan de $n-2$ condiciones; número de condiciones que se convierte en $dn-2$ para el polinomio $[P_n(X)]^d$. Es decir, la transmisión de las hipótesis —en caso de producirse— va acompañada de un efecto multiplicador sobre el número de ítems que las configuran; de ahí el término *propagación* que se ha elegido para designar este fenómeno.

De las dos *circunstancias* en las que, como hemos dicho, nos sería de utilidad que se produjera la propagación de hipótesis,

(*i*) $N = dn$ es de la forma $p^r + 1$ o $2p^r + 1$;

(*ii*) Se sabe cierta la conjetura de Casas-Alvero de grado $N = dn$,

la segunda carece actualmente de aplicabilidad, pues —incluyendo los resultados de esta Memoria—, no se conoce ningún grado n tal que la conjetura de Casas-Alvero aún no haya sido probada para n pero sí que lo haya sido para algún múltiplo suyo, dn.

Por el contrario, cualquiera que sea $n \in \mathbb{N}$, sí que está garantizada la existencia de un número $d \geq 2$ (hay, de hecho, infinitos) para el cual tenga lugar la circunstancia (*i*); ello es consecuencia de un clásico teorema de Dirichlet que recordamos a continuación.

Teorema 3.6.3 (Dirichlet). *Si los números enteros a y d son primos entre sí, entonces en la progresión aritmética dada por $a_n = a + nd$ se encuentran infinitos números primos.*

Demostración. Véase, por ejemplo, [Ser]. □

Teorema 3.6.4. *Las tres conjeturas que se indica son equivalentes entre sí.*

(*a*) *Conjetura de Casas-Alvero de grado n.*

(*b*) *Conjetura de propagación general de grado n: Si $P_n(X) = X^n + \sum_{i=1}^{n-2} \binom{n}{n-i} b_{n-i} X^i \in \mathbb{C}[X]$ comparte una raíz con cada una de sus derivadas de orden menor o igual que $n-2$, entonces para todo $d \in \mathbb{N}$ el polinomio $\left[P_n(X)\right]^d$ comparte una raíz con cada una de sus derivadas de orden menor o igual que $dn-2$.*

(*c*) *Conjetura de propagación selectiva de grado n: Existe $d \in \mathbb{N}$, $d \geq 2$, tal que para $N = dn$ se da la circunstancia (i) o la circunstancia (ii), y tal que si el polinomio $P_n(X) = X^n + \sum_{i=1}^{n-2} \binom{n}{n-i} b_{n-i} X^i \in \mathbb{C}[X]$ comparte una raíz con cada una de sus derivadas de orden menor o igual que $n-2$, entonces $\left[P_n(X)\right]^d$ comparte una raíz con cada una de sus derivadas de orden menor o igual que $dn-2$.*

Demostración. (a)⇒(b): Si $P_n(X)$ comparte respectivas raíces con sus derivadas hasta el orden $n-2$ entonces, de ser cierta la conjetura de Casas-Alvero en grado n, se cumplirá

$$P_n(X) = X^n \qquad \text{y, por lo tanto,} \qquad \left[P_n(X)\right]^d = X^{dn},$$

polinomio que ciertamente comparte una raíz (siempre la misma, $\alpha = 0$) con cada una de sus derivadas, de hecho, hasta el orden $dn-1$.

(b)⇒(c): Se considera la progresión aritmética $\left\{-1+dn\right\}_{d=1}^{\infty}$. Obsérvese que d es aquí el índice variable; n está fijado y es, desde luego, primo con -1. El teorema de Dirichlet garantiza que existen en ella infinitos términos primos, todos los cuales salvo acaso el primero son de la forma $p = dn-1$ con $d \geq 2$. Tomando un valor d que ofrezca esta cualidad, se estará en la circunstancia (i); la conjetura de propagación general asegura el cumplimiento de las restantes condiciones.

(c)⇒(a): Sea $P_n(X) = X^n + \binom{n}{2} b_2 X^{n-2} + \ldots + \binom{n}{n-1} b_{n-1} X$ verificando las hipótesis de Casas-Alvero. La conjetura de propagación selectiva proporciona cierto entero d tal que el polinomio

$$\left[P_n(X)\right]^d = X^{nd} + d\binom{n}{2} b_2 X^{nd-2} + (\text{términos de grado intermedio}) + \binom{n}{n-1}^d b_{n-1}^d X^d$$

satisface todas la hipótesis de la conjetura de Casas-Alvero de grado $N = nd$, sabiendo efectivamente que dicha conjetura es cierta en grado N o bien, en su defecto, que se tiene

$N = p^r + 1$ o $2p^r + 1$, de modo que puede aplicarse el teorema 3.6.2. Cualquiera de estas opciones excluye la posibilidad de que $\big[P_n(X)\big]^d$ sea un contraejemplo a la conjetura de Casas-Alvero de grado N, luego necesariamente es

$$\big[P_n(X)\big]^d = X^N = X^{nd} \quad \text{y, por tanto,} \quad P_n(X) = X^n,$$

como se quería demostrar. □

Observación 3.6.5. Las conjeturas de propagación admiten una formulación en términos geométricos, y también en términos algebraicos. Hagamos algunas consideraciones.

- Aunque el polinomio $\big[P_n(X)\big]^d$ sea de grado dn, sus coeficientes siguen perteneciendo al anillo $\mathbb{Z}\big[b_2, \ldots, b_{n\text{-}1}\big]$.
- Obviamente, $[P_n(X)]^d$ comparte una raíz α con otro polinomio $Q(X)$ si y solo si dicha raíz la comparten $P_n(X)$ y $Q(X)$. Así pues, lo que las conjeturas de propagación afirman es que *el propio* $P_n(X)$ comparte una raíz con cada una de las derivadas (hasta el orden $dn-2$) del polinomio $[P_n(X)]^d$.

Introducimos la notación

$$H^{[d,k]} := \mathrm{Res}\Big(P_n, \big(P_n^d\big)^{[k]}\Big) \in \mathbb{C}\big[b_2, \ldots, b_{n\text{-}1}\big]; \quad \mathcal{I}_d := \Big\langle H^{[d,1]}, H^{[d,2]}, \ldots, H^{[d,nd\text{-}2]} \Big\rangle$$

y recuperamos la notación habitual, $H^{[k]} = \mathrm{Res}\big(P_n, P_n^{[k]}\big)$; $\mathcal{I} = \big\langle H^{[1]}, H^{[2]}, \ldots, H^{[n\text{-}2]} \big\rangle$. Las conjeturas de propagación afirman, entonces, que —para todo d, o bien para un d específico, según el caso—, se tiene

$$\textit{Si} \;\; (\beta_2, \beta_3, \ldots, \beta_{n\text{-}2}) \in V(\mathcal{I}) \;\; \textit{entonces} \;\; (\beta_2, \beta_3, \ldots, \beta_{n\text{-}2}) \in V(\mathcal{I}_d),$$

lo cual se resume en la inclusión $V\big(\mathcal{I}\big) \subset V\big(\mathcal{I}_d\big)$.

Equivalentemente, según el teorema de los Ceros de Hilbert, las conjeturas de propagación postulan —de nuevo, para todo $d \in \mathbb{N}$ o bien solo para cierto d— que el radical de $\mathcal{I}$ contiene al radical de $\mathcal{I}_d$, o lo que es igual, se verifica la inclusión $\mathcal{I}_d \subset \mathrm{Rad}\big(\mathcal{I}\big)$. Esta expresión admite la siguiente reescritura:

$$\text{Para cada } i = 1, 2, \ldots, dn-2, \;\; \text{existe } \; m_i \in \mathbb{N} \;\; \text{tal que } \Big(H^{[d,i]}\Big)^{m_i} \in \mathcal{I}.$$

3.6.2. Conjeturas de desplazamiento

Llamaremos *desplazamiento de hipótesis* a la transmisión del cumplimiento de las hipótesis de Casas-Alvero desde un polinomio $P_n(X)$ hasta el producto $X^e \cdot P(X)$.

Las $n-2$ condiciones que configuran las hipótesis de Casas-Alvero para el polinomio de partida se convertirían esta vez en $e+n-2$ para el polinomio $X^e \cdot P(X)$. Significa

entonces que la transmisión de las hipótesis —en caso de producirse— iría acompañada del incremento (en e unidades) del número de ítems que comprenden; sin embargo este incremento es solo aparente y queda anulado en la práctica, pues para el nuevo polinomio las e primeras condiciones devienen triviales y solamente son significativas las que se refieren a las $n-2$ derivadas de orden más alto. El término *desplazamiento* alude este efecto, y también refleja el hecho de que la multiplicación por X^e simplemente desplaza solidariamente e posiciones a todos los coeficientes del polinomio original.

Para nuestros fines resultaría de utilidad el desplazamiento de hipótesis que tuviera lugar en una de las dos *circunstancias* ya indicadas anteriormente, y que son:

(i) $N=e+n$ es de la forma p^r+1 o $2p^r+1$;

(ii) Se sabe cierta la conjetura de Casas-Alvero de grado $N=e+n$.

Observemos que, cualquiera que sea el entero n, se dispone de infinitos valores e tales que $N=e+n$ sea del tipo p^r o $2p^r$, en cuyo caso —como los corolarios 3.3.2 y 3.5.4 garantizan— se producirá la circunstancia (ii); así mismo, tomando estos mismos valores de e incrementados en una unidad se logra producir la circunstancia (i).

A continuación se va a reproducir *mutatis mutandis* el mismo discurso que en la subsección anterior se refirió a las conjeturas de propagación, referido esta vez a las conjeturas de desplazamiento. Deliberadamente se ha mantenido casi idéntico al otro, de modo que sea patente el paralelismo entre ambos desarrollos.

Teorema 3.6.6. *Las tres conjeturas que se indica son equivalentes entre sí.*

(a) *Conjetura de Casas-Alvero de grado n.*

(b) *Conjetura de desplazamiento general de grado n: Si $P_n(X)=X^n+\sum_{i=1}^{n-2}\binom{n}{n-i}b_{n-i}X^i\in\mathbb{C}[X]$ comparte una raíz con cada una de sus derivadas de orden menor o igual que $n-2$, entonces para todo $e\geq 1$ el polinomio $X^e\cdot P(X)$ comparte una raíz con cada una de sus derivadas de orden menor o igual que $e+n-2$.*

(c) *Conjetura de desplazamiento selectivo de grado n: Existe $e\in\mathbb{N}$, $e\geq 1$, tal que para $N=e+n$ se da la circunstancia (i) o la circunstancia (ii), y tal que si el polinomio $P_n(X)=X^n+\sum_{i=1}^{n-2}\binom{n}{n-i}b_{n-i}X^i\in\mathbb{C}[X]$ comparte una raíz con cada una de sus derivadas de orden menor o igual que $n-2$, entonces $X^e\cdot P(X)$ comparte una raíz con cada una de sus derivadas de orden menor o igual que $e+n-2$.*

Demostración. (a)⇒(b): Si $P_n(X)$ comparte respectivas raíces con sus derivadas hasta el orden $n-2$ entonces, de ser cierta la conjetura de Casas-Alvero en grado n, se cumplirá

$$P_n(X) = X^n \qquad \text{y, por lo tanto,} \qquad X^e \cdot P(X) = X^{e+n},$$

que ciertamente comparte una raíz (siempre la misma, $\alpha = 0$) con cada una de sus derivadas, de hecho, hasta el orden $e+n-1$.

(b)⇒(c): La existencia de infinitos números primos garantiza que existen infinitos enteros $e \geq 1$ tales que $n+e-1$ es un número primo (resp., $n+e$ es un número primo) y que entonces nos sitúan en la circunstancia (i) (resp., atendiendo al corolario 3.3.2, en la circunstancia (ii)). Para un valor e que presente estas características, la conjetura de desplazamiento general asegura el cumplimiento de las restantes condiciones.

(c)⇒(a): Sea $P_n(X) = X^n + \binom{n}{2} b_2 X^{n-2} + \ldots + \binom{n}{n-1} b_{n-1} X$ verificando las hipótesis de Casas-Alvero. La conjetura de desplazamiento selectivo proporciona cierto entero e tal que el polinomio

$$X^e \cdot P(X) = X^{e+n} + \binom{n}{2} b_2 X^{e+n-2} + \ldots + \binom{n}{n-1} b_{n-1} X^{e+1}$$

satisface todas la hipótesis de la conjetura de Casas-Alvero de grado $N = e+n$, sabiendo efectivamente que dicha conjetura es cierta en grado N o bien, en su defecto, que se tiene $N = p^r+1$ o $2p^r+1$, de modo que puede aplicarse el teorema 3.6.2. Cualquiera de estas opciones excluye la posibilidad de que $X^e \cdot P(X)$ sea un contraejemplo a la conjetura de Casas-Alvero de grado N, luego necesariamente es

$$X^e \cdot P(X) = X^N = X^{e+d} \quad \text{y, por tanto,} \quad P_n(X) = X^n,$$

como se quería demostrar. □

Observación 3.6.7. Las conjeturas de desplazamiento admiten también una formulación en términos algebraicos-geométricos análoga a la vista en 3.6.5 para las conjeturas de propagación. En el caso actual, puesto que las e condiciones de que $X^e \cdot P_n(X)$ comparta una raíz con sus derivadas de orden menor o igual que e se verifican trivialmente, bastará considerar las resultantes dadas por

$$H'^{[d,k]} := \mathrm{Res}\Big(P_n, \big(X^e P_n\big)^{[k]}\Big) \in \mathbb{C}\big[b_2, \ldots, b_{n-1}\big]$$

para $k = e+1, \ldots, e+n-2$, y el ideal $\mathcal{I}'_e$ generado por los polinomios $H'^{[d,k]}$.

Las conjeturas de desplazamiento afirman, entonces, que —para todo e, o bien para un e específico, según el caso—, se tiene la inclusión $V(\mathcal{I}) \subset V(\mathcal{I}'_e)$ o, equivalentemente, que para cada $i = e+1, \ldots, e+n-2$ existe un exponente $m_i \in \mathbb{N}$ tal que $\Big(H'^{[d,i]}\Big)^{m_i} \in \mathcal{I}$.

Observación 3.6.8. Merece la pena observar que, si bien el producto por X^e desplaza los coeficientes de $P_n(X)$, no desplaza en cambio la presentación binómica del mismo.

En efecto, el coeficiente $\binom{n}{n-i} b_{n-i}$ de X^i en $P_n(X)$ se desplaza para ser el coeficiente de X^{e+i} en $X^e \cdot P_n(X)$, pero en la presentación binómica propia de este polinomio el coeficiente de X^{e+i} debe ser del tipo $\binom{e+n}{n-i} b'_{n-i}$. La dificultad de probar la conjetura de Casas-Alvero se puede interpretar como la de probar las conjeturas de desplazamiento, cuyo enunciado analítico tiene una visible fuerte dependencia del manejo y de las propiedades de los números combinatorios.

3.6.3. Enunciado transversal al grado

Cada vez que hemos expresado el enunciado de la conjetura de Casas-Alvero en cualquiera de sus formas equivalentes, incluso bajo las modalidades de conjetura de propagación o conjetura de desplazamiento, ha sido preciso hacer alguna referencia explícita al grado n. Esto es, en realidad no estamos hablando de una conjetura, sino de infinitas conjeturas —una por cada entero $n \in \mathbb{N}$— algunas de las cuales han dejado de serlo, puesto que ya han sido demostradas.

Como consecuencia inmediata del teorema 3.6.6 obtenemos un enunciado independiente de n que equivale a la que propiamente cabría llamar *la* conjetura de Casas-Alvero —por contemplar la totalidad de los grados—. El nuevo enunciado ya no se formula *por grados* y no admite ningún tipo de discriminación basada en el grado, esto es, que pueda ser cierta en algunos grados pero no en otros; por el contrario, expresa la transferencia de ciertas propiedades entre polinomios de grados sucesivos.

Corolario 3.6.9. *Las siguientes afirmaciones son equivalentes:*

(a) *La conjetura de Casas-Alvero de grado n es cierta para todo entero positivo n.*

(b) *Si $P(X) \in \mathbb{C}$ es un polinomio que carece de término vicelíder y comparte una raíz con cada una de sus derivadas de grado positivo entonces el polinomio $X \cdot P(X)$ comparte una raíz con cada una de sus derivadas de grado positivo.*

Demostración. (a)⇒(b): Es inmediato, pues siendo cierto (a) y bajo las hipótesis de (b), no puede sino ser $P(X) = X^n$ (para cierto n) y, por tanto, $X \cdot P(X) = X^{n+1}$.

(b)⇒(a): Dado $P_n(X) = X^n + \sum_{i=1}^{n-2} \binom{n}{n-i} b_{n-i} X^i \in \mathbb{C}[X]$ satisfaciendo las hipótesis de la conjetura de Casas-Alvero de grado n, y fijado $e \in \mathbb{N}$, podemos aplicar (b) sucesivamente a los polinomios $P(X)$, $X \cdot P(X)$, $X^2 \cdot P(X)$, ..., $X^{e-1} \cdot P(X)$ para obtener que $X^e \cdot P(X)$ comparte una raíz con cada una de sus derivadas, de hecho, hasta el orden $n+e-1$. Concluimos

de aquí que es verdadera la conjetura de desplazamiento —general o específica, según se quiera— de grado n, equivalente, tal como establece 3.6.6, a la conjetura de Casas-Alvero de ese mismo grado. □

Capítulo 4

Condensación y expansión

La primera proposición recogida en esta Memoria, ya en la sección 1.1, consistió en reducir la conjetura de Casas-Alvero —sin ninguna pérdida de generalidad— al conjunto de los polinomios sin término vicelíder. Consecuentemente con ello, en todos los desarrollos posteriores y, en particular, en la construcción del esquema Y_n, se ha trabajado bajo ese supuesto, que nos libraba de dos indeterminadas y de una ecuación. Tiene sentido plantearse cuál sería el comportamiento del esquema Y_n'', análogo a Y_n , que prescindiendo de la preparación de Tschirnhausen partiera del polinomio general de grado n presentado en forma binómica,

$$P_n(X) \;= X^n + \tbinom{n}{1} b_1\, X^{n-1} + \tbinom{n}{2} b_2\, X^{n-2} + \;\cdots\; + \tbinom{n}{n-2} b_{n-2}\, X^2 + \tbinom{n}{n-1} b_{n-1}\, X + \tbinom{n}{n} b_n$$

y, empleando las resultantes $H^{[i]} := \mathrm{Res}\big(P_n, P_n^{[i]}\big) \in \mathbb{Z}[b_1, b_2, \ldots, b_n]$, quedara definido como subesquema de $\mathbb{P}^{n-1}_{1,2,\ldots,n}$ por las $n-1$ ecuaciones $H^{[1]} = H^{[2]} = \ldots = H^{[n-1]} = 0$.

Pues bien: con este esquema, la respuesta afirmativa al problema de Casas-Alvero no se caracteriza por que $Y_n''(\mathbb{C})$ sea vacío, sino por poseer $Y_n''(\mathbb{C})$ únicamente un punto, $[\tilde{\alpha}] = \big[(-\alpha, \alpha^2, -\alpha^3, \ldots, (-\alpha)^n)\big]$, correspondiente a los infinitos polinomios de la forma $\big(X-\alpha\big)^n$ con $\alpha \neq 0$ que no cumplen $b_1 = b_2 = \ldots = b_n = 0$ pero que no contradicen a la conjetura de Casas-Alvero. La presencia de este punto resulta un inconveniente que se logra evitar imponiendo a $P_n(X)$ la condición de que *una* de sus raíces sea nula, esto es, que sea nulo el término independiente b_n.

4.1. El supraesquema Y_n'

Se considera el polinomio genérico de grado n y término independiente nulo

$$P_n(X) \;= X^n + \tbinom{n}{1} b_1\, X^{n-1} + \tbinom{n}{2} b_2\, X^{n-2} + \;\cdots\; + \tbinom{n}{n-2} b_{n-2}\, X^2 + \tbinom{n}{n-1} b_{n-1}\, X$$

y, para cada $i=1,\ldots,n-1$, se define $H^{[i]}:=\mathrm{Res}\big(P_n, P_n^{[i]}\big)\in\mathbb{Z}\big[b_1,b_2,\ldots,b_{n\text{-}1}\big]$. Denotamos por Y_n' al subesquema del espacio proyectivo pesado $\mathbb{P}^{n-2}_{1,2,\ldots,n\text{-}1}$ definido por las ecuaciones $H^{[1]}=H^{[2]}=\ldots=H^{[n\text{-}1]}=0$.

Observación 4.1.1. Suprimida por construcción la posibilidad de tener $P_n(X)=\big(X-\alpha\big)^n$ con $\alpha\neq 0$, ahora sí que se verifica la equivalencia que se expresa como sigue:

$$Y_n'(\mathbb{C})=\emptyset \quad \textit{si y solo si es verdadera la conjetura de Casas-Alvero de grado } n.$$

Por otra parte, dado que es

$$P_n^{[k]}(X)=X^{n\text{-}k}+\tbinom{n\text{-}k}{1}b_1\,X^{n\text{-}1\text{-}k}+\tbinom{n\text{-}k}{2}b_2\,X^{n\text{-}2\text{-}k}+\ldots+\tbinom{n\text{-}k}{n\text{-}k}b_{n\text{-}k},$$

la condición $b_{n\text{-}k}=0$ garantiza que $P_n(X)$ y $P_n^{[k]}(X)$ comparten la raíz $\alpha=0$; esto es, haciendo $b_{n\text{-}k}=0$ se satisface automáticamente la ecuación k-ésima del sistema, $H^{[k]}=0$. También de esta interesante cualidad carece el esquema Y_n'' mencionado anteriormente, por lo que renunciamos a utilizarlo en lo sucesivo.

Observación 4.1.2. En el contexto del capítulo 3 no se contemplaba a b_1 como variable, y tanto Y_n como todos los demás esquemas $Z_{n,I}$ eran vistos como subesquemas de $\mathbb{P}^{n-3}_{2,\ldots,n\text{-}1}$. Sin más que introducir a $b_1=0$ como la ecuación $(n-1)$-ésima del sistema que lo define, cada uno de estos esquemas pasa a ser considerado subesquema del espacio proyectivo pesado $\mathbb{P}^{n-2}_{1,2,\ldots,n\text{-}1}$.

En este escenario, Y_n' se incorpora de forma natural a esta familia de esquemas al identificarse con $Z_{n,J'}$ para $J'=\big\{1,\,2,\,\ldots\,,\,n-1\big\}$. Su relación con todos ellos responde a la misma lógica que ya conocemos, incluido el abuso de notación que supone denominar a las resultantes de forma indiferenciada como $H^{[i]}$ aunque estén ligadas a conjuntos de exponentes distintos. Es claro que tanto $Y_n=Z_{n,J}$ como los restantes esquemas $Z_{n,I}$ son subesquemas de Y_n', de modo que este ejerce como un *supraesquema* que encabeza toda la jerarquía.

La proposición 1.1.2, según la cual existen contraejemplos a la conjetura de Casas-Alvero de grado n si y solo si existe algún contraejemplo de grado n sin término vicelíder, se traduce en la siguiente equivalencia:

$$Y_n'\big(\mathbb{C}\big)=\emptyset \quad\Longleftrightarrow\quad Y_n\big(\mathbb{C}\big)=\emptyset.$$

Será de gran utilidad establecer el resultado análogo a este que, en lugar de al cuerpo $\mathbb{C}$, se refiera a los cuerpos $\overline{\mathbb{F}}_p$. Como paso previo necesitamos el siguiente lema, donde se muestra

cómo, en característica p, la derivación neta y el cambio de variable correspondiente a una traslación son operaciones que conmutan. Esto no es ninguna trivialidad: en el comentario 3.2.4 ya se puso de manifiesto el peculiar comportamiento de la derivación neta en característica p, que de hecho solo queda bien definida cuando se aplica, no ya a polinomios que *admitan* una presentación binómica, sino a lo que llamamos *polinomios presentados*, esto es, los que vienen acompañados de una presentación binómica explícitamente fijada.

Lema 4.1.3 (Regla de la cadena para la derivada neta en característica p). *Se considera un polinomio presentado de grado n y coeficientes en $\overline{\mathbb{F}}_p$,*

$$P_n(X) \;= c_0\,X^n + \tbinom{n}{1} c_1\,X^{n-1} + \tbinom{n}{2} c_2\,X^{n-2} + \;\cdots\; + \tbinom{n}{n-2} c_{n-2}\,X^2 + \tbinom{n}{n-1} c_{n-1}\,X + \tbinom{n}{n} c_n,$$

y se considera asimismo el cambio de variable $X = \widetilde{X} - a$. En estas condiciones,

(*a*) *El polinomio $P_n(\widetilde{X}-a) \in \overline{\mathbb{F}}_p[\,\widetilde{X}\,]$ viene dado como un polinomio presentado, con una presentación inducida por la de $P_n(X)$.*

(*b*) *Si se considera, para cada $j = 1, 2, \ldots, n-1$, la derivada neta de orden j del polinomio presentado $P_n(X)$,*

$$P_n{}^{[j]}(X) \;= c_0\,X^{n-j} + \tbinom{n-j}{1} c_1\,X^{n-1-j} + \tbinom{n-j}{2} c_2\,X^{n-2-j} + \;\cdots\; + \tbinom{n-j}{n-j} c_{n-j},$$

entonces, para todo $j = 1, 2, \ldots, n-1$ se verifica: $\Big(P_n(\widetilde{X}-a)\Big)^{[j]} = P_n{}^{[j]}(\widetilde{X}-a)\,.$

Demostración. Al realizar en $P_n(X)$ el cambio de variable $X = \widetilde{X} - a$, se obtiene

$$\begin{aligned} P_n(X) \;&=\; P_n(\widetilde{X}-a) = \\ &=\; \tbinom{n}{0} c_0 (\widetilde{X}-a)^n + \tbinom{n}{1} c_1 (\widetilde{X}-a)^{n-1} + \ldots + \tbinom{n}{i} c_i (\widetilde{X}-a)^{n-i} + \ldots + \tbinom{n}{n} c_n = \qquad (4.1) \\ &=\; B_0\,\widetilde{X}^n + B_1\,\widetilde{X}^{n-1} + \ldots + B_k\,\widetilde{X}^{n-k} + \ldots + B_n. \end{aligned}$$

El desarrollo de (4.1) proporciona, expresado en términos de los c_i, el coeficiente de $\widetilde{X}^{n-k}$,

$$B_k = \tbinom{n}{0} c_0 \tbinom{n}{k} (-a)^k + \tbinom{n}{1} c_1 \tbinom{n-1}{k-1} (-a)^{k-1} + \ldots + \tbinom{n}{i} c_i \tbinom{n-i}{k-i} (-a)^{k-i} + \ldots + \tbinom{n}{k} c_k \tbinom{n-k}{0}. \qquad (4.2)$$

En este momento vuelve a ser de aplicación la igualdad (2.13) sobre la que trata el comentario 2.3.5; en este caso y para los números $i \le k < n$ nos conviene expresarla bajo la forma

$$\left(\begin{smallmatrix} n \\ i \end{smallmatrix}\right)\left(\begin{smallmatrix} n-i \\ k-i \end{smallmatrix}\right) = \left(\begin{smallmatrix} n \\ k \end{smallmatrix}\right)\left(\begin{smallmatrix} k \\ i \end{smallmatrix}\right),$$

la cual nos permite sustituir el producto de los dos números combinatorios presentes en cada uno de los términos de (4.2) por otro producto en el que siempre figura el factor $\binom{n}{k}$. De este modo, sacando factor común, resulta

$$B_k = \binom{n}{k}\Big[\sum_{i=0}^{k}\binom{k}{i}c_i\,(-a)^{k-i}\Big]. \tag{4.3}$$

Esto demuestra el primer apartado del lema, ya que, sin más que denotar por b_k al contenido del corchete en la expresión (4.3), se tiene

$$P_n(\widetilde{X}-a) = \tbinom{n}{0}b_0\,\widetilde{X}^n + \tbinom{n}{1}b_1\,\widetilde{X}^{n-1} + \ldots + \tbinom{n}{i}b_i\,\widetilde{X}^{n-i} + \ldots + \tbinom{n}{n}b_n,$$

donde cada $b_i \in \overline{\mathbb{F}}_p$ está perfectamente determinado a partir de los datos $c_0, c_1, \ldots, c_{n-1}, a \in \overline{\mathbb{F}}_p$. Observemos que, en consecuencia, también están definidas las derivadas netas del polinomio presentado $P_n(\widetilde{X}-a)$; en efecto,

$$\Big(P_n(\widetilde{X}-a)\Big)^{[j]} = \tbinom{n-j}{0}b_0\,\widetilde{X}^{n-j} + \tbinom{n-j}{1}b_1\,\widetilde{X}^{n-j-1} + \ldots + \tbinom{n-j}{i}b_i\,\widetilde{X}^{n-j-i} + \ldots + \tbinom{n-j}{n-j}b_{n-j}. \tag{4.4}$$

Por otra parte, si el cambio de variable se efectúa en ${P_n}^{[j]}(X)$, resulta

$$\begin{aligned} {P_n}^{[j]}(X) \;&=\; P_n^{[j]}(\widetilde{X}-a) = \\ &= \tbinom{n-j}{0}c_0(\widetilde{X}-a)^{n-j} + \tbinom{n-j}{1}c_1(\widetilde{X}-a)^{n-j-1} + \ldots + \tbinom{n-j}{i}c_i(\widetilde{X}-a)^{n-j-i} + \ldots + \tbinom{n-j}{n-j}c_{n-j} = \\ &= D_0\,\widetilde{X}^{n-j} + D_1\,\widetilde{X}^{n-j-1} + \ldots + D_k\,\widetilde{X}^{n-j-k} + \ldots + D_{n-j}. \end{aligned} \tag{4.5}$$

Igual que antes, del desarrollo de las potencias en la línea central de (4.5) se obtiene el coeficiente del término de grado $n-j-k$, que es

$$D_k = \tbinom{n-j}{0}c_0\tbinom{n-j}{k}(-a)^k + \tbinom{n-j}{1}c_1\tbinom{n-j-1}{k-1}(-a)^{k-1} + \ldots + \tbinom{n-j}{i}c_i\tbinom{n-j-i}{k-i}(-a)^{k-i} + \ldots + \tbinom{n-j}{k}c_k\tbinom{n-j-k}{0}.$$

De nuevo, el uso de la identidad (2.13), ahora bajo la forma $\binom{n-j}{i}\binom{n-j-i}{k-i} = \binom{n-j}{k}\binom{k}{i}$, permite reescribir D_k, y el resultado es

$$D_k = \binom{n-j}{k}\Big[\sum_{i=0}^{k}\binom{k}{i}c_i\,(-a)^{k-i}\Big].$$

Observamos que el contenido del corchete es justo el mismo que aparecía en (4.3), al que habíamos denotado b_k; de modo que, para todo $k = 0, 1, \ldots, n-j$, se cumple la igualdad $D_k = \binom{n-j}{k}b_k$. Transladando estas igualdades a (4.5) y confrontando el resultado con (4.4) resulta evidente que es, en efecto,

$$\Big(P_n(\widetilde{X}-a)\Big)^{[j]} \;=\; P_n^{[j]}(\widetilde{X}-a)$$

tal como afirma el segundo apartado del lema. □

Si el lema 4.1.3 ha validado en característica p la regla de la cadena para la derivación neta, otro tanto había hecho el lema 3.2.1 con la posibilidad de seguir identificando cada solución del sistema $H^{[1]} = \ldots = H^{[n-1]} = 0$ con un polinomio P_n que comparta raíces con los sucesivos $P_n^{[i]}$, incluso cuando el cuerpo base es $\overline{\mathbb{F}}_p$. Ambos lemas son esenciales en la demostración del siguiente teorema.

Teorema 4.1.4 (Eliminación del vicelíder en característica p). *Dado $n \geq 3$ se consideran los esquemas proyectivos $Y_n' = Z_{n,J'}$ e $Y_n = Z_{n,J}$. Para todo número primo p se verifica la equivalencia*

$$Y_n'\big(\overline{\mathbb{F}}_p\big) = \emptyset \quad \Longleftrightarrow \quad Y_n\big(\overline{\mathbb{F}}_p\big) = \emptyset.$$

Demostración. (⇒) Es una obviedad, pues se tiene la inclusión $Y_n\big(\overline{\mathbb{F}}_p\big) \subset Y_n'\big(\overline{\mathbb{F}}_p\big)$.

(⇐) Esta implicación se va a demostrar bajo su forma contrarrecíproca,

$$Y_n'\big(\overline{\mathbb{F}}_p\big) \neq \emptyset \quad \Longrightarrow \quad Y_n\big(\overline{\mathbb{F}}_p\big) \neq \emptyset.$$

Supongamos que existe algún punto $[c] = \big[(c_1, \ldots, c_{n\text{-}1})\big] \in Y_n'\big(\overline{\mathbb{F}}_p\big)$.

• Si es $c_1 = 0$, entonces $[c]$ pertenece, de hecho, a $Y_n\big(\overline{\mathbb{F}}_p\big)$, y hemos terminado.

• Si es $c_1 \neq 0$, entonces, tomando por ejemplo a $(c_1, \ldots, c_{n\text{-}1}) \in \overline{\mathbb{F}}_p^{n\text{-}1} \smallsetminus \{(0, \ldots, 0)\}$ como representante fijo de $[c]$ tendremos un polinomio presentado, $P_n(X) = X^n + \sum_{i=1}^{n-1} \binom{n}{i} c_i\, X^{n-i} \in \overline{\mathbb{F}}_p[X]$, que comparte una raíz en $\overline{\mathbb{F}}_p$ con cada una de sus derivadas netas; así pues

$$\text{Para cada } j = 1, \ldots, n-1, \quad \text{existe } \alpha_j \in \overline{\mathbb{F}}_p \quad \text{cumpliendo} \quad P_n(\alpha_j) = P_n{}^{[j]}(\alpha_j) = 0$$

Mediante el cambio de variable $X = \widetilde{X} - c_1$, obtenemos el polinomio presentado

$$Q(\widetilde{X}) = P_n(\widetilde{X} - c_1) = \widetilde{X}^n + \tbinom{n}{1} b_1\, \widetilde{X}^{n\text{-}1} + \ldots + + \tbinom{n}{n\text{-}1} b_{n\text{-}1}\, \widetilde{X} + \tbinom{n}{n}\, b_n \in \overline{\mathbb{F}}_p[\widetilde{X}]; \qquad (4.6)$$

según la fórmula (4.3), el coeficiente de $\widetilde{X}^{n\text{-}1}$ es $\binom{n}{1}\big[-c_1 + c_1\big] = \binom{n}{1} \cdot 0$, de modo que se tiene $b_1 = 0$.

Por otra parte, para cada $j = 1, \ldots, n-1$, el elemento $\beta_j = \alpha_j + c_1 \in \overline{\mathbb{F}}_p$ va a ser una raíz compartida por los polinomios $Q(\widetilde{X})$ y $Q^{[j]}(\widetilde{X})$, pues se cumple

$$\begin{aligned} Q(\beta_j) &= P_n(\beta_j - c_1) = P_n(\alpha_j) = 0 \\ Q^{[j]}(\beta_j) &= P_n^{[j]}(\beta_j - c_1) = P_n^{[j]}(\alpha_j) = 0. \end{aligned}$$

(la línea anterior hace uso de la igualdad $Q^{[j]}(\widetilde{X}) = \Big(P_n(\widetilde{X} - c_1)\Big)^{[j]} = P_n^{[j]}(\widetilde{X} - c_1)$, obtenida mediante el lema 4.1.3)

Observemos que, en particular, el hecho de que $Q(\widetilde{X})$ y $Q^{[n\text{-}1]}(\widetilde{X}) = \widetilde{X} + b_1 = \widetilde{X}$ compartan una raíz significa que es, necesariamente, $b_n = 0$.

Se concluye que los coeficientes b_i del polinomio presentado dado en (4.6) configuran una solución sobre $\overline{\mathbb{F}}_p$ del sistema homogéneo $H^{[1]} = \ldots = H^{[n-1]}$ que tiene $b_1 = b_n = 0$, pero que no puede ser la solución trivial. En efecto, si lo fuera, entonces tendríamos $Q(\widetilde{X}) = \widetilde{X}^n$, con lo cual quedaría

$$P_n(X) = P_n(\widetilde{X} - c_1) = Q(\widetilde{X}) = (X + c_1)^n = X^n + \cdots + c_1^n, \quad \text{con } c_1^n \neq 0, \text{ por serlo } c_1;$$

cosa absurda puesto que $P_n(X)$ carecía de término independiente.

Hemos hallado un punto, $b = [(0, b_2, \ldots, b_{n-1})] \in \mathbb{P}^{n-2}_{1,2,\ldots,n-1}(\overline{\mathbb{F}}_p)$, que sin duda pertenece a $Y_n\big(\overline{\mathbb{F}}_p\big)$; queda así probado que este conjunto no es vacío. □

4.2. El método de condensación

El teorema que a continuación se expone constituye en sí mismo una propuesta de actuación frente al problema de Casas-Alvero. Su demostración describe un proceso, que llamaremos *de condensación*, mediante el cual cierto enunciado en grado $n = \mathrm{h}p^r$ se transforma en el enunciado análogo en grado h, con el sorprendente resultado de que ambos enunciados son equivalentes. Es destacable el decisivo papel desempeñado aquí por el teorema (4.1.4) de eliminación del vicelíder en característica p.

Teorema 4.2.1 (Resolución por condensación). *Sea p un número primo, y sean h y r dos números naturales con $h \geq 3$ y $r > 0$. Se verifica la equivalencia*

$$Y_{hp^r}\big(\overline{\mathbb{F}}_p\big) = \emptyset \quad \Longleftrightarrow \quad Y_h\big(\overline{\mathbb{F}}_p\big) = \emptyset.$$

Demostración. Sea $n = hp^r$. Consideramos el polinomio

$$P_n(X) = X^n + \tbinom{n}{2} b_2 X^{n-2} + \cdots + \tbinom{n}{n-1} b_{n-1} X.$$

Utilizaremos los resultados sobre congruencias recogidos en la proposición 3.4.1. Por de pronto, se sabe que solo es $\binom{\mathrm{h}p^r}{j} \not\equiv 0 \mod p$ para $j = 0, p^r, 2p^r, \ldots, \mathrm{h}p^r$, de modo que es $J_p = \{p^r, 2p^r, \cdots, (\mathrm{h}-1)p^r\}$. Entonces, la reducción módulo p nos deja

$$\overline{P}_n(X) = X^{\mathrm{h}p^r} + \binom{\mathrm{h}p^r}{p^r} b_{p^r} X^{(\mathrm{h}-1)p^r} + \binom{\mathrm{h}p^r}{2p^r} b_{2p^r} X^{(\mathrm{h}-2)p^r} + \ldots + \binom{\mathrm{h}p^r}{(\mathrm{h}-1)\,p^r} b_{(\mathrm{h}-1)p^r} X^{p^r}$$

y, además, para cada $k = i \cdot p^r$ con $i = 1, \ldots, \mathrm{h}-1$,

$$\overline{P}_n^{\,[k]}(X) = \overline{P}_n^{\,[ip^r]}(X) = X^{(\mathrm{h}-i)p^r} + \binom{(\mathrm{h}-i)p^r}{p^r} b_{p^r} X^{(\mathrm{h}-i-1)p^r} + \binom{(\mathrm{h}-i)p^r}{2p^r} b_{2p^r} X^{(\mathrm{h}-i-2)p^r} +$$
$$+ \ldots + \binom{(\mathrm{h}-i)p^r}{(\mathrm{h}-i+1)\,p^r} b_{(\mathrm{h}-i+1)p^r} X^{p^r} + \binom{(\mathrm{h}-i)p^r}{(\mathrm{h}-i)\,p^r} b_{(\mathrm{h}-i)p^r}.$$

Sabemos asimismo que es $\binom{\mathrm{h}p^r}{jp^r} \equiv \binom{\mathrm{h}}{j} \mod p$, y también $\binom{(\mathrm{h}\text{-}i)p^r}{jp^r} \equiv \binom{\mathrm{h}\text{-}i}{j} \mod p$, y podemos observar que en todas las potencias de X que aparecen en los anteriores polinomios reducidos el exponente es un múltiplo de p^r; entonces, si introducimos una nueva variable $Y = X^{p^r}$, en característica p será válido escribir

$$\overline{P}_n(X) = Y^{\mathrm{h}} + \binom{\mathrm{h}}{1} b_{p^r}\, Y^{\mathrm{h}\text{-}1} + \ldots + \binom{\mathrm{h}}{\mathrm{h}\text{-}1} b_{(\mathrm{h}\text{-}1)p^r}\, Y \tag{4.7}$$

y, para cada $i = 1, \ldots, \mathrm{h}-1$,

$$\overline{P}_n^{[ip^r]}(X) = Y^{\mathrm{h}\text{-}i} + \binom{\mathrm{h}\text{-}i}{1} b_{p^r}\, Y^{\mathrm{h}\text{-}i\text{-}1} + \ldots + \binom{\mathrm{h}\text{-}i}{\mathrm{h}\text{-}i} b_{(\mathrm{h}\text{-}i)p^r}\,. \tag{4.8}$$

Si denotamos por $Q_h(Y)$ al polinomio en (4.7) se observa que, para cada $i = 1, \ldots, \mathrm{h}-1$, el polinomio en (4.8) es justo $Q_h^{[i]}(Y)$. El hecho que $\overline{P}_n(X)$ y $\overline{P}_n^{[ip^r]}(X)$ compartan una raíz $\alpha \in \overline{\mathbb{F}}_p$, traducido en que se verifiquen las igualdades

$$\begin{aligned} \alpha^{\mathrm{h}p^r} \;+\; \sum_{j=1}^{\mathrm{h}\text{-}1} \binom{\mathrm{h}}{j} b_{jp^r}\, \alpha^{(\mathrm{h}\text{-}j)p^r} \;&=\; 0 \\ \alpha^{(\mathrm{h}\text{-}i)p^r} \;+\; \sum_{j=1}^{\mathrm{h}\text{-}i} \binom{\mathrm{h}\text{-}i}{j} b_{jp^r}\, \alpha^{(\mathrm{h}\text{-}i\text{-}j)p^r} \;&=\; 0\,, \end{aligned}$$

admite ahora la lectura alternativa —y equivalente— de que $Q_h(Y)$ y $Q_h^{[i]}(Y)$ compartan en $\overline{\mathbb{F}}_p$ la raíz $\beta = \alpha^{p^r}$.

Así pues, acerca de una (h-1)-upla $(b_{p^r}, b_{2p^r}, \ldots, b_{(\mathrm{h}\text{-}1)p^r}) \neq (0, 0, \ldots, 0)$ de elementos de $\overline{\mathbb{F}}_p$, es indistinto afirmar

$$\overline{P}_{\mathrm{h}p^r}(X) = X^{\mathrm{h}p^r} + \sum_{j=1}^{\mathrm{h}\text{-}1} \binom{\mathrm{h}p^r}{jp^r} b_{jp^r}\, X^{(\mathrm{h}\text{-}j)p^r} \text{ comparte la raíz } \alpha_i \in \overline{\mathbb{F}}_p \text{ con } \overline{P}_{\mathrm{h}p^r}^{[ip^r]}(X)\ \forall i = 1, \ldots, \mathrm{h}\text{-}1, \tag{4.9}$$

que afirmar

$$Q_{\mathrm{h}}(Y) = Y^{\mathrm{h}} + \sum_{j=1}^{\mathrm{h}\text{-}1} \binom{\mathrm{h}}{j} b_{jp^r}\, Y^{(\mathrm{h}\text{-}j)} \text{ comparte la raíz } \alpha_i^{p^r} \in \overline{\mathbb{F}}_p \text{ con } Q_{\mathrm{h}}^{[i]}(Y)\ \forall i = 1, \ldots, \mathrm{h}\text{-}1, \tag{4.10}$$

luego la existencia de un polinomio $\overline{P}_{\mathrm{h}p^r}(X)$ distinto de $X^{\mathrm{h}p^r}$ que satisfaga (4.9) es solidaria con la existencia de un polinomio $Q_{\mathrm{h}}(Y)$ distinto de Y^{h} que satisfaga (4.10). En otros términos (confrontar con el lema 3.2.1 y comentario 3.2.4), existe sobre $\overline{\mathbb{F}}_p$ una solución no trivial del sistema homogéneo de $\mathrm{h}p^r - 1$ ecuaciones y otras tantas incógnitas

que define al esquema $Z_{\mathrm{h}p^r, \{p^r, 2p^r, \ldots, (\mathrm{h}\text{-}1)p^r\}} = Z_{n, J_p}$, a saber,

$$H^{[p^r]} = H^{[2p^r]} = \ldots = H^{[(\mathrm{h}\text{-}1)p^r]} = 0, \qquad b_{n\text{-}j} = 0 \quad \forall j \neq p^r, 2p^r \ldots, (\mathrm{h}-1)p^r,$$

si y solo si existe sobre $\overline{\mathbb{F}}_p$ una solución no trivial del sistema de $\mathrm{h}-1$ ecuaciones en las

incógnitas $c_j = b_{jp^r}$, $j = 1, 2, \ldots, \mathrm{h}-1$ que define al esquema $Z_{\mathrm{h},\{1,2,\ldots,\mathrm{h\text{-}1}\}} = Y_{\mathrm{h}}'$,

$$\mathcal{H}^{[1]} = \mathcal{H}^{[2]} = \cdots = \mathcal{H}^{[\mathrm{h\text{-}1}]} = 0.$$

—se emplea diferente grafía porque las ecuaciones corresponden a un sistema distinto del anterior—. Hemos demostrado así que se verifica

$$Z_{n,J_p}\big(\overline{\mathbb{F}}_p\big) = \emptyset \quad \Longleftrightarrow \quad Y_{\mathrm{h}}'\big(\overline{\mathbb{F}}_p\big) = \emptyset,$$

implicación que ocupa la posición central en la siguiente cadena:

$$Y_{\mathrm{h}p^r}\big(\overline{\mathbb{F}}_p\big) = Z_{\mathrm{h}p^r,J}\big(\overline{\mathbb{F}}_p\big) = \emptyset \quad \Leftrightarrow \quad Z_{\mathrm{h}p^r,J_p}\big(\overline{\mathbb{F}}_p\big) = \emptyset \quad \Leftrightarrow \quad Y_{\mathrm{h}}'\big(\overline{\mathbb{F}}_p\big) = \emptyset \quad \Leftrightarrow \quad Y_{\mathrm{h}}\big(\overline{\mathbb{F}}_p\big) = \emptyset.$$

Pero primera implicación de la cadena viene justificada por el teorema (3.3.5) de resolución por elevación, y la última es justamente el teorema (4.1.4) de eliminación de vicelíder en característica p. La demostración está, por tanto, completa. □

Corolario 4.2.2. *La conjetura de Casas-Alvero es verdadera para todo número de la forma $n = 4p^r$, siendo $p \neq 3, 5, 7$.*

Demostración. La proposición 3.1.4 garantiza la veracidad de la conjetura de Casas-Alvero para todos aquellos números de la forma $n = 4p^r$ tales que sea $Y_{4p^r}\big(\overline{\mathbb{F}}_p\big) = \emptyset$; ahora bien, según el teorema de condensación 4.2.1, esto último sucede si y solo si es $Y_4\big(\overline{\mathbb{F}}_p\big) = \emptyset$.

Al ser $P_4(X) = X^4 + \binom{4}{2} b_2 X^2 + \binom{4}{3} b_3 X$ un polinomio con solo dos términos adicionales al líder, resulta que el conjunto completo de exponentes a considerar es $J = \{1, 2\}$, de modo que el esquema Y_4 es simplemente $Z_{4,\{1,2\}}$. En estas condiciones podemos aplicar el teorema 3.5.1, apartado b), teniendo en cuenta que es $i = 1$, $j = 2$ y, por tanto:

$$a = \binom{4}{1} = 4; \quad b = \binom{4}{2} = 6; \quad c = \binom{3}{2} = 3; \quad d = \text{m.c.d.}(2,1) = 1; \quad \rho = \frac{2}{1} = 2, \quad \sigma = \frac{1}{1} = 1.$$

Dicha proposición afirma que $Y_4\big(\overline{\mathbb{F}}_p\big) = Z_{4,\{1,2\}}\big(\overline{\mathbb{F}}_p\big)$ es vacío si y sólo si se cumple la terna de condiciones

(i) $4 \not\equiv 1 \mod p$

(ii) $6 \not\equiv 1 \mod p$

(iii) $4^2\,(6-3)^2(6-12)^1 - (-1)^1(4-1)^3(6-1)^2 = -\,3^3 \cdot 7 \not\equiv 0 \mod p.$

Los únicos primos que incumplen alguna de estas condiciones son $p = 3$, $p = 5$ y $p = 7$; para todos los restantes es $Y_4\big(\overline{\mathbb{F}}_p\big) = \emptyset$, tal como se quería demostrar. □

Ejemplo. El problema de Casas-Alvero en grado $n=4\cdot 11^3=5324$ nos hace considerar el polinomio $P_{5324}(X)=X^{5324}+\sum_{i=2}^{5323}\binom{5324}{i}b_i\,X^{5324-i}$, así como sus 5322 primeras derivadas.

Puesto que es $11^3=1331$, tenemos $J_{11}=\{1331,\,2662,\,3993\}$, por lo que, al reducir módulo 11, basta considerar tan solo los polinomios

$$\begin{aligned}
\overline{P}_{5324}(X) &= X^{5324}+\binom{5324}{1331}b_{1331}\,X^{3993}+\binom{5324}{2662}b_{2662}\,X^{2662}+\binom{5324}{3993}b_{3993}\,X^{1331},\\
\overline{P}_{5324}^{[1331]}(X) &= X^{3993}+\binom{3993}{1331}b_{1331}\,X^{2662}+\binom{3993}{2662}b_{2662}\,X^{1331}+b_{3993},\\
\overline{P}_{5324}^{[2662]}(X) &= X^{2662}+\binom{2662}{1331}b_{1331}\,X^{1331}+b_{2662},\\
\overline{P}_{5324}^{[3993]}(X) &= X^{1331}+b_{1331};
\end{aligned}$$

los cuales, mediante el cambio $X^{1331}=Y$, y siendo $\binom{\mathrm{h}\cdot 11^3}{k\cdot 11^3}\equiv\binom{\mathrm{h}}{k}$ mod 11, se reescriben simplemente como

$$\begin{aligned}
Q_4(Y) &= Y^4+\binom{4}{1}b_{1331}\,Y^3+\binom{4}{2}b_{2662}\,Y^2+\binom{4}{3}b_{3993}\,Y,\\
Q_4^{[1]}(Y) &= Y^3+\binom{3}{1}b_{1331}\,Y^2+\binom{3}{2}b_{2662}\,Y+b_{3993},\\
Q_4^{[2]}(Y) &= Y^2+\binom{2}{1}b_{1331}\,Y+b_{2662},\\
Q_4^{[3]}(Y) &= Y+b_{1331}.
\end{aligned}$$

(Aquí, si se prefiere, se puede denotar $b_{1331\cdot i}$ como c_i). Obsérvese que, a diferencia de $\overline{P}_{5324}(X)$, el polinomio $Q_4(Y)$ sí que cuenta con término vicelíder.

Las condiciones acerca de $\overline{P}_{5324}(X)$ que identifican cuándo un punto $[(0,\,b_2,\ldots,\,b_{5323})]$ que tenga nulas todas las componentes de subíndice distinto de 1331, 2662, 3993, pertenece a $Y_{5324}\big(\overline{\mathbb{F}}_{11}\big)$, coinciden exactamente con las condiciones acerca de $Q_4(Y)$ que caracterizan cuándo el punto $[(\,b_{1331},\,b_{2661},\,b_{3993})]=[(c_1,c_2,c_3)]$ pertenece a $Y_4'\big(\overline{\mathbb{F}}_{11}\big)$.

Así pues, existe un punto en $Z_{5324,\{1331,2662,3993\}}\big(\,\overline{\mathbb{F}}_{11}\big)$ si y solo si existe un punto en $Y_4'\big(\,\overline{\mathbb{F}}_{11}\big)$. Sabíamos ya que lo primero equivale a que sea distinto de vacío el conjunto $Y_{5324}\big(\,\overline{\mathbb{F}}_{11}\big)$ (teorema de elevación), y que lo segundo equivale a que sea distinto de vacío el conjunto $Y_4\big(\,\overline{\mathbb{F}}_{11}\big)$ (teorema de eliminación del vicelíder en característica p).

En definitiva, se tiene la equivalencia: $Y_{5324}\big(\,\overline{\mathbb{F}}_{11}\big)\neq\emptyset$ si y solo si $Y_4\big(\,\overline{\mathbb{F}}_{11}\big)\neq\emptyset$.

Pero la cuestión de si existen o no puntos en $Y_4\big(\,\overline{\mathbb{F}}_p\big)$ ya la tenemos resuelta, de hecho, para todo p (ver la demostración del corolario 4.2.2), y sabemos que es $Y_4\big(\,\overline{\mathbb{F}}_{11}\big)=\emptyset$. De modo que también es $Y_{5324}\big(\,\overline{\mathbb{F}}_{11}\big)=\emptyset$, lo cual garantiza que es verdadera la conjetura de Casas-Alvero de grado 5324.

4.3. El principio de expansión

Dado un número n, el interés en disponer de un primo p tal que sea

$$Y_n\big(\overline{\mathbb{F}}_p\big) = \emptyset \tag{4.11}$$

se debe a la proposición 3.1.4, según la cual (4.11) constituye una condición suficiente para que el problema de Casas-Alvero de grado n reciba respuesta afirmativa. Para expresar que n y p verifican tan ventajosa condición diremos que p es un *primo eficaz con* n, y también que el par (n,p) es un *par eficaz*.

Vamos a indagar acerca de cómo son los pares eficaces, y de qué modo pueden obtenerse. Comenzamos por enunciar un resultado que en realidad ya conocemos, y que presenta como única novedad el énfasis en una determinada perspectiva.

Principio de Expansión. *Si h es un número natural con $h \geq 3$, y p es un primo, siendo $p > h$, entonces para todo $r > 0$ se verifica*

$$Y_h\big(\overline{\mathbb{F}}_p\big) = \emptyset \quad \Longrightarrow \quad Y_{hp^r}\big(\overline{\mathbb{F}}_p\big) = \emptyset.$$

En efecto, el recién bautizado principio no es otra cosa que la lectura de derecha a izquierda del teorema de condensación, 4.2.1, para el caso particular de que sea $h < p$. En la terminología recién introducida, el principio de expansión dice lo siguiente:

Principio de Expansión. *Si (h,p) es un par eficaz, siendo $3 \leq h < p$, entonces los infinitos pares de la forma (hp^r, p) con $r \in \mathbb{N}$ son también pares eficaces.*

A un par eficaz (h,p) cumpliendo $h < p$ lo llamaremos *par eficaz básico*; al conjunto formado por los infinitos pares eficaces de la forma (hp^r, p) con $r \in \mathbb{N}$ lo denominaremos *estela de* (h,p). Dado que todo par de la forma (p^r, p) o $(2p^r, p)$ es siempre eficaz —corolarios 3.3.2 y 3.5.4, respectivamente—, convendremos en considerar a los pares $(1,p)$ y $(2,p)$ como pares eficaces básicos, y escribiremos $Y_1\big(\overline{\mathbb{F}}_p\big) = \emptyset$ e $Y_2\big(\overline{\mathbb{F}}_p\big) = \emptyset$ recurriendo a unos esquemas Y_1 e Y_2 carentes de entidad geométrica (ver nota 3.0.5). De este modo, tanto el teorema 4.2.1 como el principio de expansión resultan válidos también para $h = 1$ y $h = 2$, lo que permite eliminar la restricción $h \geq 3$.

Veremos a continuación cómo cada par eficaz (n,p) remite a un único par básico (h,p), a cuya estela pertenece.

Teorema 4.3.1. *Sea (n,p) un par eficaz con $n \geq p$. Existe un único $h \in \mathbb{N}$ tal que*

(i) Es $h < p$,

(ii) $n = hp^r$, para algún $r > 0$,

(iii) $Y_h\big(\overline{\mathbb{F}}_p\big) = \emptyset$;

de modo que (h,p) es un par eficaz básico, y (n,p), un elemento de su estela.

Demostración. Supongamos que el primo p no divide a n, y tomemos el resto k de la división euclídea de n entre p, de modo que es $n=c\cdot p+k$ con $0<k<p<n$. Manifiestamente,

$$\binom{n}{k}=\frac{(c\cdot p+k)\cdot(c\cdot p+k-1)\cdot\quad\cdots\cdots\quad\cdot(c\cdot p+2)\cdot(c\cdot p+1)}{k\quad\cdot\quad(k-1)\quad\cdot\quad\cdots\cdots\quad\cdot\quad 2\quad\cdot\quad 1}\equiv 1\mod p$$

—pues cada factor del numerador es congruente módulo p con el factor del denominador que está en la misma posición relativa—. Puesto que k pertenece al conjunto completo de exponentes, J, (por ser $0<k\leq n-2$), podemos aplicar el teorema 3.5.1, apartado (a), y obtenemos

$$\emptyset\neq Z_{n,\{k\}}\big(\overline{\mathbb{F}}_p\big)\subset Y_n\big(\overline{\mathbb{F}}_p\big),$$

en contra de que el par (n,k) era eficaz.

Asumimos, pues, que p sí divide a n, y por tanto podemos escribir $n=h\cdot p^r$ con $r>0$ y $\text{m.c.d.}\big(h,p\big)=1$. Suponemos ahora que h es estrictamente mayor que p, y procedemos como antes: Al ser $h=a\cdot p+k$ con $0<k<p<h$, —en particular, $0<kp^r<\text{h}p^r$— resulta

$$\binom{h}{k}=\frac{(a\cdot p+k)\cdot(a\cdot p+k-1)\cdot\quad\cdots\cdots\quad\cdot(a\cdot p+2)\cdot(a\cdot p+1)}{k\quad\cdot\quad(k-1)\quad\cdot\quad\cdots\cdots\quad\cdot\quad 2\quad\cdot\quad 1}\equiv 1\mod p$$

y, por tanto, también $\binom{\text{h}p^r}{kp^r}\equiv 1 \mod p$ —en aplicación de 3.4.1—; en consecuencia, se tiene

$$\emptyset\neq Z_{\text{h}p^r,\{kp^r\}}\big(\overline{\mathbb{F}}_p\big)\subset Y_n\big(\overline{\mathbb{F}}_p\big),$$

lo cual de nuevo contradice que el par (n,k) sea eficaz. Queda así probado que en todo par eficaz (n,p) en el que sea $p<n$ ha de cumplirse: $n=h\cdot p^r$ con $r>0$ y $h<p$, según afirman los apartados (i) y (ii).

Para probar el apartado (iii) basta aplicar el teorema 4.2.1 de resolución por condensación, según el cual, si fuera $Y_h\big(\overline{\mathbb{F}}_p\big)\neq\emptyset$ entonces también habría de ser $Y_{\text{h}p^r}\big(\overline{\mathbb{F}}_p\big)\neq\emptyset$, en contra de la hipótesis. □

Dados n y p, diremos que p es el *primo dominante de n* si es $n=hp^r$ con $h<p$. Esto es, si p es un factor primo de n que supera estrictamente al producto h de todos los factores diferentes de p presentes en la factorización prima de n. Del teorema anterior extraemos una conclusión inmediata:

Corolario 4.3.2. *Para que el par (n,p), con $p\leq n$, pueda ser un par eficaz, es condición necesaria que p sea el primo dominante de n.* □

Observación 4.3.3. **(1.)** Si es $p < n$ y p no divide a n, o bien si lo divide pero no es dominante, entonces (n, p) no puede ser un par eficaz. Esto reduce drásticamente el número de pares a tomar en consideración.

(2.) Hay miríadas de números n que *carecen* de primo dominante. El primo dominante, si lo hay, debe coincidir con el mayor de los factores primos de n (siendo, por tanto, único), pero no basta con que supere *uno a uno* a los demás factores primos: se pide que supere al *producto* de todos ellos, multiplicidades incluidas. Cualquier primo p que fijemos dominará solamente en los números de la forma $n = hp^r$ con $h \in \{1, 2, \ldots, p-1\}$; sin embargo, existen infinitos valores de h mayores que p —producto de potencias tan altas como se quiera de primos *pequeños*— de forma que $n = hp^r$ no es dominado, ni por p, ni por ningún otro primo . Así por ejemplo, salvo que (a, b, c) sea una de las seis configuraciones para las cuales resulta $2^a \cdot 3^b \cdot 5^c \leq 6$, el número $n = (2^a \cdot 3^b \cdot 5^c) \cdot 7^r$ carece de primo dominante sean cuales sean los exponentes a, b, c, r.

(3.) Existen números que poseen primo dominante, pero con los cuales el primo dominante resulta no ser eficaz. Por ejemplo, los números de la forma $n = 4 \cdot 5^r$, que tienen al 5 como primo dominante, encuentran que es $Y_4\big(\overline{\mathbb{F}}_5\big) \neq \emptyset$ (ver corolario 4.2.2) y por tanto, en aplicación del teorema 4.2.1, $Y_{4 \cdot 5^r}\big(\overline{\mathbb{F}}_5\big) \neq \emptyset$, de modo que ningún par de la forma $(4 \cdot 5^r, 5)$ es eficaz. Podríamos decir que el par *ineficaz básico* $(4, 5)$ nos deja toda una estela de pares ineficaces.

(4.) El teorema 3.5.1 caracteriza en términos aritméticos cuándo $Z_{h,\{i\}}\big(\overline{\mathbb{F}}_p\big)$ e incluso $Z_{h,\{i,j\}}\big(\overline{\mathbb{F}}_p\big)$ son diferentes de vacío. Puesto que estos conjuntos de puntos son subconjuntos del correspondiente $Y_h\big(\overline{\mathbb{F}}_p\big)$, cuando aquello ocurra, se tendrá $Y_h\big(\overline{\mathbb{F}}_p\big) \neq \emptyset$, y sabremos que tanto (h, p) como todos los demás pares de su estela son ineficaces.

(5.) Saber si un número n posee o no primo dominante y, en su caso, encontrarlo, es sencillo (supuesta la capacidad de factorizar n, claro está): basta para ello separar toda la potencia de su máximo factor primo p, y mirar si el correspondiente *cofactor* h es superado o no por p.

En caso afirmativo, para saber si p es eficaz con n se necesita determinar si el conjunto $Y_n\big(\overline{\mathbb{F}}_p\big)$ es o no vacío, problema que, gracias al teorema de condensación, queda reducido a averiguar si lo es $Y_h\big(\overline{\mathbb{F}}_p\big)$. La realidad es que, aun tras esta simplificación, la respuesta queda en la mayoría de los casos fuera de nuestro alcance.

En esta Memoria, hasta el momento solo para $h = 1,\ 2,\ 3$ y 4 hemos obtenido el listado específico de todos los primos p tal que el par (h, p) es eficaz; de inmediato lo obtendremos para $h = 5$ y, en el próximo capítulo, también para $h = 6$. Por ahora, para mayores valores de h, a la pregunta de si el par si (h, p) es eficaz solamente estamos en condiciones dar

respuesta (negativa, naturalmente) en el eventual caso de que $Y_h\big(\overline{\mathbb{F}}_p\big)$ contenga puntos con solo una o dos componentes no nulas, caso comentado en el apartado anterior; en cambio, si $Y_h\big(\overline{\mathbb{F}}_p\big)$ *no* contiene tal tipo de puntos, faltará todavía por averiguar si es que posee algún punto con 3 o más componentes distintas de cero (respuesta negativa a la pregunta), o si tampoco tiene puntos de esta clase y es, por tanto, vacío (respuesta afirmativa).

En la literatura [CLO-2] se ha comunicado el cómputo de todos los primos ineficaces para $h=7$, realizado mediante el empleo de muy sofisticados métodos y medios informáticos.

Comentario 4.3.4. De acuerdo con las anteriores consideraciones, podemos encuadrar a cada número natural n en uno de los siguientes tipos (identificados por sus acrónimos):

DEf (Números con **D**ominante **Ef**icaz): Aquellos cuyo primo dominante p se ha comprobado que es eficaz con n, esto es, que satisface $Y_n\big(\overline{\mathbb{F}}_p\big)=\emptyset$.

DIn (Números con **D**ominante **In**eficaz): Aquellos de cuyo primo dominante p se tiene constancia de que verifica $Y_n\big(\overline{\mathbb{F}}_p\big)\neq\emptyset$.

SPD (Números **S**in **P**rimo **D**ominante): Los que carecen de primo dominante.

DSC (**D**ominante **S**in **C**ontrastar): Números poseedores de primo dominante p para los que se desconoce si $Y_n\big(\overline{\mathbb{F}}_p\big)$ contiene algún punto o es, por el contrario, vacío.

Así, por el momento podemos afirmar:

- Son del tipo DEf todos los números de la forma
  - p^r, para todo primo p. [Corolario 3.3.2]
  - $2p^r$, para todo primo p. [Corolario 3.5.4]
  - $3p^r$, para todo primo $p\neq 2$. [Corolario 3.5.6]
  - $4p^r$, para todo primo $p\neq 3, 5, 7$. [Corolario 4.2.2]
- Son del tipo DIn todos los números de la forma $4\cdot 5^r$, $4\cdot 7^r$. [Corolario 4.2.2] En particular: 20, 28, 100 y 196.
- Entre los 100 primeros números, son del tipo SPD los dieciséis números siguientes:

  12, 24, 30, 36, 40, 45, 48, 56, 60, 63, 70, 72, 80, 84, 90, 96

  y hay otros veintitrés número del tipo SPD comprendidos entre 101 y 200, que son:

  105, 108, 112, 120, 126, 132, 135, 140, 144, 150, 154, 160, 165,
  168, 175, 176, 180, 182, 189, 192, 195, 198, 200

- El número $296 = 8 \cdot 37$ y todos los demás números de la forma $n = 8 \cdot 37^r$ se encuentran inicialmente en el tipo DSC puesto que desconocemos si su primo dominante, $p = 37$, es o no eficaz con ellos, es decir, si es o no vacío el conjunto $Y_8\big(\overline{\mathbb{F}}_{37}\big)$. Sabemos que el sistema homogéneo en las seis incógnitas $b_2, \cdots, b_7$ que define al esquema Y_8 no posee sobre $\overline{\mathbb{F}}_{37}$ ninguna solución con solo una o dos componentes no nulas, pues sometiendo cada una de las 15 posibles combinaciones $\{i, j\} \subset J = \{1, 2, \ldots, 6\}$ al análisis indicado en el teorema 3.5.1 se concluye que en todos los casos es $Z_{8,\{i,j\}}\big(\overline{\mathbb{F}}_{37}\big) = \emptyset$, pero ello no implica que no puedan existir soluciones con tres, cuatro, cinco o seis componentes no nulas.

La pertenencia a la categoría DSC reviste carácter *provisional*: cualquier avance en el conocimiento de los conjuntos de puntos $Y_n\big(\overline{\mathbb{F}}_p\big)$ puede desplazar series enteras de números desde DSC hasta DEf o DIn, en donde se instalan con carácter definitivo. Así por ejemplo: por efecto del teorema 4.4.3, los números de la forma $n = 5 \cdot 7^r$ y $n = 5 \cdot 13^r$, inicialmente en situación análoga a la referida para $n = 8 \cdot 37^r$, pasarán inmediatamente a ubicarse en el tipo DIn y el tipo DEf, respectivamente; de igual modo, por efecto del trabajo [CLO-2], los números $n = 7 \cdot 19^r$ pasan de DSC a DIn, y los números $n = 7 \cdot 127^r$, de DSC a DEf. El número más pequeño cuyo primo dominante no nos consta que haya sido contrastado es $187 = 11 \cdot 17$.

Observación 4.3.5. Para los números n de tipo DEf tenemos garantizada la respuesta afirmativa al problema de Casas-Alvero de grado n (véase el inicio de esta sección). Para los números n de tipo SPD o DIn se conoce la imposibilidad de que exista un primo estrictamente menor que sea eficaz con n, pero nada impide que exista un primo $p > n$ que sí sea eficaz con él. En ese caso, el par (n, p) sería un par eficaz básico que da inicio a una estela de pares eficaces; dicho de otro modo, n estaría ocupando el papel que h desempeña en el Principio de Expansión, en virtud del cual todos los números de la forma np^r (para ese n y ese p particulares) serían del tipo DEf.

4.4. Niveles de ineficacia

Los primos que no son eficaces con un número n dado se distribuyen en estratos o niveles, según cuál sea el mínimo número de componentes no nulas de un punto cuando se recorre el conjunto $Y_n\big(\overline{\mathbb{F}}_p\big)$, para el primo p de que se trate. Precisemos esto:

Definición 4.4.1. Dado un primo p ineficaz con el número n, esto es, tal que $Y_n\big(\overline{\mathbb{F}}_p\big) \neq \emptyset$, diremos que p es *ineficaz de nivel* k con n si el sistema que define al esquema Y_n,

$H^{[1]}=H^{[2]}=\ldots=H^{[n-2]}=0$, posee sobre $\overline{\mathbb{F}}_p$ alguna solución con exactamente k componentes distintas de cero, pero no posee ninguna solución con un número de componentes no nulas inferior a k. En otras palabras, si para todo conjunto de exponentes I de cardinal menor que k contenido en el conjunto completo de exponentes $J=\{1,2,\ldots,n-2\}$, es $Z_{n,I}\big(\overline{\mathbb{F}}_p\big)=\emptyset$, pero sin embargo se tiene algún conjunto $\{i_1,\ldots,i_k\}\subset J$ —de cardinal k— tal que $Z_{n,\{i_1,\ldots,i_k\}}\big(\overline{\mathbb{F}}_p\big)\neq\emptyset$. El nivel de ineficacia con n del primo p expresa de cuál de las $n-2$ maneras posibles, excluyentes entre sí, se realiza el hecho de que el sistema anterior posea sobre el cuerpo $\overline{\mathbb{F}}_p$ soluciones no nulas:

Nivel 1: Existe alguna solución con una única componente distinta de cero; es decir, para algún $i\in J=\{1,2,\ldots,n-2\}$ ocurre que es $Z_{n,\{i\}}\big(\overline{\mathbb{F}}_p\big)\neq\emptyset$.

Nivel 2 : No se tienen sobre $\overline{\mathbb{F}}_p$ soluciones con una única componente no nula, pero sí con dos. Es decir, existe $\{i,j\}\subset J=\{1,2,\ldots,n-2\}$ tal que $Z_{n,\{i,j\}}\big(\overline{\mathbb{F}}_p\big)\neq\emptyset$, pero $Z_{n,\{k\}}\big(\overline{\mathbb{F}}_p\big)=\emptyset$ para todo $k\in J$.

... ...

Nivel n−2 : Todas las soluciones no triviales que el sistema posee sobre $\overline{\mathbb{F}}_p$ tienen todas sus componentes diferentes de cero. Es decir, aunque es $Z_{n,J}\big(\overline{\mathbb{F}}_p\big)=Y_n\big(\overline{\mathbb{F}}_p\big)\neq\emptyset$, para todo I subconjunto propio de J se tiene $Z_{n,I}\big(\overline{\mathbb{F}}_p\big)=\emptyset$.

Observación 4.4.2. Los primos ineficaces de niveles 1 y 2 se localizan aplicando el teorema 3.5.1. En concreto,

- p es ineficaz de nivel 1 con n si existe $i\in J$ tal que $\binom{n}{i}\equiv 1 \mod n$.
- p es ineficaz de nivel 2 con n si no lo es de nivel 1 y además existe $\{i,j\}\subset J$ tal que el número
$$\Delta_{i,j}=a^{\,\rho}\,(b-c)^{\rho}(b-ac)^{\sigma}-(-1)^{\sigma}(a-1)^{\rho+\sigma}(b-1)^{\rho}$$
—donde $a=\binom{n}{i}$, $b=\binom{n}{j}$, $c=\binom{n-i}{n-j}$ y $\rho=\frac{n-j}{d}$, $\sigma=\frac{j-i}{d}$, con $d=\text{m.c.d.}(n-j,j-i)$— es múltiplo de p.

Cabe señalar que en la demostración del teorema 4.3.1 se probó, específicamente, el resultado siguiente: "Si p es un primo menor que n, y p no divide a n o bien lo divide pero no es dominante, entonces p es ineficaz de nivel 1 con n".

Nuestro próximo objetivo será determinar qué primos son eficaces con $h=5$ y cuáles no; para ello hemos de estudiar qué soluciones posee sobre $\overline{\mathbb{F}}_p$ el sistema $H^{[1]}=H^{[2]}=H^{[3]}=0$ que define al esquema Y_5. Esta tarea es todavía abordable de forma directa con los medios

de que disponemos, aunque ya requiere el uso de algunas tácticas y una moderada capacidad de cálculo aritmético.

Teorema 4.4.3. *El conjunto de puntos* $Y_5\big(\overline{\mathbb{F}}_p\big)$ *es distinto de vacío si y solo si el primo* p *es uno de los siguientes:* 2, 3, 7, 11, 131, 193, 599, 3541 *y* 8009.

Demostración. Recordemos que el esquema Y_5 se construye al imponer sobre el polinomio

$$P_5(X) = X^5 + \tbinom{5}{2} b_2\, X^3 + \tbinom{5}{3} b_3\, X^2 + \tbinom{5}{4} b_4\, X$$

la triple condición de que se anulen las resultantes

$$H^{[1]} = \mathrm{Res}\big(P_5(X), P_5{}^{[1]}(X)\big)\,, \quad H^{[2]} = \mathrm{Res}\big(P_5(X), P_5{}^{[2]}(X)\big)\,, \quad H^{[3]} = \mathrm{Res}\big(P_5(X), P_5{}^{[3]}(X)\big).$$

Sabemos que $H^{[1]}$, $H^{[2]}$ y $H^{[3]}$ son polinomios homogéneos pesados de grados 20, 15 y 10, respectivamente, del anillo graduado $\mathbb{Z}\big[b_2, b_3, b_4\big]$ (donde cada b_i tiene peso i), y que cada punto $[(\beta_2, \beta_3, \beta_4)] \in Y_5\big(\overline{\mathbb{F}}_p\big)$ corresponde a una familia de ternas $\big\{(\lambda^2\beta_2, \lambda^3\beta_3, \lambda^4\beta_4)\big\}_{\lambda \in \overline{\mathbb{F}}_p\text{-}\{0\}}$ que son soluciones no triviales del sistema $H^{[1]} = H^{[2]} = H^{[3]} = 0$.

Los primos ineficaces con $n = 5$ de niveles 1 y 2 —esto es, tales que $Y_5\big(\overline{\mathbb{F}}_p\big)$ posee algún punto con solo una o dos componentes distintas de cero— los encontramos del modo que se indica en la observación 4.4.2 :

- p es ineficaz con 5 de nivel 1 si y solo si

  $$\tbinom{5}{1} \equiv 1 \mod p, \quad \text{o bien} \quad \tbinom{5}{2} \equiv 1 \mod p, \quad \text{o bien} \quad \tbinom{5}{3} \equiv 1 \mod p,$$

  es decir, si y solo si es $4 \equiv 0 \mod p$ o $9 \equiv 0 \mod p$. Esto nos da: $p = 2$ o 3.

- p es ineficaz con 5 de nivel 2 si es $p \neq 2, 3$, y además es múltiplo de p alguno de los tres números siguientes (obviamos la transcripción de los cálculos):

  $$\Delta_{1,2} = -2^4 \cdot 3^3 \cdot 193; \qquad \Delta_{1,3} = -2^8; \qquad \Delta_{2,3} = -11 \cdot 3541.$$

  Esto proporciona los primos $p = 11$, 193, 3541.

Falta solo encontrar los primos ineficaces con 5 de nivel 3. Reproducimos a continuación el sistema $H^{[1]} = H^{[2]} = H^{[3]} = 0$, adoptando por conveniencia la letras a, b y c para significar las incógnitas b_2, b_3 y b_4, respectivamente:

$$\begin{aligned} 16c^2 \cdot (400\,a^4\,c - 200\,a^3\,b^2 - 160\,a^2\,c^2 + 360\,a\,b^2\,c - 135\,b^4 + 16\,c^3) &= 0 \\ b \cdot (2205\,a^4\,c - 980\,a^3\,b^2 - 1050\,a^2\,c^2 + 2160\,a\,b^2\,c - 729\,b^4 + 125\,c^3) &= 0 \\ a \cdot (81\,a^4 - 90\,a^2\,c + 100\,a\,b^2 + 25\,c^2) &= 0. \end{aligned} \tag{4.12}$$

Si (α, β, γ) con $\alpha \neq 0$ es solución de este sistema, entonces también lo es $(\alpha\lambda^2, \beta\lambda^3, \gamma\,\lambda^4)$, en particular, para λ cumpliendo $\alpha \cdot \lambda^2 = 1$. Nos interesa caracterizar el hecho de que (4.12) posea alguna solución con sus tres componentes no nulas, la primera de las cuales podemos ya suponer que es igual a 1.

- La terna $(1,\beta,\gamma)$ con $\beta,\gamma\neq 0$ es solución del sistema (4.12) si y solo si el par (β,γ) lo es del siguiente sistema, más simple —se ha prescindido del primer factor en cada uno de los miembros izquierdos— y ya deshomogeneizado —la incógnita a ha sido sustituida por el valor 1:

$$\begin{aligned} 400\,c-200\,b^2-160\,c^2+360\,b^2\,c-135\,b^4+16\,c^3 &= 0\\ 2205\,c-980\,b^2-1050\,c^2+2160\,b^2\,c-729\,b^4+125\,c^3 &= 0\\ 81-90\,c+100\,b^2+25\,c^2 &= 0. \end{aligned} \tag{4.13}$$

- Lo anterior sucede si y solo si el par (β^2,γ) tiene sus dos componentes distintas de cero y es solución del siguiente sistema en las incógnitas m (que sustituye a b^2, aprovechando que b siempre lleva exponente par) y c:

$$\begin{aligned} 400\,c-200\,m-160\,c^2+360\,m\,c-135\,m^2+16\,c^3 &= 0\\ 2205\,c-980\,m-1050\,c^2+2160\,m\,c-729\,m^2+125\,c^3 &= 0\\ 81-90\,c+100\,m+25\,c^2 &= 0. \end{aligned}$$

Puesto que la última ecuación es lineal en m, podemos despejar dicha incógnita:

$$m \;=\; \frac{-1}{100}\,(25\,c^2-90\,c+81); \tag{4.14}$$

y sustituirla en las dos ecuaciones restantes, obteniendo

$$\frac{-1}{2000}\left(16875\,c^4+26500\,c^3-99950\,c^2-250460\,c-146853\right) \;=\; 0 \tag{4.15}$$

$$\frac{-1}{10000}\left(455625\,c^4+869500\,c^3-2532650\,c^2-6362820\,c-3155031\right) \;=\; 0. \tag{4.16}$$

Estamos buscando los primos p que son ineficaces con 5 de nivel 3, por tanto, distintos de 2, 3, 11, 193, 3541 —ineficaces de niveles 1 y 2 con $n=5$— y también distintos de 5 —eficaz con $n=5$, pues es $Y_5\big(\overline{\mathbb{F}}_5\big)=\emptyset$—. Habiendo apartado los primos 2 y 5, los números 100, 2000 y 10000 (o, mejor, sus imágenes mediante la aplicación característica $\varphi:\mathbb{Z}\to\overline{\mathbb{F}}_p$) son unidades en $\overline{\mathbb{F}}_p$, luego su presencia en las igualdades anteriores no resulta problemática; de hecho, en las ecuaciones (4.15) y (4.16) pueden suprimirse sin más.

Debemos localizar aquellos primos que cumplen la siguiente condición:

sobre el cuerpo $\overline{\mathbb{F}}_p$, las dos ecuaciones (4.15) y (4.16) tienen en común una solución γ

puesto que ella identifica a los primos ineficaces con $n=5$ de nivel 3. En efecto, esta condición es necesaria para que existan $\beta,\gamma\in\overline{\mathbb{F}}_p$ tales que $(1,\beta,\gamma)$ satisface el sistema (4.12), y también es suficiente para ello: considerando el valor μ que (4.14) le asigna a m cuando c se sustituye por γ, basta tomar β como una de las soluciones que en el cuerpo $\overline{\mathbb{F}}_p$ siempre posee la ecuación $\beta^2=\mu$. (En rigor, deberíamos tener la cautela de comprobar

que tanto γ como β sean distintos del elemento $0 \in \overline{\mathbb{F}}_p$; pero si así no fuera, y dado que, en todo caso, se tendría un punto $[(1, \beta, \gamma)]$ perteneciente a $Y_5\big(\overline{\mathbb{F}}_p\big)$, seguiría siendo cierto que p es un primo ineficaz con 5 —aunque de nivel inferior a 3— y, por tanto, habría de coincidir con alguno de los hallados anteriormente.)

Hemos de considerar, pues, la resultante de los polinomios

$$16875\,c^4 + 26500\,c^3 - 99950\,c^2 - 250460\,c - 146853$$
$$455625\,c^4 + 869500\,c^3 - 2532650\,c^2 - 6362820\,c - 3155031,$$

cuyo valor es, exactamente,

$$-\,2^{32} \cdot 3^7 \cdot 5^{16} \cdot 7^3 \cdot 131 \cdot 599^2 \cdot 8009.$$

Esta resultante es nula en característica p si y solo si es $p = 7, 131, 599, 8009$ (recordemos que en este momento no disponemos de 2, ni de 3, ni de 5). Como estos primos no dividen a los coeficientes directores, $16875 = 3^3 \cdot 5^4$ y $455625 = 3^6 \cdot 5^4$, la anulación de la resultante verdaderamente equivale a que dichos polinomios compartan una raíz $\gamma \in \overline{\mathbb{F}}_p$ o, en otros términos, a que exista $\gamma \in \overline{\mathbb{F}}_p$ solución común de las ecuaciones (4.15) y (4.16), lo que era precisamente la condición expresada en el recuadro.

Se concluye que los cuatro primos citados: 7, 131, 599, y 8009, son todos los primos ineficaces de nivel 3 con $n = 5$ que existen. Hemos completado así la nómina de los primos que son ineficaces con $n = 5$—esto es, tales que $Y_5\big(\overline{\mathbb{F}}_p\big) \neq \emptyset$—; cualquier primo p que no figure en ella es, pues, eficaz con $n = 5$. □

Corolario 4.4.4. *El problema de Casas-Alvero tiene respuesta afirmativa para todos los números de la forma* $n = 5p^r$ *con* $p \neq 2,\ 3,\ 7,\ 11,\ 131,\ 193,\ 599,\ 3541,\ 8009$.

Demostración. El teorema anterior garantiza que para todo primo p distinto de los mencionados se tiene $Y_5\big(\overline{\mathbb{F}}_p\big) = \emptyset$; la lectura hacia la izquierda del teorema de condensación (4.2.1) expande este resultado y permite asegurar que es $Y_{5p^r}\big(\overline{\mathbb{F}}_p\big) = \emptyset$ para todo $r \in \mathbb{N}$. Finalmente, la proposición 3.1.4 conduce hasta el resultado enunciado en este corolario. □

Comentario 4.4.5. Todo el trabajo de cálculo tanto algebraico como aritmético que se ha precisado para localizar los primos ineficaces con $n = 5$ se ha podido ejecutar sin dificultad con el auxilio del programa informático DERIVE. Con este antecedente, resulta lógico abordar el mismo problema para el caso $n = 6$ utilizando el mismo planteamiento, y explorar hasta qué punto podemos avanzar en su resolución y qué nuevos obstáculos se interponen en el camino.

Caso:	Fijar	Incógnitas	Última Ecuación	Primos cumpliendo $Z_{6,\{i,j,k\}}(\overline{\mathbb{F}}_p) \neq \emptyset$
I: $a=0$	$b=1$	$c\ ,\ d$	grado 3 en c	47, 811, 3209, 3877, 9337, 17 250187
II: $b=0$	$a=1$	$c\ ,\ d^2$	lineal en $m=d^2$	257, 1069, 3881, 150203, 547061
III: $c=0$	$a=1$	$b\ ,\ d$	cuadrática en d	8699, 15823, 2 610767 527031
IV: $d=0$	$a=1$	$b^2\ ,\ c$	lineal en $m=b^2$	21379, 7 783207, 40 362599, 7390 044713 023799

Cuadro 4.1: Casuística en la búsqueda de primos ineficaces de nivel 3 con $n=6$.

Del mismo modo que con $n=5$, la búsqueda de los primos ineficaces con $n=6$ se realiza por niveles, en cada uno de los cuales se investiga cuáles son las condiciones necesarias y suficientes para que el sistema homogéneo pesado $H^{[1]}=H^{[2]}=H^{[3]}=H^{[4]}=0$ en las incógnitas a, b, c, d (usadas, por simplicidad, en lugar de b_2, b_3, b_4, b_5, y con pesos respectivos 2, 3, 4 y 5) posea sobre el cuerpo $\overline{\mathbb{F}}_p$ alguna solución con un determinado número de componentes distintas de cero. Y esto es lo que ocurre:

Niveles 1 y 2: En estos niveles, la complejidad de la tarea no experimenta ningún incremento —aunque sí, obviamente, su volumen—; todo se reduce a aplicar el procedimiento recogido en la observación 4.4.2.

Nivel 3: Localizar aquellos primos no surgidos en los niveles anteriores y para los cuales no sea vacío el conjunto $Z_{6,\{1,2,3\}}(\overline{\mathbb{F}}_p) \cup Z_{6,\{1,2,4\}}(\overline{\mathbb{F}}_p) \cup Z_{6,\{1,3,4\}}(\overline{\mathbb{F}}_p) \cup Z_{6,\{2,3,4\}}(\overline{\mathbb{F}}_p)$ requiere trabajar con el consabido sistema homogéneo en cuatro casos particulares, que son, naturalmente: **I:** $a=0$, **II:** $b=0$, **III:** $c=0$ y **IV:** $d=0$. Tenemos así cuatro subproblemas que, si bien son esencialmente iguales al problema de hallar los primos ineficaces de nivel 3 con $n=5$ —cuya resolución se expuso en la demostración del teorema 4.4.3—, presentan alguna complicación adicional debida al mayor grado de sus ecuaciones. Baste esbozar la pauta común a todos los casos y señalar los rasgos diferenciales (que se recogen en la tabla 4.1):

En todos los casos, tras anular una de las indeterminadas y asumiendo que las tres restantes son distintas de cero, imponemos que una de ellas (la de menor peso y, por ello, portadora de exponentes más altos) tome el valor 1. Descargamos también el factor trivial de cada resultante. Queda entonces un sistema de tres ecuaciones en dos incógnitas, y el objetivo es encontrar todas aquellas características p en las que dicho sistema pueda ser compatible. No se trata de ecuaciones lineales; si tomamos el grado total —en sentido ordinario, no pesado— de cada una de las ecuaciones del sistema, resultan las siguientes ternas (respectivamente para los casos **I** , **II** , **III** y **IV**): $(5,5,3)$, $(5,5,2)$, $(5,5,2)$ y $(4,4,2)$.

- Los casos **II** y **IV** guardan completa similitud con el problema para $n=5$ estudiado en 4.4.3: ocurre que una de las incógnitas figura siempre con exponente par, lo que permite sustituir por m a su cuadrado; tras hacerlo, la última ecuación queda lineal

en m. Es pues inmediato despejar m y sustituirlo en las dos ecuaciones anteriores.

- En el caso **III**, la última ecuación es de segundo grado en d —también lo es en b—; elegimos despejar d y sustituirlo en las dos ecuaciones previas. El proceso, que en principio ha de efectuarse dos veces, una por cada signo en la fórmula de las raíces del trinomio, puede completarse rigurosamente dentro del cuerpo $\overline{\mathbb{F}}_p$ representando las raíces mediante el uso de símbolos literales definidos por la identidad que satisfacen (así, por ejemplo, en lugar de $\sqrt{3}i$ empleamos $u \in \overline{\mathbb{F}}_p$ tal que $u^2 = -3$). Procediendo de este modo, de hecho, es superflua la repetición, puesto que se cubren simultáneamente las dos elecciones del signo.

- En el caso **I**, la más sencilla de las ecuaciones del sistema—que, como en los otros casos, es la que proviene de $H^{[3]}$— es ya de grado 3 en c, pero con la afortunada particularidad de que su primer miembro factoriza dentro del anillo $\mathbb{Z}[d][c]$ como producto de un polinomio lineal y otro cuadrático. El sistema inicial se desdobla, pues, en dos sistemas diferentes —según que dicha ecuación se supla por la que expresa la nulidad de uno u otro factor—; en cada uno de ellos, la situación que se presenta es análoga a la de uno de los ítems previos: tres ecuaciones en dos incógnitas, siendo la tercera ecuación, o bien lineal en una de sus incógnitas (como en los casos **II** y **IV**), o bien cuadrática en una de ellas (como en el caso **III**); tanto en una como en otra tesitura, la incógnita en cuestión se despeja empleando la ecuación tercera, para luego sustituirla en las dos anteriores.

En definitiva, en cada uno de los casos **I**, **II**, **III** y **IV**, las referidas operaciones han desembocado en la obtención de (al menos) un sistema de dos ecuaciones en una única incógnita, cuya compatibilidad interesa estudiar, por ser condición necesaria y suficiente para que sea compatible el sistema de partida que lo sea alguno de estos.

Fijémonos en uno cualquiera de tales sistemas: Consiste en dos ecuaciones algebraicas de grado 5 (4, en el caso **IV**), y lo que se pretende ahora es hallar aquellos valores de p tales que sobre el cuerpo $\overline{\mathbb{F}}_p$ ambas ecuaciones posean una solución común. Dado que ello equivale a que se anule la resultante de sus correspondientes polinomios, basta con calcular y factorizar en $\mathbb{Z}$ dicha resultante para obtener los primos que buscábamos (ver tabla 4.1).

Nivel 4: Si el sistema $H^{[1]} = H^{[2]} = H^{[3]} = H^{[4]} = 0$ admite sobre $\overline{\mathbb{F}}_p$ alguna solución con sus cuatro componentes no nulas, admitirá, en particular, una de la forma $(-1, \beta, \gamma, \delta)$ (elegir -1 en vez de 1 facilitará cálculos posteriores). Tendremos entonces $(\beta, \gamma, \delta) \in \overline{\mathbb{F}}_p^3$ que es solución del sistema

$$F_1(b, c, d) = F_2(b, c, d) = F_3(b, c, d) = F_4(b, c, d) = 0,$$

obtenido del anterior al prescindir del factor trivial en cada $H^{[i]}$ y hacer $a=-1$. De la última ecuación, cuadrática en b, obtenemos que se cumple $b=f_1(c,d)=\frac{1}{20}(15c-6d-14)$ o bien $b=f_2(c,d)=\frac{1}{20}(-15c-6d+14)$. Asumiendo —por ejemplo—que para (β,γ,δ) se cumpla $\beta=f_1(\gamma,\delta)$, tendremos que (γ,δ) satisface el sistema dado por

$$F_1\big(f_1(c,d),c,d\big)=F_2\big(f_1(c,d),c,d\big)=F_3\big(f_1(c,d),c,d\big)=0 \tag{4.17}$$

Cada F_i, una vez multiplicado por el entero adecuado, puede ser visto como un polinomio en la indeterminada c y coeficientes en el anillo $\mathbb{Z}[\,d\,]$. El grado en c de tales polinomios es 6, 6 y 5, respectivamente; construyendo S-polinomios adecuados podemos hallar un sistema equivalente a (4.17) de la forma

$$G_1(c,d)=G_2(c,d)=G_3(c,d)=0 \tag{4.18}$$

donde el grado en la indeterminada c de los polinomios $G_i\in\mathbb{Z}[d][c]$ sea, respectivamente, 6, 5 y 4. El hecho de que (γ,δ) sea solución de (4.18) se traduce en que γ es una raíz compartida por los tres polinomios

$$M_{1,\delta}(c)=G_1(c,\delta),\qquad M_{2,\delta}(c)=G_2(c,\delta)(c),\qquad M_{3,\delta}=G_3(c,\delta),$$

cuyos coeficientes pertenecen al anillo $\mathbb{Z}[\delta]\subset\overline{\mathbb{F}}_p$. Para que ello sea posible, es condición necesaria (aunque no suficiente) la anulación simultánea de las tres resultantes

$$Q_{1,2}(\delta)=\mathrm{Res}\big(M_{1,\delta},M_{2,\delta}\big),\ \ Q_{1,3}(\delta)=\mathrm{Res}\big(M_{1,\delta},M_{3,\delta}\big),\ \ Q_{2,3}(\delta)=\mathrm{Res}\big(M_{2,\delta},M_{3,\delta}\big)\in\mathbb{Z}[\delta],$$

es decir, es necesario que exista $\delta\in\overline{\mathbb{F}}_p$ que sea raíz común de los tres polinomios

$$Q_{1,2}(d)=\mathrm{Res}\big(M_{1,d},M_{2,d}\big),\ \ Q_{1,3}(d)=\mathrm{Res}\big(M_{1,d},M_{3,d}\big),\ \ Q_{2,3}(d)=\mathrm{Res}\big(M_{1,d},M_{3,d}\big)\in\mathbb{Z}[d],$$

siendo $M_{i,d}(c)=G_i(c,d)$, para $i=1,2,3$.

Los primos ineficaces que estamos buscando se encuentran, pues, entre los que cumplen la siguiente condición:

sobre $\overline{\mathbb{F}}_p$, los tres polinomios $Q_{1,2}(d)$, $Q_{1,3}(d)$ y $Q_{2,3}(d)$, poseen una raíz común, δ.

para lo cual conocemos una condición necesaria (aunque, como antes, no suficiente): que en característica p sean nulas las tres resultantes obtenidas al tomar dos a dos los polinomios $Q_{1,2}(d)$, $Q_{1,3}(d)$ y $Q_{2,3}(d)$. Así pues, si logramos construir y factorizar en $\mathbb{Z}$ estas tres resultantes, entonces el conjunto formado por los factores primos comunes a las tres —que es finito— contendrá todos los primos ineficaces de nivel 4 con $n=6$; cabe examinar uno a uno para tratar de confirmar o descartar que en efecto posean dicha condición, pero en todo caso es seguro que todo primo ausente de este listado (y que no haya aparecido como ineficaz de un nivel inferior) será eficaz con $n=6$.

Bien, el problema está conceptualmente resuelto: la obtención de los tres polinomios $Q_{i,j}(d)$ es perfectamente factible, y el cálculo de las tres resultantes no debería ofrecer dificultad. Sin embargo, el procedimiento es poco viable a causa de la impresionante magnitud de los datos:

- $Q_{1,3}(d)$ tiene grado 30, y coeficientes de un orden comprendido entre 10^{70} y 10^{85}
- $Q_{2,3}(d)$ tiene grado 29, y sus coeficientes de un orden comprendido entre 10^{62} y 10^{75}
- $Q_{1,2}(d)$ tiene grado 32, y el orden de sus coeficientes está entre 10^{39} y 10^{52}

(y esto, una vez descontada la presencia, en cada polinomio, de un factor constante, del orden de 10^{24}, 10^{26} y 10^{28}, respectivamente). Otras elecciones posibles—de la incógnita a despejar, de la indeterminada respecto de la cual ordenar...—ofrecen resultados similares, también con llegada a una vía muerta.

No nos obstinaremos aquí en tratar de resolver este problema siguiendo el camino iniciado. En el próximo capítulo dispondremos de un enfoque alternativo, ligado a un esquema proyectivo diferente, que nos permitirá el cálculo efectivo de *todos* los primos ineficaces con $n=6$.

La siguiente proposición no es sino la precisa recopilación de los resultados efectivamente obtenidos en 4.4.5:

Proposición 4.4.6. *Los primos ineficaces con $n=6$ de nivel estrictamente menor que 4 son los siguientes:*

Nivel 1: 2, 5, 7, 19.
Nivel 2: 11, 13, 29, 37, 61, 67, 73, 1487, 20771, 23993.
Nivel 3: 47, 257, 811, 1069, 3209, 3877, 3881, 8699, 9337, 15823, 21379, 150 203, 547 061, 7 783 207, 17 250 187, 40 362 599, 2 610 767 527 031, 7390 044 713 023 799. □

El cuadro 4.2, que cierra el capítulo, ofrece el listado completo de los valores ineficaces de primer y segundo nivel —calculados según se dijo en 4.4.2— para los números 7, 8, 9, 10, 11 y 12.

Es ilustrativo observar cómo para muy pequeños valores de n aparecen, ya en el nivel 2 de ineficacia, primos descomunales (del orden de los trillones, para $n=10$, de miles de cuatrillones, para $n=12$), y lo rápidamente que se incrementa tanto su número como la magnitud que llegan a alcanzar, a medida que crece n. Incluso en los dos primeros niveles, en los que se dispone de procedimientos sistemáticos, la selección de los primos parece responder al más puro capricho, del mismo modo en que caprichosa parece la

$n=7$	Nivel 1	2, 3, 5, 17.
	Nivel 2	11, 13, 23, 29, 31, 71, 79, 137, 149, 293, 383, 491, 599, 1373, 2393, 19583, 2 700319, 44 446559.
$n=8$	Nivel 1	3, 5, 7, 11, 23.
	Nivel 2	13, 17, 19, 29, 31, 41, 53, 59, 61, 71, 73, 109, 193, 283, 449, 457, 491, 691, 821, 1033, 1471, 1747, 1753, 4447, 6047, 70321, 72053, 96851, 100069, 102121, 151787, 3 042997, 15 083609, 133578 667529.
$n=9$	Nivel 1	2, 5, 7, 83.
	Nivel 2	11, 13, 17, 19, 29, 31, 37, 43, 59, 67, 71, 79, 89, 101, 103, 131, 137, 157, 163,379, 449, 1051, 2069, 3187, 5527, 5849, 17903, 35531, 51329, 178909, 333769, 1 268797, 1 681363, 2 012419, 85 301959, 4152 858113, 7879 713071, 10566 565489, 10628 250767, 31170 485999, 170050 183063, 684178 526303, 9 442649 977903, 18 294891 489449, 78 207719 634491.
$n=10$	Nivel 1	2, 3, 7, 11, 17, 19, 251.
	Nivel 2	13, 23, 29, 31, 37, 41, 47, 61, 73, 79, 89, 101, 139, 151, 181, 233, 277, 307, 347, 503, 563, 619, 757, 787, 991, 997, 1123, 1171, 1223, 1489, 2731, 2963, 4243, 6143, 10429, 11689, 11933, 17623, 17839, 21661, 25847, 26573, 80933, 112207, 260573, 508159, 1 176239, 1 311733, 3 361639, 6 403181, 36 737209, 40 193311, 67 623761, 114 750589, 285 641119, 1171 604881, 1659 214621, 50882 649709, 94648 571077, 115744 767907, 137495 218381, 201550 614547, 1 938388 976717, 76 317432 445741, 2819 457712 745081, 6271 487438 874901, 6 980592 529231 704811.
$n=11$	Nivel 1	2, 3, 5, 7, 41, 47, 461.
	Nivel 2	13, 19, 23, 29, 31, 37, 43, 53, 59, 67, 71, 73, 89, 103, 107, 131, 139, 163, 173, 197, 229, 233, 293, 409, 503, 557, 577, 661, 691, 877, 919, 1069, 1091, 1483, 1667, 1733, 1871, 1997, 2011, 2671, 7549, 10289 10631, 10891, 11749, 12611, 13217, 16937, 17957, 27551, 29537, 40933, 41621, 56167, 66529, 75787, 102539, 203659, 233173, 283669, 621017, 727249, 1 381349, 1 469087, 4 907921, 10 803127, 22 551359, 24 438067, 67 903357, 91 580407, 135 356759, 158 210317, 186 674237, 811 306481, 2478 679711, 2691 188471, 10017 222473, 15321 591739, 43129 826189, 107248 950013, 304706 871407, 330889 336223, 4 227618 081473, 6 028006 702481, 51 856639 765607, 53 921320 856779, 71 007003 754523, 328 768690 304689 , 657 320600 102303 , 8118 451553 135971 , 15629 057690 606267 , 138032 248224 512461 , 4 753874 264034 777383, 2 674461 312915 117968 508667, 7 498690 019676 445564 846049.
$n=12$	Nivel 1	2, 3, 5, 7, 11, 13, 19, 71, 73, 113.
	Nivel 2	17, 23, 29, 31, 41, 47, 53, 59, 61, 67, 83, 89, 101, 103, 107, 127, 149, 157, 167, 181, 191, 193, 211, 223, 229, 241, 271, 293, 307, 313, 373, 419, 421, 431, 509, 547, 599, 631, 643, 739, 821, 827, 859, 941, 1009, 1193, 1423, 1481, 1489, 1567, 3433, 3697, 3733, 3929, 5437, 5779, 6221, 6269, 6977, 9697, 9851, 13217, 14327, 17911, 18041 18947, 19219, 19993, 20063, 23593, 29983, 32341, 33589, 65831, 126961, 152563, 152639, 161773, 166471, 168281, 183877, 196279 368059, 543593, 1948987, 3079711, 4132151, 6009683, 6531709, 8 502581, 10 058941, 14 378417 , 33 821509 , 114 068599 , 129 769301 , 182 705903 , 361 846721 , 552 843719 , 1067 538217 , 2541 640561 , 5696 929037 , 7731 840929 , 19023 084637 , 71130 026657 , 271420 993729 , 336048 035693 , 538228 539671 , 729595 481339, 1 509579 945103 , 1 807000 523543 , 16 738247 804093 , 21 094483 630223, 41 581475 975341, 45 261742 243997, 81 431483 854691, 155 351610 321851, 198 478256 072773, 266 377988 861953 , 373 119427 470043 , 832 378889 412121 , 62171 145343 492699 , 172994 176982 555267, 18 534085 940905 810921 , 41 051564 324089 235071 , 221 683353 776645 181007 , 2377 225815 083191 016081 , 2430 025954 712382 144281 , 206177 862036 793816 019327 , 219117442609717502451619, 859540281549223625605679, 815428295703795827589085 21, 1393 978154 153831 038607 107121 , 3992 883635 832874 870245 154277.

Cuadro 4.2: Primos ineficaces de niveles 1 y 2 para $n=7,\ldots,12$

descomposición en factores de un entero tomado al azar. Cabe aún imaginar cómo pueden ser los listados de primos ineficaces de niveles 3 o 4, pero siendo n —tan solo— igual a 12 se antojan ya inimaginables los listados de primos ineficaces de niveles 9 o 10. Aún nos encontramos casi en el umbral, apenas iniciada la inspección de un territorio que es doblemente ilimitado —en extensión, y en profundidad— y ya se ha constatado el total desbordamiento que inmediatamente se produce.

Capítulo 5

Esquemas alternativos

El tratamiento del problema de Casas-Alvero seguido hasta el momento utilizaba como indeterminadas a los coeficientes b_i del polinomio genérico de grado n, que no son intercambiables entre sí. Por el contrario, la estrategia de expresar el polinomio como producto de n binomios de la forma $X-x_i$, cede el protagonismo a las propias raíces del mismo, x_1, x_2, ..., x_n. Puesto que estas pueden permutarse libremente sin que el producto indicado sufra ninguna alteración, emplear a las raíces $x_1, x_2, \ldots, x_n$ como las incógnitas del sistema que plasma el problema de Casas-Alvero proporciona una simetría inicial que se rentabiliza durante la construcción del esquema proyectivo. Como ventaja adicional, la condición sobre $P_n(X)$ de compartir una raíz con su primera derivada —la más incómoda de las ecuaciones en el esquema Y_n— encuentra ahora su expresión más simple y conveniente, pues supone tan sólo la igualdad entre dos de las raíces del polinomio.

5.1. El esquema de raíces

En primera instancia, podemos escribir:

Conjetura de Casas-Alvero. *Si el polinomio*

$$P_n(X)=(X-x_1)\cdot(X-x_2)\cdot\ \cdots\ \cdot(X-x_n),\quad \textit{con } (x_1,x_2,\ldots,x_n)\in\mathbb{C}^n \tag{5.1}$$

comparte una raíz con cada uno de los polinomios $P_n'(X)$, $P_n''(X)$, ..., $P_n^{(n-1)}(X)$, *entonces se verifica:* $x_1 = x_2 = \ldots = x_n$.

De existir algún polinomio que sirva de contraejemplo a esta conjetura, admitiría la reordenación de sus factores y, por tanto, cualquier ordenación particular de sus raíces, $(x_{i_1}, x_{i_2}, \ldots, x_{i_n}) \in \mathbb{C}^n$, figuraría como manifestación del contraejemplo en cuestión; en consecuencia, para su rastreo podemos —sin pérdida de generalidad— concretar el objeto

de la búsqueda, estableciendo de antemano en qué orden esperamos encontrar dispuestas a las raíces.

Por otra parte, ya la proposición 1.1.2 permitió circunscribir el problema de Casas-Alvero a aquellos polinomios que carecen de término vicelíder, en cuyo caso, tal como se observó en su momento, la $(n-1)$-ésima condición sobre $P_n(X)$ significa exactamente que es nulo su término independiente o, equivalentemente, que el cero es una de las raíces de $P_n(X)$. En esa situación restringida nos mantendremos en lo sucesivo.

Cuando se desarrolla el polinomio indicado en (5.1), queda :

$$P_n(X) = X^n + (-1)\, s_1\, X^{n-1} + (-1)^2\, s_2\, X^{n-2} + \cdots + (-1)^i\, s_i\, X^{n-i} + \cdots + (-1)^n\, s_n \qquad (5.2)$$

donde cada s_i es la llamada *función simétrica elemental* de orden i:

$$s_1 = \sum_{i=1}^{n} x_i, \quad s_2 = \sum_{i<j} x_i\, x_j, \quad s_3 = \sum_{i<j<k} x_i\, x_j\, x_k, \qquad \ldots \quad , \quad s_n = x_1\, x_2 \cdots x_n \qquad (5.3)$$

y, por tanto, establecer que el término vicelíder tenga coeficiente nulo supone asumir:

(1) que s_1 es nulo, esto es, se verifica $\quad x_1 + x_2 + \cdots + x_n = 0$.

(2) que s_n es nulo—amortizando así la condición sobre $P_n^{(n-1)}(X)$—, de modo que alguna de las raíces es igual a cero. Convenimos en fijar esta raíz nula en la primera posición, haciendo que sea $x_1 = 0$.

Abordamos ahora la caracterización de la condición relativa a $P_n'(X)$. La resultante tiene un comportamiento multiplicativo, y es particularmente sencilla cuando uno de los polinomios es de grado 1 (pues se cumple: $\mathrm{Res}\big(P(X), X-\alpha\big) = (-1)^n P(\alpha)$, siendo n el grado de $P(X)$). Puesto que es

$$P_n'(X) = \Big(\prod_{i=1}^{n} (X - x_i)\Big)' = \sum_{k=1}^{n} \Big(\prod_{j\neq k} (X - x_j)\Big)$$

se tiene:

$$\mathrm{Res}\big(P_n(X), P_n'(X)\big) = \mathrm{Res}\Big(\prod_{i=1}^{n} (X - x_i)\,,\, \sum_{k=1}^{n} \Big(\prod_{j\neq k} (X - x_j)\Big)\Big) = \prod_{i=1}^{n} \Big[\sum_{k=1}^{n} \Big(\prod_{j\neq k} (x_i - x_j)\Big)\Big].$$

Todos los sumandos contenidos en el corchete llevan un factor igual a $x_i - x_i$, a excepción, justamente, de aquel en que k toma el valor coincidente con i, así que queda, simplemente,

$$\mathrm{Res}\big(P_n(X), P_n'(X)\big) = \prod_{i=1}^{n} \Big[\prod_{j\neq i} (x_i - x_j)\Big] = \prod_{i<j} \Big[-(x_i - x_j)^2\Big]$$

Ha quedado patente el hecho (bien conocido, y ya mencionado al inicio del capítulo) de que $P_n(X)$ comparte una raíz con su derivada $P_n'(X)$ —o equivalentemente, es nula la

resultante de ambos— si y solo si dos de las raíces de $P_n(X)$ son iguales entre sí. Aplicado al polinomio en (5.1), que por hipótesis verifica dicha propiedad, si elegimos ubicar en la segunda posición, denominándola x_2, a una raíz del polinomio que sea idéntica a otra de las raíces x_i, entonces necesariamente habrá de cumplirse una de estas dos alternativas: o bien x_2 coincide precisamente con x_1 (y por tanto es, como ella, nula), o bien esto no sucede, y entonces coincide con una tercera raíz que no es nula y a la que podemos identificar como x_3. El enunciado de la conjetura adopta entonces la siguiente forma:

Conjetura de Casas-Alvero. *Si el polinomio* $P_n(X)=(X-x_1)(X-x_2)\ \cdots\ (X-x_n)$, *con* $x_1, x_2, \ldots, x_n \in \mathbb{C}$, *satisface las condiciones:*

(1) $x_1 + x_2 + \cdots + x_n = 0$, *y además* $x_1 = 0$.

(2) *Es* $x_2 = 0$, *o bien es* $x_2 = x_3 \neq 0$.

(3) *Para cada* $i = 2, \ldots, n-2$, $P_n(X)$ *comparte una raíz con su derivada* i*-ésima,* $P_n^{(i)}(X)$, *entonces se verifica:* $x_1 = x_2 = \ldots = x_n = 0$.

Escribamos el polinomio anterior bajo la forma $P_n(X) = X^n + a_2\, X^{n-2} + \ldots + a_{n-1}\, X$. Sabemos que $P_n(X)$ compartirá una raíz en $\mathbb{C}$ con su derivada ordinaria i-ésima si y solo si la comparte con la derivada de Hasse del mismo orden,

$$P_n^{<i>}(X) = \frac{1}{i!}\ P_n^{(i)}(X) = \\ = \tbinom{n}{i}\, X^{n-i} + \tbinom{n-2}{i} a_2\, X^{n-2-i} + \ldots + \tbinom{n-k}{i} a_k\, X^{n-k-i} + \ldots + \tbinom{i}{i} a_{n-i},$$

esto es, si se anula la resultante

$$G^{<i>} := \mathrm{Res}\big(P_n\,,\, P_n^{<i>}\big) \in \mathbb{Z}[a_2, \ldots, a_{n-1}]. \tag{5.4}$$

A la vista de (5.2) y (5.3) es claro que las sustituciones

$$a_k := (-1)^k\, s_k = (-1)^k \cdot \sum_{i_1 < i_2 < \ldots < i_k} x_{i_1}\, x_{i_2} \ldots x_{i_k}, \quad \text{para} \quad k = 2, \ldots n-1, \tag{5.5}$$

reexpresan el polinomio $P_n(X)$ en función de sus raíces, mientras que efectuadas en cada $G^{<i>}$ expresan la resultante entre $P_n(X)$ y su i-ésima derivada de Hasse mediante un polinomio $K^{<i>}$ perteneciente a $\mathbb{Z}[x_1, \ldots, x_n]$. Cuando este anillo se gradúa en el modo usual —esto es, dando peso igual a 1 a cada indeterminada x_i— cada a_k es un polinomio homogéneo de grado k y, en consecuencia, cada resultante $K^{<i>}$ es homogénea de grado $n(n-i)$, puesto que ese es el grado del polinomio homogéneo pesado $G^{<i>}$ en el anillo $\mathbb{Z}[a_2, \ldots, a_{n-1}]$ cuando precisamente se le atribuye peso k a cada indeterminada a_k.

En conclusión, empleando los polinomios $K^{<i>}$ que acabamos de introducir, el enunciado de la conjetura puede reformularse como sigue:

Conjetura de Casas-Alvero. *Si* $(x_2, x_3, \ldots, x_n) \in \mathbb{C}^{n\text{-}1}$ *satisface las condiciones:*

(1) $x_2 + x_3 + \cdots + x_n = 0$.

(2) Es $x_2\,(x_2 - x_3) = 0$.

(3) Es $K^{<2>} = K^{<3>} = \cdots = K^{<n\text{-}2>} = 0$ *(según definiciones previas),*

entonces necesariamente se verifica: $x_2 = x_3 = \ldots = x_n = 0$.

El esquema proyectivo que denotaremos R_n y que definimos mediante las $n-1$ ecuaciones homogéneas en las $n-1$ incógnitas $x_2, \ldots, x_n$:

$$x_2 + x_3 + \cdots + x_n \;=\; x_2\,(x_2 - x_3) \;=\; K^{<2>} = K^{<3>} = \;\cdots\; = K^{<n\text{-}2>} = 0,$$

proporciona una traducción inmediata del enunciado anterior:

Proposición 5.1.1. *La conjetura de Casas-Alvero de grado n es verdadera si y solo si es* $R_n(\mathbb{C}) = \emptyset$. □

En el manejo práctico de este esquema, aparte de la obvia eliminación de una variable gracias a la primera ecuación, encontraremos tres aspectos muy ventajosos:

- La segunda ecuación divide en realidad el problema en dos *casos* más sencillos.
- Las ecuaciones $K^{<i>} = 0$ han servido para demostrar que en efecto se tiene un esquema proyectivo, pero no necesitaremos resolverlas. Lo que ellas expresan puede reducirse a un juego combinatorio con un número finito de variaciones.
- Precisamente por saber que todas las ecuaciones son homogéneas, podemos fijar a 1 el valor de alguna componente no nula durante el rastreo de eventuales soluciones no triviales del sistema.

Estos aspectos, que aquí han sido apenas apuntados, podrán apreciarse más adelante con ocasión del empleo efectivo del esquema R_n para diversos valores de n.

5.2. El esquema de coeficientes ordinarios

Como mero puente para la construcción del esquema de raíces, en la sección anterior habíamos expresado el polinomio $P_n(X)$ de nuestro interés bajo la forma que suele considerarse usual, y que nosotros llamaremos *ordinaria*:

$$P_n(X) = X^n + a_2\,X^{n\text{-}2} + a_3\,X^{n\text{-}3} + \ldots + a_{n\text{-}1}\,X. \tag{5.6}$$

En efecto, bastó efectuar en cada polinomio $G^{<i>} = \mathrm{Res}\big(P_n\,,\,P_n{}^{<i>}\big)$ las sustituciones (5.5) para obtener los polinomios $K^{<i>} \in \mathbb{Z}[x_2,\ldots,x_n]$ empleados en la definición de R_n. En esta ocasión obviaremos dichas sustituciones.

Llamaremos *esquema de coeficientes ordinarios*, y denotaremos por X_n, al esquema proyectivo en las $n-2$ variables $a_2,\ldots,a_{n\text{-}1}$ definido por los polinomios homogéneos $G^{<1>}$, $G^{<2>},\ldots,G^{<n\text{-}2>}$. Mediante argumentos idénticos a los que conducían a la proposición 3.1.2(a), se obtiene esta vez:

Proposición 5.2.1. *La conjetura de Casas-Alvero de grado n es verdadera si y solo si es $X_n(\mathbb{C}) = \emptyset$.* □

Estos dos nuevos esquemas, X_n y R_n, suponen, en relación con la conjetura de Casas-Alvero de grado n, una alternativa al esquema Y_n utilizado en capítulos anteriores — y al que, a partir de ahora, llamaremos *esquema de coeficientes presentados*—. Cada uno de ellos caracteriza la validez de dicha conjetura mediante el hecho de no poseer ningún punto sobre el cuerpo $\mathbb{C}$. Por otra parte, también a cada uno de ellos le es aplicable la proposición 3.0.3, de modo que el hallazgo de un primo p para el que se tenga $X_n\big(\overline{\mathbb{F}}_p\big) = \emptyset$ o $R_n\big(\overline{\mathbb{F}}_p\big) = \emptyset$ garantiza que es, respectivamente, $X_n(\mathbb{C}) = \emptyset$ o $R_n(\mathbb{C}) = \emptyset$, y por tanto demuestra la conjetura para el grado n.

Por dicha razón, y en analogía con el concepto de par eficaz (n,p) definido en la sección 4.3 para el esquema Y_n, diremos que el par (n,p) es *X_n-eficaz* o que es *R_n-eficaz* si se verifica $X_n\big(\overline{\mathbb{F}}_p\big) = \emptyset$ o $R_n\big(\overline{\mathbb{F}}_p\big) = \emptyset$, respectivamente. El siguiente resultado demuestra que los tres conceptos son en realidad equivalentes.

Teorema 5.2.2. *Dados un grado $n \geq 3$ y un primo p, se verifican las equivalencias:*

(1) $R_n\big(\overline{\mathbb{F}}_p\big) = \emptyset$ *si y solo si* $X_n\big(\overline{\mathbb{F}}_p\big) = \emptyset$.

(2) $X_n\big(\overline{\mathbb{F}}_p\big) = \emptyset$ *si y solo si* $Y_n\big(\overline{\mathbb{F}}_p\big) = \emptyset$.

Demostración. *(1)* Tomemos $\alpha_2,\ldots,\alpha_{n\text{-}1},\gamma_2,\ldots,\gamma_n \in \overline{\mathbb{F}}_p$, con $\gamma_2+\cdots+\gamma_n = 0$, tales que los coeficientes ordinarios α_i y las raíces γ_j dan lugar —en cada caso, de la forma que le es propia— a un mismo polinomio, esto es, se tiene

$$X^n + \alpha_2\,X^{n\text{-}2} + \cdots + \alpha_{n\text{-}1}\,X \;=\; X(X-\gamma_2)\,\cdots\,(X-\gamma_n).$$

En consecuencia, los valores α_i y los valores γ_j guardan entre sí la misma relación que (5.5) establecía entre las a_i y las x_j:

$$\alpha_k = (-1)^k \cdot \sum_{i_1<i_2<\ldots<i_k} \gamma_{i_1}\,\gamma_{i_2}\ldots\gamma_{i_k}, \quad \text{para} \;\; k = 2,\ldots n-1.$$

Es claro entonces que $\alpha=(\alpha_2,\ldots,\alpha_{n\text{-}1})$ cumple $G^{<i>}=0$ si y solo si $\gamma=(\gamma_2,\ldots,\gamma_n)$ cumple $K^{<i>}=0$, para todo $i=1,\ldots,n-2$. Ciertamente, la condición $K^{<1>}=0$ es más débil que la condición $x_2(x_2-x_3)$ exigida por el esquema R_n; pero ocurre que γ satisface $K^{<1>}=0$ si y solo si una adecuada reordenación de sus componentes, $\gamma^*=(\gamma_{j_1},\ldots,\gamma_{j_{n\text{-}1}})$, satisface $x_2(x_2-x_3)$, de modo que la existencia de algún $\alpha\in X_n\big(\overline{\mathbb{F}}_p\big)$ equivale en efecto a la existencia de algún $\gamma^*\in R_n\big(\overline{\mathbb{F}}_p\big)$.

(*2*) Tomemos $\alpha_2,\ldots,\alpha_{n\text{-}1},\beta_2,\ldots,\beta_{n\text{-}1}\in\overline{\mathbb{F}}_p$, y consideremos el polinomio

$$P_{n,\alpha}(X)=X^n+\alpha_2\,X^{n\text{-}2}+\cdots+\alpha_l\,X^{n\text{-}l}+\cdots+\alpha_{n\text{-}1}\,X,$$

así como el polinomio presentado

$$P_{n,\beta}(X)=X^n+\tbinom{n}{2}\beta_2\,X^{n\text{-}2}+\cdots+\tbinom{n}{l}\beta_l\,X^{n\text{-}l}+\cdots+\tbinom{n}{n\text{-}1}\beta_{n\text{-}1}\,X.$$

Los subíndices α,β expresan aquí, respectivamente, la especialización de los coeficientes a_k del polinomio $P_n(X)$ en los valores α_k, y de los coeficientes b_k del polinomio presentado llamado igualmente $P_n(X)$ —en un abuso de notación que se repite con $P_{n,\beta}(X)$ y $P_{n,\beta}(X)$— en los valores β_k. Entonces, las especializaciones de las respectivas derivada de Hasse y derivada neta están dadas, para cada $i=1,2,\ldots,n-2$, por

$$P^{<i>}_{n,\alpha}(X)=\tbinom{n}{i}\,X^{n-i}+\tbinom{n\text{-}2}{i}\alpha_2\,X^{n-i-2}+\cdots+\tbinom{n\text{-}l}{i}\alpha_l\,X^{n-l-i}+\cdots+\tbinom{i+1}{i}\alpha_{n-i+1}\,X+\alpha_{n-i}\,;\quad(5.7)$$

$$P^{[\,i\,]}_{n,\beta}(X)=\,X^{n-i}+\tbinom{n\text{-}i}{2}\beta_2\,X^{n-i-2}+\cdots+\tbinom{n\text{-}i}{l}\beta_l\,X^{n-i-l}+\cdots+\tbinom{n\text{-}i}{n\text{-}i\text{-}1}\beta_{n-i-1}\,X+\beta_{n-i}\,.\quad(5.8)$$

Si $\beta=(\beta_2,\ldots,\beta_{n\text{-}1})$ representa a un punto $[\beta]\in Y_n\big(\overline{\mathbb{F}}_p\big)$, y tomamos $\alpha=(\alpha_2,\ldots,\alpha_{n\text{-}1})$ con $\alpha_l=\binom{n}{l}\beta_l$, entonces podremos probar que α es un punto de $X_n\big(\overline{\mathbb{F}}_p\big)$. Para ello:

• En primer lugar, es obvio que para dichos α,β se tiene la igualdad $P_{n,\alpha}(X)=P_{n,\beta}(X)$.

• En segundo lugar, α verdaderamente define un punto $[\alpha]$ del correspondiente espacio proyectivo pesado. En efecto, si todas las componentes de α fueran nulas significaría que son nulos módulo p todos los factores $\binom{n}{l}$ que acompañan a los $\beta_l\neq 0$, o, en términos del capítulo 3, que para el conjunto de grados $I=\big\{\,n-l\;\mid\;\beta_l\neq 0\big\}$ se tiene $I_p=\emptyset$. Entonces, por el teorema 3.3.1 de resolución por interpretación, se tendría $Z_{n,I}\big(\overline{\mathbb{F}}_p\big)=\emptyset$, en contra de que es $[\beta]\in Z_{n,I}\big(\overline{\mathbb{F}}_p\big)$.

• En tercer lugar, aplicando en (5.7) la sustitución $\alpha_l=\binom{n}{l}\beta_l$, multiplicando en ambos miembros de en (5.8) por $\binom{n}{i}$, y teniendo en cuenta las igualdades

$$\tbinom{n-l}{i}\cdot\tbinom{n}{l}=\tbinom{n}{i}\cdot\tbinom{n-i}{l},\qquad l=2,\ldots,n-i$$

se obtiene para cada $i=1,\ldots,n-2$ la igualdad $P^{<i>}_{n,\alpha}(X)=\binom{n}{i}\,P^{[\,i\,]}_{n,\beta}(X)$.

• En cuarto y último lugar: Sabemos que la anulación de la resultante entre dos polinomios equivale a la existencia de una raíz compartida siempre que al menos uno de los dos

polinomios tenga un grado verdadero coincidente con el atribuido(véase la sección 1.3; esto es válido aun cuando uno de ellos sea el polinomio cero, de quien cualquier $\rho \in \overline{\mathbb{F}}_p$ es raíz. Así, como se dijo al demostrar el lema 3.2.1, la ecuación $H^{[i]}=0$ vinculada al esquema Y_n expresa sobre el cuerpo $\overline{\mathbb{F}}_p$ la condición de que $P_n(X)$ y $P_n{}^{[i]}(X)$ compartan una raíz. Aunque las derivadas de Hasse ya no son mónicas y por ello en característica p su verdadero grado puede ser inferior al atribuido, $P_n(X)$ queda libre de esa eventualidad; por tanto, la ecuación $G^{<i>}=0$ vinculada al esquema X_n también equivale sobre $\overline{\mathbb{F}}_p$ a que $P_n(X)$ y $P_n{}^{<i>}(X)$ compartan una raíz.

Por hipótesis, para cada $i=1,\ldots,n-2$, y puesto que β verifica la ecuación $H^{[i]}=0$,

$$\text{Existe } \rho_i \in \overline{\mathbb{F}}_p \text{ tal que } \quad P_{n,\beta}(\rho_i)=0=P^{[i]}_{n,\beta}(\rho_i).$$

De las igualdades $P_{n,\alpha}(X)=P_{n,\beta}(X)$ y $P^{<i>}_{n,\alpha}(X)=\binom{n}{i}P^{[i]}_{n,\beta}(X)$ se desprende que, entonces,

$$P_{n,\alpha}(\rho_i)=0=P^{<i>}_{n,\alpha}(\rho_i).$$

Queda así probado que α verifica todas las ecuaciones $G^{<i>}=0$, y por tanto, que en efecto el punto $[\alpha]$ pertenece a $X_n\big(\overline{\mathbb{F}}_p\big)$, como se quería demostrar.

Recíprocamente, dado $[\alpha]=[\alpha_2,\ldots,\alpha_{n\text{-}1}]\in X_n\big(\overline{\mathbb{F}}_p\big)$ mostraremos que se tiene β tal que se cumple $\binom{n}{l}\beta_l=\alpha_l$ para todo $l=2,\ldots,n-1$, y además, $[\beta]\in Y_n\big(\overline{\mathbb{F}}_p\big)$. La existencia de β no es obvia: cuando $\binom{n}{l}$ es nulo módulo p, no se hallará ningún β_l válido a menos que el correspondiente α_l sea igual a cero. Y eso es exactamente lo que sucede, como se demuestra a continuación procediendo por recurrencia sobre el índice l.

Para $l=2$, consideramos la derivada de Hasse de orden $n-2$, que está dada por

$$P^{<n\text{-}2>}_{n,\alpha}(X)=\binom{n}{n\text{-}2}X^2+\alpha_2$$

y, como sabemos, posee una raíz $\rho_{n\text{-}2}\in\overline{\mathbb{F}}_p$ compartida con $P_{n,\alpha}(X)$; se cumple, en particular,

$$-\binom{n}{n\text{-}2}\rho^2_{n\text{-}2}=\alpha_2.$$

Determinamos β_2 de la siguiente manera:

$$\beta_2=\begin{cases}\binom{n}{n\text{-}2}^{-1}\cdot\alpha_2=-\rho^2_{n\text{-}2}, & \text{si } \binom{n}{n\text{-}2}\not\equiv 0 \mod p,\\ 0, & \text{si } \binom{n}{n\text{-}2}\equiv 0 \mod p.\end{cases} \tag{5.9}$$

Por recurrencia, si β_k está construido para $k=2,\ldots,l-1$ con la propiedad $\binom{n}{k}\beta_k=\alpha_k$, consideramos la derivada de Hasse de orden $n-l$, que está dada por

$$P^{<n\text{-}l>}_{n,\alpha}(X)=\binom{n}{n\text{-}l}X^l+\binom{n\text{-}2}{n\text{-}l}\alpha_2X^{l\text{-}2}+\ldots+\binom{n\text{-}k}{n\text{-}l}\alpha_kX^{l\text{-}k}+\ldots+\binom{n\text{-}l+1}{n\text{-}l}\alpha_{l\text{-}1}X+\alpha_l.$$

Si, empleando los β_k anteriormente construidos, sustituimos en esta expresión cada α_k por $\binom{n}{k}\beta_k$, y además tenemos en cuenta las igualdades

$$\binom{n-k}{n-l}\cdot\binom{n}{k}=\binom{n}{n-l}\cdot\binom{l}{k},\qquad k=2,\ldots,l-1$$

entonces se obtiene

$$P_{n,\alpha}^{<n\text{-}l>}(X)=\binom{n}{n-l}\left[X^l+\binom{l}{2}\beta_2\,X^{l-2}+\cdots+\binom{l}{k}\beta_k\,X^{l-k}+\cdots+\binom{l}{l\text{-}1}\beta_{l\text{-}1}\,X\right]+\alpha_l$$

Por hipótesis, existe una raíz $\rho_{n\text{-}l}\in\overline{\mathbb{F}}_p$ que $P_{n,\alpha}^{<n\text{-}l>}(X)$ comparte con $P_{n,\alpha}(X)$; tenemos, pues

$$-\binom{n}{n-l}\left[\rho_{n\text{-}l}^l+\binom{l}{2}\beta_2\,\rho_{n\text{-}l}^{l\text{-}2}+\cdots+\binom{l}{k}\beta_k\,\rho_{n\text{-}l}^{l\text{-}k}+\cdots+\binom{l}{l\text{-}1}\beta_{l\text{-}1}\,\rho_{n\text{-}l}\right]=\alpha_l,\qquad(5.10)$$

así que construimos β_l de la forma siguiente:

$$\beta_l=\begin{cases}\binom{n}{n\text{-}l}^{-1}\cdot\alpha_l=-\left[\rho_{n\text{-}l}^l+\binom{l}{2}\beta_2\,\rho_{n\text{-}l}^{l\text{-}2}+\;\cdots\;+\binom{l}{l\text{-}1}\beta_{l\text{-}1}\,\rho_{n\text{-}l}\right], & \text{si } \binom{n}{n\text{-}l}\not\equiv 0 \mod p\\[2ex] 0, & \text{si } \binom{n}{n\text{-}l}\equiv 0 \mod p.\end{cases}\qquad(5.11)$$

Es importante observar en (5.10) que, cuando para $l\geq 2$ se tiene $\binom{n}{n\text{-}l}\equiv 0 \mod p$, es necesariamente nula α_l, y por ello tiene sentido imponer que entonces sea $\beta_l=0$, independientemente del valor contenido en el corchete. Lógicamente, cuando $\binom{n}{l}$ no es múltiplo de p, el valor de β_l está perfectamente determinado y se obtiene por mera *división* en el cuerpo $\overline{\mathbb{F}}_p$, lo que hace en realidad innecesaria la segunda expresión en la primera línea de (5.9) y (5.11).

Una vez construido β cumpliendo la relación esperada con α es ya posible considerar el polinomio $P_{n,\beta}(X)$ que, como se ha mostrado anteriormente, es idéntico a $P_{n,\alpha}(X)$ y además satisface, para cada $i=1,\ldots,n-2$, la relación $P_{n,\alpha}^{<i>}(X)=\binom{n}{i}P_{n,\beta}^{[i]}(X)$; de este modo, las igualdades

$$P_{n,\alpha}(\rho_i)=0=P_{n,\alpha}^{<i>}(\rho_i)$$

se reescriben en la forma

$$P_{n,\beta}(\rho_i)=0=\binom{n}{i}P_{n,\beta}^{[i]}(\rho_i).$$

De aquí puede deducirse que ρ_i es, también, una raíz común a $P_{n,\beta}$ y $P_{n,\beta}^{[i]}$ —y, por tanto, β anula la resultante $H^{[i]}$— para todos aquellos i tales que $\binom{n}{i}$ sea inversible en $\overline{\mathbb{F}}_p$; evidentemente, este argumento no es aplicable para los i tales que sea $\binom{n}{i}\equiv 0 \mod p$, pero en este caso, y por construcción, se tiene $\beta_{n\text{-}i}=0$, de modo que β satisface la ecuación $b_{n\text{-}i}=0$, lo cual vimos —ya en la observación 2.1.1— que es suficiente para que se cumpla $H^{[i]}=0$. Ha quedado probado que es $[\beta]\in Y_n\big(\overline{\mathbb{F}}_p\big)$. □

Observación 5.2.3. El punto $[\beta] \in Y_n\big(\overline{\mathbb{F}}_p\big)$ que acabamos de construir a partir de un punto $[\alpha] \in X_n\big(\overline{\mathbb{F}}_p\big)$ cumple $\beta_l = 0$ en todos los casos en que es $\alpha_l = 0$, según se desprende de (5.9) y (5.11). En la construcción recíproca, de $[\alpha] \in X_n\big(\overline{\mathbb{F}}_p\big)$ a partir de $[\beta] \in Y_n\big(\overline{\mathbb{F}}_p\big)$, es aún más evidente que se cumple el enunciado análogo.

De lo anterior se deduce que, fijado un conjunto de grados $I \subset \{2, \ldots, n-1\}$, y si se define el subesquema proyectivo $X_{n,I}$ del esquema de coeficientes ordinarios X_n por analogía a como, en el capítulo 3, se había definido el subesquema proyectivo $Z_{n,I}$ del esquema Y_n, entonces, cualquiera que sea el primo p se tiene la equivalencia:

$$X_{n,I}\big(\overline{\mathbb{F}}_p\big) = \emptyset \quad \Longleftrightarrow \quad Z_{n,I}\big(\overline{\mathbb{F}}_p\big) = \emptyset.$$

De acuerdo con la proposición 3.0.3, de aquí se deduce la equivalencia

$$X_{n,I}(\mathbb{C}) = \emptyset \quad \Longleftrightarrow \quad Z_{n,I}(\mathbb{C}) = \emptyset,$$

que no puede sorprendernos por cuanto que cada una de estas dos igualdades caracteriza independientemente la respuesta afirmativa para el I-problema parcial de Casas-Alvero en grado n; el hecho destacable es que los primos que resultan eficaces para garantizar (en el sentido de la proposición 3.0.3) dicha respuesta afirmativa son los mismos ya sea $X_{n,I}$ o $Z_{n,I}$ el esquema que utilicemos, de modo que podemos consistentemente hablar de primos I-eficaces para el grado n.

5.3. Los supraesquemas X'_n y R'_n

Las ecuaciones del esquema Y_n expresan las hipótesis de la conjetura de Casas-Alvero de grado n y los puntos que dicho esquema pudiera poseer sobre $\mathbb{C}$ revelarían los eventuales contraejemplos a la misma, por construcción, siempre bajo la premisa de que $\alpha = 0$ es *la raíz que $P_n(X)$ comparte con su derivada de orden $n-1$*. Relajando esta premisa de modo que *solamente* suponga que $\alpha = 0$ es *una de las raíces de $P_n(X)$*, en el capítulo 4 se construyó un nuevo esquema proyectivo que denotamos Y'_n. Pasar de Y_n a Y'_n significó incorporar a b_1 como una indeterminada más, y añadir $H^{[n-1]} = 0$ como ecuación adicional. Una vez hecho esto, el propio Y_n se recupera como el subesquema de Y'_n obtenido al sustituir por $b_1 = 0$ a dicha ecuación $H^{[n-1]} = 0$ (más débil que aquella),

La construcción de los esquemas X_n y R_n parte de aquella misma premisa, traducida ahora en que sea $a_1 = a_n = 0$ y $x_1 = \sum x_i = 0$, respectivamente. Denotaremos por X'_n y R'_n a los esquemas proyectivos que aparecen tras la relajación de la premisa de partida; es sencillo identificar las novedades: en el primer caso, se introduce la variable a_1 y la nueva ecuación $G^{<n-1>} = 0$; en el segundo caso, la restricción $\sum x_i = 0$ se ve sustituida por la ecuación $K^{<n-1>} = 0$.

Otra vez, los esquemas X_n y R_n se recuperan bajo la forma de subesquemas de X'_n y R'_n cuando se impone que el cumplimiento de las ecuaciones $G^{<n\text{-}1>}=0$ y $K^{<n\text{-}1>}=0$ se concrete en el de las antiguas y más exigentes $a_1=0$ y $\sum x_i=0$. Es en este sentido en el que empleamos la denominación de *supraesquema* para cada uno de los esquemas Y'_n, X'_n y R'_n respecto del correspondiente esquema Y_n, X_n y R_n.

La demostración del teorema 5.2.2 se puede adaptar sin ningún cambio significativo al caso de los esquemas X'_n, R'_n y Y'_n, obteniendo que, para n y p dados, se tiene la equivalencia entre las tres afirmaciones siguientes:

$$(i)\ \ X'_n\big(\overline{\mathbb{F}}_p\big)=\emptyset, \qquad (ii)\ \ R'_n\big(\overline{\mathbb{F}}_p\big)=\emptyset, \qquad (iii)\ \ Y'_n\big(\overline{\mathbb{F}}_p\big)=\emptyset.$$

Aplicando resultados del capítulo 4, el teorema siguiente prueba que, de hecho, los pares eficaces para cada uno de los seis esquemas proyectivos X_n, X'_n, R_n, R'_n, Y_n y Y'_n son exactamente los mismos.

Teorema 5.3.1. *Para un grado n y un primo p dados, las seis afirmaciones siguientes son equivalentes entre sí:*

$$(i)\ \ X_n\big(\overline{\mathbb{F}}_p\big)=\emptyset, \qquad (iv)\ \ X'_n\big(\overline{\mathbb{F}}_p\big)=\emptyset,$$
$$(ii)\ \ R_n\big(\overline{\mathbb{F}}_p\big)=\emptyset, \qquad (v)\ \ R'_n\big(\overline{\mathbb{F}}_p\big)=\emptyset,$$
$$(iii)\ \ Y_n\big(\overline{\mathbb{F}}_p\big)=\emptyset, \qquad (vi)\ \ Y'_n\big(\overline{\mathbb{F}}_p\big)=\emptyset\ .$$

En particular, cada una de las anteriores igualdades constituye una condición suficiente para que el problema de Casas-Alvero de grado $n\geq 3$ posea respuesta afirmativa.

Demostración. Para $n=1$ o $n=2$ la equivalencia resulta obvia, pues las seis igualdades son verdaderas por carecer todos estos esquemas de entidad geométrica (ver Nota 3.0.5): En efecto, cuando es $n=1$, así como en el caso de X_2, R_2 e Y_2, son esquemas que no involucran ninguna variable; X'_2, R'_2 e Y'_2, por su parte, involucran cada uno una sola variable, obligada a anularse por la ecuación que define al esquema ($-a_1^2=0$, $-b_1^2=0$ y $-x_2^2=0$, respectivamente), cualquiera que sea el cuerpo considerado.

En el caso $n\geq 3$, las tres condiciones de la terna $(i),(ii),(iii)$ equivalen entre sí por el teorema 5.2.2 y, según acabamos de afirmar, el resultado análogo se verifica para los supraesquemas, esto es, las tres condiciones de la terna $(iv),(v),(vi)$ también equivalen entre sí. La cadena de equivalencias se cierra con la existente entre las condiciones (iii) y (vi), establecida por el teorema 4.1.4 de eliminación del término vicelíder.

Para concluir, basta apelar a la proposición 3.1.4. □

Corolario 5.3.2. *El teorema de condensación (4.2.1) y, en consecuencia, el principio de expansión, así como el teorema 4.3.1 que sitúa a todo par eficaz dentro de una estela, se verifican igualmente para los esquemas* X_n, R_n, Y_n', X_n' *y* R_n'

Observación 5.3.3. Dado que los seis esquemas considerados en 5.3.1 disponen de los mismos pares eficaces, podemos elegir cualquiera de ellos para trabajar en la práctica. Así, en la Memoria se ha utilizado principalmente el esquema Y_n, mientras que en [BLSW] el esquema empleado es X', que involucra una variable más que Y_n. En el próximo apartado, y usando el esquema de raíces, R_n —con el mismo número de variables que Y_n— se recuperarán con notable economía de esfuerzo los resultados de capítulos anteriores correspondientes a $h=3,4$ y 5; además —como ya se ha anunciado— se realizarán cálculos concluyentes también para $h=6$, y se mostrará asimismo que son viables para $n=7$. Se observa que, mientras que el esquema Y_n ha facilitado desarrollos de mayor valor conceptual, el esquema R_n parece más operativo cuando se trata de llevar a cabo cálculos efectivos orientados a nuestros fines.

5.4. Aplicación del esquema de raíces a la determinación de los primos eficaces

Nos proponemos a continuación, fijado un grado $n \geq 3$, hallar el modo de discriminar los primos ineficaces con n, es decir, aquellos primos p tales que sobre el cuerpo $\overline{\mathbb{F}}_p$ existan soluciones no triviales del sistema de $n-1$ ecuaciones en las $n-1$ incógnitas $x_2, \ldots, x_n$:

$$x_2 + x_3 + \cdots + x_n \;=\; x_2\,(x_2 - x_3) \;=\; K^{<2>} = K^{<3>} = \;\cdots\; = K^{<n-2>} = 0 \qquad (5.12)$$

que define al esquema proyectivo R_n. Ello equivale a preguntarse por las condiciones que hacen posible la existencia de un polinomio $P_n(X) = (X-x_1)\,(X-x_2)\;\cdots\;(X-x_n)$, con raíces no todas nulas $x_1, x_2, \ldots, x_n$ pertenecientes a $\overline{\mathbb{F}}_p$, y tal que se cumpla:

(*1*) $x_1 = 0$; $\quad x_2 + x_3 + \cdots + x_{n\text{-}1} + x_n = 0$.
(*2*) La raíz x_2 coincide, o bien con la raíz $x_1 = 0$, o bien con una tercera raíz $x_3 \neq 0$.
(*3*) Para cada $i = 2, \ldots, n-2$, $P_n^{<i>}(X)$ tiene una raíz en común con $P_n(X)$.

Supongamos que exista un polinomio como el descrito. Podemos asumir que la raíz de $P_n(X)$ ubicada en la posición de x_3 es distinta de cero: Si es $x_2 \neq 0$, porque entonces habrá de ser $x_3 = x_2$; y si, por el contrario, se verifica $x_2 = 0$, porque entonces podremos elegir en tercer lugar una raíz no nula que en todo caso posee $P_n(X)$, ya que no figura como x_1 ni como x_2. Más aún: por ser (5.12) un sistema homogéneo, podemos suponer

que el valor de x_3 es exactamente igual a 1, pues, de no ser así, bastaría cambiar la solución de partida por otra de su misma clase de equivalencia. Por otra parte, gracias a la existencia de dos modos alternativos (aunque no excluyentes mediando una permutación de las raíces) de satisfacer la condición *(2)*, el problema se escinde de forma natural en dos subproblemas independientes, correspondientes a cada uno de estos dos casos:

Caso I, abreviado [**C- I**]: Es $x_2 = 0$; las raíces de $P_n(X)$ son, por tanto:

$$0,\quad 0,\quad 1,\quad x_4,\quad x_5,\quad \ldots\quad ,\quad x_{n\text{-}1},\quad x_n,\qquad \text{con}\ \ x_4 = -\big(1 + \sum_{5\le j\le n} x_j\big).$$

Caso II, abreviado [**C-II**]: Es $x_2 = x_3 = 1$; y las raíces de $P_n(X)$ son:

$$0,\quad 1,\quad 1,\quad x_4,\quad x_5,\quad \ldots\quad ,\quad x_{n\text{-}1},\quad x_n,\qquad \text{con}\ \ x_4 = -\big(2 + \sum_{5\le j\le n} x_j\big).$$

Obsérvese que, en virtud de la condición *(1)*, cada uno de estos subproblemas requiere el uso de tan solo $n-4$ variables, pues x_4 viene dada por el valor de las restantes. En cuanto a la condición *(3)*, es obvio que $P_n^{<i>}(X)$ comparte alguna raíz con $P_n(X)$ si y solo si ocurre:

$$P_n^{<i>}(0) = 0,\quad \text{o bien}\ \ P_n^{<i>}(1) = 0,\quad \text{o bien}\ \ P_n^{<i>}(x_4) = 0,\quad \ldots\qquad \text{o bien}\ \ P_n^{<i>}(x_n) = 0,$$

de modo que *(3)* se materializa en un número finito de casos particulares —en principio, $(n-1)^{n\text{-}3}$, tantos como formas de adjudicar a cada derivada $P_n^{<2>}, \ldots, P_n^{<n\text{-}2>}$, una raíz elegida entre 0, 1, x_4, …, x_n; si bien, en la práctica, el número de casos distinguibles será mucho menor debido a las simetrías que se aprecian entre algunas configuraciones—.

Para $n = 3$**,** las raíces son simplemente $[\,0,\,0,\,1\,]$, en el caso I, y $[\,0,\,1,\,1\,]$, en el caso II. La condición *(3)* es vacía; así pues, solamente precisamos que se cumpla *(1)*, es decir, que sea nula la suma de las tres raíces. Pero,

[**C- I**] $\quad 0 + 0 + 1 = 0$, nunca ocurre;

[**C-II**] $\quad 0 + 1 + 1 = 0$, ocurre si y solo si es $p = 2$.

Este análisis recupera de forma elemental el hecho de que el primo 2 sea el único ineficaz para $n = 3$.

Para $n = 4$**,** la condición *(1)* obliga a que las raíces sean $[\,0,\ 0,\ 1, -1\,]$ en el caso I, y $[\,0,\ 1,\ 1, -2\,]$ en el caso II. Imponemos ahora la condición *(3)*:

[**C- I**] $P_4^{<2>}(X) = 6X^2 - 1$; por tanto: $P_4^{<2>}(0) = -1$, $P_4^{<2>}(1) = P_4^{<2>}(-1) = 5$.
Ninguno de ellos se anula, a menos que sea $p = 5$.

[**C-II**] $P_4^{<2>}(X) = 6X^2 - 3$; por tanto: $P_4^{<2>}(0) = -3$, $P_4^{<2>}(1) = 3$, $P_4^{<2>}(-2) = 21$.
Solamente para $p = 3$ o $p = 7$ se anula alguno de los tres.

Recuperamos así el hecho de que 3, 5 y 7 son los únicos primos ineficaces para $n = 4$.

A partir de aquí se introduce la variable $u = x_5 + x_6 + \cdots + x_n$, con lo cual la condición *(1)* deja $x_4 = -u-1$ en el caso I, y $x_4 = -u-2$ en el caso II. Esta expresión de x_4 la emplearemos para la raíz que nos interese singularizar en cuarta posición —que puede ser cualquiera de las raíces que quedan una vez apartadas x_1, x_2 y x_3 pues, a diferencia de estas, no han sido *marcadas* a priori siendo, por tanto, intercambiables—.

Para $n=5$, en particular, la variable u da forma concreta a las dos únicas raíces que no necesariamente son 0 o 1, y se tiene

[**C- I**] $P_5(X) = X^2(X-1)(X+u+1)(X-u)$
[**C-II**] $P_5(X) = X(X-1)^2(X+u+2)(X-u)$.

La condición *(3)* impone esta vez que, para respectivos valores x e y coincidentes con alguna de las raíces de $P_5(X)$, se verifiquen las igualdades $P_5{}^{<3>}(x)=0$, $P_5{}^{<2>}(y)=0$. Calculamos las derivadas de Hasse de órdenes 3 y 2 del polinomio $P_5(X)$ y obtenemos la expresión explícita de este par de igualdades:

[**C- I**] $10x^2-u^2-u-1=0$; $\quad -10y^2+3y\,(u^2+u+1)-u(u+1)=0$,
[**C-II**] $10x^2-u^2-2u-3=0$; $\quad -10y^3+3y\,(u^2+2u+3)-2(u+1)^2=0$.

La simetría entre las raíces $-1-u$ y u reduce a tan solo 20 (10 en cada caso) las posibilidades distinguibles de adjudicar valores a x e y. Se detalla a continuación, para cada una ellas, el par de polinomios $[f(u),g(u)] = [P_5{}^{<3>}(x), P_5{}^{<2>}(y)]$, y el valor de su resultante, R.

Caso I:	$x=y=0$,	$\left[-u^2-u-1,\ -u^2-u\right]$,	$R=1$
	$x=0,\ y=1$,	$\left[-u^2-u-1,\ 2u^2+2u-7\right]$,	$R=3^4$
	$x=0,\ y=u$,	$\left[-u^2-u-1,\ -7u^3+2u^2+2u\right]$	$R=3^4$
	$x=1,\ y=0$,	$\left[-u^2-u+9,\ -u^2-u\right]$,	$R=3^4$
	$x=y=1$,	$\left[-u^2-u+9,\ 2u^2+2u-7\right]$,	$R=11^2$
	$x=1,\ y=u$,	$\left[-u^2-u+9,\ -7u^3+2u^2+2u\right]$,	$R=3^2\cdot 3541$
	$x=u,\ y=0$,	$\left[9u^2-u-1,\ -u^2-u\right]$	$R=-3^2$
	$x=u,\ y=1$,	$\left[9u^2-u-1,\ 2u^2+2u-7\right]$	$R=3541$
	$x=y=u$,	$\left[9u^2-u-1,\ -7u^3+2u^2+2u\right]$	$R=11^2$
	$x=u,\ y=-u-1$,	$\left[9u^2-u-1,\ 7u^3+23u^2+23u+7\right]$,	$R=3^2\cdot 3541$

Caso II:	$x=y=0$,	$\left[-u^2-2u-3,\ -2u^2-4u-2\right]$,	$R=2^4$
	$x=0,\ y=1$,	$\left[-u^2-2u-3,\ u^2+2u-3\right]$,	$R=2^2\cdot 3^2$
	$x=0,\ y=u$,	$\left[-u^2-2u-3,\ -7u^3+4u^2+5u-2\right]$,	$R=-2^2\cdot 3\cdot 193$
	$x=1,\ y=0$,	$\left[-u^2-2u+7,\ -2u^2-4u-2\right]$,	$R=2^8$
	$x=y=1$,	$\left[-u^2-2u+7,\ u^2+2u-3\right]$,	$R=2^4$
	(continúa)		

(C-II)	(*continuación*)		
	$x=1,\ y=u,$	$\left[-u^2-2u+7,\ -7u^3+4u^2+5u-2\right],$	$R=2^4\cdot 599$
	$x=u,\ y=0,$	$\left[9u^2-2u-3,\ -2u^2-4u-2\right],$	$R=2^8$
	$x=u,\ y=1,$	$\left[9u^2-2u-3,\ u^2+2u-3\right],$	$R=2^4\cdot 3\cdot 7$
	$x=y=u,$	$\left[9u^2-2u-3,\ -7u^3+4u^2+5u-2\right],$	$R=-2^4\cdot 131$
	$x=u,\ y=-u-2,$	$\left[9u^2-2u-3,\ 7u^3+46u^2+95u+60\right],$	$R=2^4\cdot 3\cdot 7\cdot 8009$

Un valor $u\in\overline{\mathbb{F}}_p$ que haga anularse a los dos polinomios de una misma pareja proporciona inmediatamente un polinomio $P_5(X)$ cumpliendo todas las condiciones requeridas, y viceversa; así pues, el que la resultante R sea nula módulo p es condición necesaria y (a menos que los respectivos coeficientes líder sean ambos múltiplos de p) también suficiente para que se cumpla $R_5(\overline{\mathbb{F}}_p)\neq\emptyset$. De este modo, los primos ineficaces con $n=5$ se encontrarán entre los divisores de los diferentes R así obtenidos.

Los resultados anteriores proporcionan otra demostración del corolario 4.4.4. En efecto, puesto que los coeficientes líder de los dos polinomios en cada corchete han resultado ser primos entre sí, se cumple que $R_5(\overline{\mathbb{F}}_p)\neq\emptyset$ si y solo si p divide a alguno de los valores de R que figuran en la tabla anterior. Se deduce por tanto que los primos ineficaces para $n=5$ son 2, 3, 7, 11, 131, 193, 599, 3541 y 8009.

Para $n=6$ introduciremos una nueva variable $v=x_5\,x_6$, que tomada junto con $u=x_5+x_6$ encierra la misma información que el par no ordenado formado por x_5 y x_6. Se tiene así $X^2-u\,X+v=(X-x_5)(X-x_6)$, y podemos escribir:

[**C- I**] $\quad P_6(X)=X^2(X-1)(X+u+1)(X^2-u\,X+v)$
[**C-II**] $\quad P_6(X)=X(X-1)^2(X+u+2)(X^2-u\,X+v)$

Como una alternativa al procedimiento usado con $n=5$, esta vez impondremos en primer lugar que el polinomio $P_6^{<4>}(X)$ comparta una raíz con $P_6(X)$, esto es, que se verifique la igualdad $P_6^{<4>}(x)=0$ para alguno de los valores $x\in\{0,1,-u-1\}$ en el caso I; o bien $x\in\{0,1,-u-2\}$ en el caso II —recordemos que las dos raíces restantes, x_5 y x_6, son intercambiables con x_4— dejando para un segundo momento el uso de las condiciones $\mathrm{Res}\left(P_6,P_6^{<3>}\right)=0$, $\mathrm{Res}\left(P_6,P_6^{<2>}\right)=0$. El interés de esta forma de proceder radica en que la condición $P_6^{<4>}(x)=0$ impuesta de partida permite despejar (para cada x de los citados) v en función de u, gracias a que $P_6^{<4>}$ es un polinomio de grado 1 en la variable v:

[**C- I**] $\quad P_6^{<4>}(X)=15\,X^2-u^2-u+v$
[**C-II**] $\quad P_6^{<4>}(X)=15\,X^2-u^2-2u-3+v$

Obtenido por este procedimiento el valor $v = v(u)$, al sustituirlo en las resultantes $\mathrm{Res}\big(P_6, P_6{}^{<3>}\big)$ y $\mathrm{Res}\big(P_6, P_6{}^{<2>}\big)$ se consiguen dos polinomios en la variable u, $R_1(u)$ y $R_2(u)$, respectivamente; la existencia de una raíz común a ambos será condición necesaria y suficiente para que exista un polinomio $P_6(X)$ como el buscado, lo que equivale a una solución no trivial del sistema que define a R_6. Interesa entonces hallar el valor del entero $R = \mathrm{Res}\big(R_1(u), R_2(u)\big)$ para cada uno de los seis subcasos que se presentan —tres por cada caso—, pues en la reunión de sus divisores se encuentran todos los primos ineficaces para $n = 6$ (y quizá también alguno que no lo sea). La tabla que aparece a continuación resume el desarrollo de esta casuística.

Caso I	$x = 0$	$R_1(u) = 3456\,u^{21} + \big(\text{t}^{\text{os}}\text{ menor grado}\big)$, $R_2(u) = 6859\,u^{18} + \big(\text{t}^{\text{os}}\text{ menor grado}\big)$ $R = 2^{72} \cdot 7^{24} \cdot 13^{12} \cdot 19^{27} \cdot 67^{12} \cdot 20771^{12}$
	$x = 1$	$R_1(u) = 3456\,u^{21} + \big(\text{t}^{\text{os}}\text{ menor grado}\big)$, $R_2(u) = 6859\,u^{18} + \big(\text{t}^{\text{os}}\text{ menor grado}\big)$ $R = 2^{72} \cdot 7^{51} \cdot 11^{36} \cdot 13^{9} \cdot 19^{9} \cdot 61^{12} \cdot 21379^{3} \cdot 23993^{9} \cdot$ $\cdot\, 7783207^{3} \cdot 40362599^{3} \cdot 7390044713023799^{3}$
	$x = \text{-}1\text{-}u$	$R_1(u) = 517856746176\,u^{21} + \big(\text{t}^{\text{os}}\text{ m.g.}\big)$, $R_2(u) = 47929184576\,u^{18} + \big(\text{t}^{\text{os}}\text{ m.g.}\big)$ $R = 2^{54} \cdot 7^{39} \cdot 11^{36} \cdot 13^{6} \cdot 19^{18} \cdot 61^{12} \cdot 21379^{3} \cdot 23993^{6} \cdot$ $\cdot\, 7783207^{3} \cdot 40362599^{3} \cdot 7390044713023799^{3}$
Caso II	$x = 0$	$R_1(u) = 3456\,u^{21} + \big(\text{t}^{\text{os}}\text{ menor grado}\big)$, $R_2(u) = 6859\,u^{18} + \big(\text{t}^{\text{os}}\text{ menor grado}\big)$ $R = 2^{72} \cdot 5^{108} \cdot 7^{6} \cdot 29^{3} \cdot 37^{3} \cdot 47^{6} \cdot 73^{6} \cdot 811^{9} \cdot 1487^{3} \cdot 3209^{6} \cdot$ $\cdot\, 3877^{3} \cdot 9337^{3} \cdot 17250187^{3}$
	$x = 1$	$R_1(u) = 216\,u^{21} + \big(\text{t}^{\text{os}}\text{ menor grado}\big)$, $R_2(u) = 6859\,u^{18} + \big(\text{t}^{\text{os}}\text{ menor grado}\big)$ $R = 2^{54} \cdot 5^{108} \cdot 7^{9} \cdot 19^{3} \cdot 37^{3} \cdot 73^{9} \cdot 97^{6} \cdot 1069^{3} \cdot 1499^{3} \cdot 4019^{9} \cdot$ $\cdot\, 685177^{3} \cdot 70016757407^{3}$
	$x = \text{-}2\text{-}u$	$R_1(u) = 517856746176\,u^{21} + \big(\text{t}^{\text{os}}\text{ m.g.}\big)$, $R_2(u) = 47929184576\,u^{18} + \big(\text{t}^{\text{os}}\text{ m.g.}\big)$ $R = 2^{54} \cdot 5^{108} \cdot 7^{29} \cdot 11 \cdot 19^{2} \cdot 23^{16} \cdot 37^{2} \cdot 67^{4} \cdot 257^{3} \cdot 983 \cdot 1087 \cdot 1187 \cdot$ $\cdot\, 1901 \cdot 2287 \cdot 3881 \cdot 4019^{3} \cdot 4943 \cdot 5471 \cdot 6983 \cdot 8699 \cdot 15131 \cdot 15823^{2} \cdot$ $\cdot\, 150203 \cdot 266587^{3} \cdot 547061 \cdot 885061 \cdot 1030951^{2} \cdot 9348983563 \cdot$ $\cdot\, 2610767527031 \cdot 225833117528659^{2} \cdot 51313000813080529$

Cuadro 5.1: Términos líder y resultante común de R_1 y R_2, en los seis casos distinguibles

Teorema 5.4.1. *Los primos ineficaces con $n=6$ son los 53 siguientes, dados por niveles:*

Nivel 1: 2, 5, 7, 19.

Nivel 2: 11, 13, 29, 37, 61, 67, 73, 1487, 20771, 23993.

Nivel 3: 47, 257, 811, 1069, 3209, 3877, 3881, 8699, 9337, 15823, 21379, 150 203, 547 061, 7 783 207, 17 250 187, 40 362 599, 2 610 767 527 031, 7390 044 713 023 799.

Nivel 4: 23, 97, 983, 1087, 1187, 1499, 1901, 2287, 4019, 4943, 5471, 6983, 15131, 266 587, 685 177, 885 061, 1 030 951, 9348983563, 70016757407, 225 883 117 528 659, 51 313 000 813 080 529.

En consecuencia, la conjetura de Casas-Alvero es cierta para los enteros de la forma $n=6p^r$ siempre que p sea un primo diferente de los que figuran en este listado.

Demostración. En cada uno de los seis subcasos contenidos en la tabla 5.1, es válido el siguiente razonamiento: Si el primo p divide a R pero no es un divisor común de los coeficientes líder de R_1 y R_2, entonces $R_6(\overline{\mathbb{F}}_p)\neq\emptyset$. Usando la información contenida en dicha tabla puede comprobarse que, salvo en los subcasos tercero y sexto, los mencionados coeficientes líder son primos entre sí, mientras que en el tercer y el sexto subcaso los primos divisor común de ambos coeficientes líder son únicamente $p=2$ y $p=7$, quienes se obtienen sin ninguna complicación desde los otros subcasos. Se concluye que cada uno de los primos aparecidos como factor de R en alguno de los seis subcasos es en efecto ineficaz con $n=6$.

Para $n=7$, un método combinado de los utilizados para $n=5$ y $n=6$ puede reproducirse sin apenas cambios y mínimas complicaciones de procedimiento, si bien con un considerable incremento de la capacidad de cómputo requerida para llevarlo a término. En este caso, la variable u se complementa con $v=x_5x_6+x_5x_7+x_6x_7$ y $w=x_5x_6x_7$, dando lugar a las expresiones:

[**C- I**] $\quad P_7(X)=X^2(X-1)(X+u+1)(X^3-uX^2+vX-w)$

[**C-II**] $\quad P_7(X)=X(X-1)^2(X+u+2)(X^3-uX^2+vX-w)$

En una primera etapa impondremos que $P_7^{<5>}(X)$ tenga una raíz x que tome uno de los valores $0,\ 1,\ -1-u$, en el caso I; $0,\ 1,\ -2-u$, en el caso II. En una segunda etapa, imponemos a $P_7^{<4>}(X)$ que tenga una raíz y coincidente con uno de los valores $0,\ 1,\ -1-u$, en el caso I; $0,\ 1,\ -2-u,\ t$ (siendo t una raíz de X^3-uX^2+vX-w), en el caso II.

Se obtienen nueve posibilidades distintas de combinar los valores de x e y en el caso I, y diez posibilidades en el caso II; estas últimas son, en concreto, las nueve

que corresponden a que tanto x como y sean 1, 2 o $-2-u$, más una posibilidad especial que corresponde a $x=-2-u,\ y=t$. Excluida esta última posibilidad, que seguiremos llamando *especial*, en las dieciocho restantes se verifica lo siguiente: La condición $P_7{}^{<5>}(x)=0$ es lineal en w, lo cual permite despejar w como función de (u,v) y sustituirla luego en la condición $P_7{}^{<4>}(y)=0$, y la expresión que se obtiene entonces resulta ser lineal en v. En definitiva, en cada una de estas dieciocho posibilidades, del par de condiciones

$$P_7{}^{<5>}(x)=0, \qquad P_7{}^{<4>}(y)=0$$

se logra despejar

$$v=v(u)\,, \qquad w=w\big(u,v(u)\big). \tag{5.13}$$

Las condiciones de que $P_7{}^{<3>}(X)$ y $P_7{}^{<2>}(X)$ compartan respectivas raíces con $P_7(X)$ se incorporarán a través de los polinomios

$$\mathrm{Res}\big(P_7(X),P_7{}^{<3>}(X)\big)\,,\ \mathrm{Res}\big(P_7(X),P_7{}^{<2>}(X)\big)\in\mathbb{Z}[u,v,w]$$

quienes, mediante la sustitución (5.13), dan lugar a dos polinomios

$$R_3(u)\,,\ R_2(u)\in\mathbb{Z}[u];$$

se precisa que $R_3(u)$ y $R_2(u)$ se anulen simultáneamente, esto es, que compartan una raíz en $\overline{\mathbb{F}}_p$. Las dieciocho resultantes de la forma $R=\mathrm{Res}\big(R_3(u),R_2(u)\big)$ son números enteros cuyos divisores primos son ineficaces para $h=7$.

En el caso especial, la expresión para despejar w es igualmente lineal, pero la expresión para despejar v es cuadrática en v; no obstante, mediante algunas argumentaciones adicionales, esta complicación puede aún tratarse de forma adecuada, de modo que se llegue a obtener también los primos ineficaces aportados por dicho caso, completando el conjunto de todos los primos ineficaces con $h=7$.

Puesto que el procedimiento descrito, según hemos comprobado, excede la capacidad de cómputo del programa DERIVE, no presentamos el listado de resultados que podría obtenerse del mismo; por otra parte, la lista de primos ineficaces con $h=7$ ya ha sido proporcionada por Castryck *et al.* y puede consultarse en [CLO-2]. Consta de 661 primos, denominados por los autores 'primos malos Casas-Alvero' (*CA-bad primes*).

5.5. Esquemas sintéticos

De entre los esquemas de aplicación al problema total de Casas-Alvero de grado n que hemos ido utilizando (Y_n, X_n y R_n, así como sus respectivos supraesquemas Y_n', X_n' y R_n') es el esquema de raíces el que mayor simplicidad confiere a los cálculos, como consecuencia

de haber asignado selectivamente los valores de 0 o de 1 a las tres primeras raíces del polinomio. Para manejar los problemas parciales disponemos hasta el momento de los subesquemas de Y_n denotados como $Z_{n,I}$, así como de los análogos subesquemas de X_n denotados por $X_{n,I}$.

En esta sección describiremos nuevos esquemas, que llamaremos *esquemas sintéticos*, para su aplicación en los problemas parciales de Casas-Alvero. Nos referiremos en concreto al I-problema parcial de Casas-Alvero donde I tiene cardinal $r \geq 1$ y sus elementos son los enteros k_r, $k_{r-1}, \ldots, k_1$, con

$$0 < k_r < k_{r\text{-}1} < \ldots < k_2 < k_1 < n-1 < n.$$

Sin alteración significativa del desarrollo posterior, podríamos dejar que la desigualdad $k_1 < n-1$ fuera no estricta, pero en consonancia con el resto de la Memoria prescindimos del innecesario grado $n-1$.

Puesto que el polinomio $P_n(X)$ comparte la raíz de valor 0 con cada una las derivadas cuyo orden no se encuentra en I, bastará con introducir variables s_r, $s_{r\text{-}1}, \ldots, s_1$ cuyos valores, en cada supuesto particular, sean los de las raíces de $P_n(X)$ compartidas con sus derivadas de orden k_r, $k_{r\text{-}1}$, $\ldots$, k_1, respectivamente.

Según se señaló en la observación 5.2.3 —inmediatamente después de probar que Y_n y X_n tienen los mismos primos eficaces—, siendo $\mathbb{K}$ cualquiera de los cuerpos $\overline{\mathbb{F}}_p$ o $\mathbb{C}$ se verifica la equivalencia entre las dos condiciones $Z_{n,I}(\mathbb{K}) = \emptyset$ y $X_{n,I}(\mathbb{K}) = \emptyset$, de modo que podemos utilizar indistintamente, o bien derivadas netas y coeficientes presentados, o bien derivadas de Hasse y coeficientes ordinarios para determinar la existencia de contraejemplos sobre $\mathbb{K}$ del problema parcial.

En esta sección consideraremos derivadas de Hasse y coeficientes ordinarios; en particular, a las r variables anteriores les añadiremos las r variables $a_{n\text{-}k_1}, a_{n\text{-}k_2}, \ldots, a_{n\text{-}k_r}$ que figuran como coeficientes del polinomio

$$P_{n,I}(X) = X^n + a_{n\text{-}k_1} X^{k_1} + a_{n\text{-}k_2} X^{k_2} + \cdots + a_{n\text{-}k_r} X^{k_r}.$$

Entonces se tiene que $X_{n,I}(\mathbb{K}) \neq \emptyset$ si y solo si existe una solución

$$(\alpha_{n\text{-}k_1}, \alpha_{n\text{-}k_2}, \ldots, \alpha_{n\text{-}k_r}, \sigma_r, \sigma_{r\text{-}1}, \ldots, \sigma_1) \in \mathbb{K}^{2r},$$

con no todas las componentes $\alpha_{n\text{-}l}$ nulas, para el sistema de ecuaciones

$$\begin{aligned} P_{n,I}(s_r) &= P_{n,I}(s_{r\text{-}1}) = \ldots = P_{n,I}(s_1) = 0 \\ P_{n,I}^{<k_r>}(s_r) &= P_{n,I}^{<k_{r-1}>}(s_{r\text{-}1}) = \ldots = P_{n,I}^{<k_1>}(s_1) = 0. \end{aligned} \tag{5.14}$$

Dado que se tiene $P_{n,I}^{<k_l>}(X) = \binom{n}{k_l} X^{n-k_l} + \binom{k_1}{k_l} a_{n-k_1} X^{k_1-k_l} + \ldots + a_{n-k_l}$, la condición de que no sean nulas todas las componentes $\alpha_{n\text{-}k_1}, \alpha_{n\text{-}k_2}, \ldots, \alpha_{n\text{-}k_r}$ es equivalente a que

no sean nulas todas las raíces compartidas $\sigma_r,\ \sigma_{r\text{-}1},\dots,\sigma_1$. Podemos observar que las $2r$ ecuaciones del sistema anterior son lineales en las variables $a_{n\text{-}k_1},\ a_{n\text{-}k_2},\ \dots,a_{n\text{-}k_r}$ y que, si consideramos únicamente las r últimas ecuaciones, entonces la matriz ampliada de tal subsistema de ecuaciones lineales en dichas variables es la matriz $r\times(r+1)$ siguiente (donde, por conveniencia, se ha puesto $k_0=n$):

$$\begin{pmatrix}
\binom{k_0}{k_r}s_r^{k_0\text{-}k_r} & \binom{k_1}{k_r}s_r^{k_1\text{-}k_r} & \dots & \dots & \dots & \binom{k_{r-1}}{k_r}s_r^{k_{r-1}\text{-}k_r} & 1\\
\binom{k_0}{k_{r-1}}s_{r\text{-}1}^{k_0\text{-}k_{r-1}} & \binom{k_1}{k_{r-1}}s_{r\text{-}1}^{k_1\text{-}k_{r-1}} & \dots & \dots & \dots & 1 & \\
\binom{k_0}{k_{r-2}}s_{r\text{-}2}^{k_0\text{-}k_{r-2}} & \binom{k_1}{k_{r-2}}s_{r\text{-}2}^{k_1\text{-}k_{r-2}} & \dots & \dots & 1 & & \\
\vdots & \vdots & & 1 & & & \\
\vdots & \vdots & 1 & & & & \\
\binom{k_0}{k_1}s_1^{k_0\text{-}k_1} & 1 & & & & &
\end{pmatrix} \tag{5.15}$$

habida cuenta de que la primera columna corresponde a los términos independientes (en realidad, con signo opuesto). Podemos apreciar que el término general es de la forma $\binom{k_l}{k_m}s_m^{k_l\text{-}k_m}$, con $1\le m\le r$ y $0\le l\le r$, entendiendo que $\binom{k_l}{k_m}=0$ si $m<l$. En particular, la matriz de coeficientes del subsistema es triangular con *unos* en la diagonal; por tanto, se trata de un subsistema de Cramer cuya única solución proporciona expresiones precisas

$$a_{n\text{-}k_l}=a_{n\text{-}k_l}(s_1,\dots,s_l),\qquad 1\le l\le r \tag{5.16}$$

que son polinomios homogéneos con coeficientes enteros y de grado igual al respectivo subíndice. Estas expresiones de las a_m en términos de las s_m se pueden sustituir en las r primeras ecuaciones del sistema 5.14, convirtiendo la condición $P_{n,I}(s_l)=0$ en una expresión $M_l(s_1,\dots,s_r)=0$, donde M_l es un polinomio homogéneo de grado n en las variables $s_1,\dots,s_r$.

Definición 5.5.1. Llamaremos esquema sintético correspondiente al conjunto de grados I, y denotaremos por $S_{n,I}$, al esquema proyectivo definido por el ideal del anillo $\mathbb{Z}[s_1,\dots,s_r]$ generado por los polinomios homogéneos $M_l(s_1,\dots,s_r)$, para $1\le l\le r$.

Teorema 5.5.2. *Siendo $\mathbb{K}$ cualquiera de los cuerpos $\overline{\mathbb{F}}_p$ o $\mathbb{C}$, son equivalentes:*

(*i*) $Z_{n,I}(\mathbb{K})\neq\emptyset$

(*ii*) $S_{n,I}(\mathbb{K})\neq\emptyset$.

En particular, el I-problema parcial de Casas-Alvero en grado n tiene respuesta afirmativa si y solo si $S_{n,I}(\overline{\mathbb{F}}_p)=\emptyset$ para algún primo p.

Demostración. La segunda parte es consecuencia inmediata de la primera, según las proposiciones 3.1.2 y 3.0.3. Para probar la equivalencia entre (i) y (ii) utilizaremos el hecho de que (i) equivale a su vez a que sea $X_{n,I}(\mathbb{K}) \neq \emptyset$ (ver observación 5.2.3).

Si se tiene $X_{n,I}(\mathbb{K}) \neq \emptyset$, bastará tomar un representante cualquiera de uno de sus puntos para obtener los coeficientes de un I-polinomio que comparte raíces en $\mathbb{K}$ con todas sus derivadas de grado positivo; considerando r raíces $\sigma_r, \ldots, \sigma_1$ compartidas respectivamente con las derivadas de orden $k_r, \ldots, k_1$ se completa la $2r$-upla $(\alpha_{n\text{-}k_1}, \ldots, \alpha_{n\text{-}k_r}, \sigma_r, \ldots, \sigma_1)$ que es solución no nula (y con algún $\sigma_l \neq 0$) del sistema (5.14); en particular, la r-upla $(\sigma_1, \sigma_2, \ldots, \sigma_r) \in \mathbb{K}^r$ es solución de las ecuaciones $M_l(s_1, \ldots, s_r) = 0$, $1 \leq l \leq r$, que definen al esquema $S_{n,I}$.

Recíprocamente, la existencia de algún punto en $S_{n,I}(\mathbb{K})$ supone la existencia de alguna solución no trivial $(\sigma_1, \sigma_2, \ldots, \sigma_r) \in \mathbb{K}^r$ del sistema $M_l(s_1, \ldots, s_r) = 0$, $1 \leq l \leq r$; basta ahora aplicar las fórmulas (5.16) para completar una solución del sistema (5.14), la cual describe un I-polinomio —distinto de X^n— cuyos coeficientes determinan un punto perteneciente a $X_{n,I}(\mathbb{K})$. □

Observación 5.5.3. En el problema total de Casas-Alvero de grado n (asociado al conjunto completo de exponentes, $J = \{1, 2, \ldots, n-2\}$), el concepto de primo p ineficaz con n de nivel m introducido en 4.4.1 expresa la doble condición de ser $Y_n(\overline{\mathbb{F}}_p) = Z_{n,J}(\overline{\mathbb{F}}_p) \neq \emptyset$ y de ser m el mínimo cardinal entre los subconjuntos $I \subset J$ tales que $Z_{n,I}(\overline{\mathbb{F}}_p) \neq \emptyset$. El teorema anterior y la observación 5.2.3 muestran que, a efectos de determinar el nivel de ineficacia de p, los esquemas $X_{n,I}$ y $S_{n,I}$ pueden intercambiarse con $Z_{n,I}$.

Los esquemas sintéticos son una opción alternativa para estudiar la conjetura de Casas-Alvero cuando se tiene información acerca del conjunto I en que se encuadra un hipotético contraejemplo. A continuación supondremos que conocemos I y que consideramos contraejemplos en los cuales sea $a_{n\text{-}k_r} \neq 0$. Necesitamos para ello la carta afín del esquema sintético $S_{n,I}$ dada por $s_r \neq 0$ y denotaremos por $U_{n,I}(\mathbb{K})$ el subconjunto de $S_{n,I}(\mathbb{K})$ formado por los puntos del esquema sintético tales que sus coordenadas homogéneas pueden elegirse del tipo $(s_1, \ldots, s_{r\text{-}1}, 1)$, de modo que $s_1, \ldots, s_{r\text{-}1}$ sirvan como coordenadas afines para dicha carta. Asumiremos en adelante $r \geq 2$ y, por motivos prácticos, reformularemos mínimamente la notación escribiendo $q = r-2$, $k_r = i$, $k_{r\text{-}1} = j$, $s_{r\text{-}1} = t$. En particular, las coordenadas afines serán $(s_1, \ldots, s_q, t)$ a partir de ahora, y mantendremos siempre la restricción $s_r = 1$. El sistema (5.14) adopta la siguiente forma:

$$\begin{array}{rcccccccl} P_{n,I}(1) & = & P_{n,I}(t) & = & P_{n,I}(s_q) & = & \ldots & = & P_{n,I}(s_1) = 0 \\ P_{n,I}^{<i>}(1) & = & P_{n,I}^{<j>}(t) & = & P_{n,I}^{<k_q>}(s_q) = & & \ldots & = & P_{n,I}^{<k_1>}(s_1) = 0; \end{array} \tag{5.17}$$

y de aquí, tomando la primera de cada uno de los dos grupos de $q+2$ condiciones, extraemos el sistema lineal

$$\begin{aligned} 1 \;+\; \sum_{l=1}^{q} a_{n\text{-}k_l} \;+\; a_{n\text{-}j} \;+\; a_{n\text{-}i} \;&=\; 0 \\ \tbinom{n}{i} + \sum_{l=1}^{q} \tbinom{k_l}{i}\, a_{n\text{-}k_l} + \tbinom{j}{i}\, a_{n\text{-}j} + \; a_{n\text{-}i} \;&=\; 0, \end{aligned}$$

a partir del cual se obtienen las expresiones

$$\begin{aligned} \Big(1-\tbinom{j}{i}\Big)\; a_{n\text{-}i} \;&=\; \Big(\tbinom{j}{i}-\tbinom{n}{i}\Big) \;+\; \sum_{l=1}^{q} \Big(\tbinom{j}{i}-\tbinom{k_l}{i}\Big)\; a_{n\text{-}k_l} \\ -\Big(1-\tbinom{j}{i}\Big)\; a_{n\text{-}j} \;&=\; \Big(1-\tbinom{n}{i}\Big) \;+\; \sum_{l=1}^{q} \Big(1-\tbinom{k_l}{i}\Big)\; a_{n\text{-}k_l} \end{aligned}$$

que permiten despejar $a_{n\text{-}i}, a_{n\text{-}j}$ siempre que sea $1-\binom{j}{i} \neq 0$ en $\mathbb{K}$, es decir, cuando sea $\mathbb{K} \neq \overline{\mathbb{F}}_p$ para aquellos primos p divisores de $1-\binom{j}{i}$; si este es el caso, podemos sustituir las expresiones obtenidas en las $2q+2$ ecuaciones restantes de (5.17) dando lugar a otras tantas condiciones lineales en $a_{n\text{-}k_1}, \ldots, a_{n\text{-}k_q}$ cuyos coeficientes son polinomios no homogéneos en las variables $s_1, \ldots, s_q, t$. De estas condiciones, las que se obtienen a partir de las últimas $q+1$ ecuaciones del primer grupo se expresan respectivamente en la forma siguiente:

$$\begin{aligned} C_n(t) \;+\; \sum_{l=1}^{q} C_{k_l}(t)\, a_{n\text{-}k_l} \;&=\; 0 \\ C_n(s_m) \;+\; \sum_{l=1}^{q} C_{k_l}(s_m)\, a_{n\text{-}k_l} \;&=\; 0, \quad m=1,\ldots,q, \end{aligned} \tag{5.18}$$

siendo $C_h(X) = \Big(1-\tbinom{j}{i}\Big)\,\big(X^h - X^i\big) - \Big(1-\tbinom{h}{i}\Big)\,\big(X^j - X^i\big)$ para $h \geq j$. Además, del segundo grupo de ecuaciones en (5.17), la segunda condición está dada por

$$C_n^{<j>}(t) \;+\; \sum_{l=1}^{q} C_{k_l}^{<j>}(t)\, a_{n\text{-}k_l} \;=\; 0, \tag{5.19}$$

y las q condiciones últimas forman un sistema de Cramer de ecuaciones lineales en las incógnitas $a_{n\text{-}k_1}, \ldots, a_{n\text{-}k_q}$,

$$C_n^{<k_m>}(s_m) + \sum_{l=1}^{m} C_{k_l}^{<k_m>}(s_m)\, a_{n\text{-}k_l} = 0, \quad m=1,\ldots,q,$$

cuya matriz ampliada es la submatriz obtenida de (5.15) al suprimir las dos primeras filas y las dos últimas columnas. En particular, la solución única de este sistema de Cramer vuelve a proporcionar para estas q indeterminadas las mismas expresiones

$$a_{n\text{-}k_l} = a_{n\text{-}k_l}(s_1, \ldots, s_l)$$

que se tenían en (5.16). Las sustitución de estas $a_{n\text{-}k_l}$ en las $q+1$ ecuaciones (5.18) y en la ecuación (5.19) da lugar a expresiones polinómicas no homogéneas en $\mathbb{Z}\big[s_1, \ldots, s_q, t\big]$

$$\begin{aligned} N(s_1,\ldots,s_q,t) &= 0 \\ N_m(s_1,\ldots,s_q) &= 0, \quad 1\le m\le q, \\ N'(s_1,\ldots,s_q,t) &= 0\,, \end{aligned} \tag{5.20}$$

de las cuales, las q intermedias no involucran a la variable t; la primera es de grado n en t y coeficiente inicial $1-\binom{j}{i}$, y la última es de grado $n-j$ en t y coeficiente inicial $\left(1-\binom{j}{i}\right)\binom{n}{j}$. Definimos finalmente

$$R(s_1,\ldots,s_q) = \mathrm{Res}_t\big(N(s_1,\ldots,s_q,t)\,,\, N'(s_1,\ldots,s_q,t)\big) \in \mathbb{Z}[s_1,\ldots,s_q],$$

y consideramos las $q+1$ condiciones en las variables $s_1,\ldots,s_q$ dadas por

$$\begin{aligned} R(s_1,\ldots,s_q) &= 0 \\ N_m(s_1,\ldots,s_q) &= 0\,, \quad 1\le m\le q. \end{aligned} \tag{5.21}$$

Proposición 5.5.4. *Sea $\mathbb{K}=\mathbb{C}$ o $\overline{\mathbb{F}}_p$. Si se cumple $1-\binom{j}{i}\neq 0$ en $\mathbb{K}$, entonces son condiciones equivalentes:*

(*i*) $U_{n,I}(\mathbb{K})=\emptyset$

(*ii*) *El sistema (5.20) no tiene solución en $\mathbb{K}^{q+1}$.*

(*iii*) *El sistema (5.21) no tiene solución en $\mathbb{K}^{q}$.*

Demostración. La equivalencia entre (*i*) y (*ii*) se debe a que (5.20) expresa la condición necesaria y suficiente para que $\big[(s_1,\ldots,s_q,t,1)\big]$ se encuentre en $S_{n,I}(\mathbb{K})$ —perteneciendo, de hecho, a la carta local adecuada para ser un elemento de $U_{n,I}(\mathbb{K})$—. La implicación (*iii*)⇒(*ii*) también es evidente, ya que si $(\sigma_1,\ldots,\sigma_q,\tau)\in\mathbb{K}^{q+1}$ es solución de (5.20) entonces $(\sigma_1,\ldots,\sigma_q)\in\mathbb{K}^q$ es solución de (5.21). Recíprocamente, si $(\sigma_1,\ldots,\sigma_q)\in\mathbb{K}^q$ es solución de (5.21) entonces se tiene, en particular, $R(\sigma_1,\ldots,\sigma_q)=0$. Dado que este valor numérico es la resultante de los polinomios $N(\sigma_1,\ldots,\sigma_q,t)$ y $N'(\sigma_1,\ldots,\sigma_q,t)$ pertenecientes a $\mathbb{K}[t]$, y que el coeficiente de grado n del primero es $1-\binom{j}{i}$ —por hipótesis, no nulo— ello significa que existe $\tau\in\mathbb{K}$ cumpliendo $N(\sigma_1,\ldots,\sigma_q,\tau)=N'(\sigma_1,\ldots,\sigma_q,\tau)=0$, de modo que la $(q+1)$-upla formada es solución de (5.20); esto prueba la implicación (*ii*)⇒(*iii*). □

5.6. Discriminantes

Con las notaciones anteriores, denotaremos por $\mathcal{J}(n,I)$ y $\mathcal{J}(n,I)_{\mathbb{K}}$ a los ideales respectivamente de $\mathbb{Z}[s_1,\ldots,s_q]$ y de $\mathbb{K}[s_1,\ldots,s_q]$ generados por los $q+1$ polinomios $R(s_1,\ldots,s_q)$ y $N_m(s_1,\ldots,s_q)$, $1\le m\le q$. De igual modo, denotaremos por $\mathcal{J}_{\mathrm{o}}(n,I)$ y $\mathcal{J}_{\mathrm{o}}(n,I)_{\mathbb{K}}$ a los ideales respectivamente de $\mathbb{Z}[s_1,\ldots,s_q,t]$ y de $\mathbb{K}[s_1,\ldots,s_q,t]$ generados por los $q+2$ polinomios $N(s_1,\ldots,s_q,t)$, $N'(s_1,\ldots,s_q,t)$ y $N_m(s_1,\ldots,s_q)$, $1\le m\le q$.

Definición 5.6.1. Llamaremos discriminante asociado a los datos (n, I) a un generador $\Delta(n,I)$ del ideal principal de $\mathbb{Z}$ dado por $\mathcal{J}(n,I)\cap\mathbb{Z}$, y llamamos discriminante primitivo asociado a (n, I) a un generador $\Delta_{\rm o}(n,I)$ del ideal principal de $\mathbb{Z}$ dado por $\mathcal{J}_{\rm o}(n,I)\cap\mathbb{Z}$.

El discriminante y el discriminante primitivo —siempre que sean no nulos— están bien definidos salvo el signo; por esta razón en las igualdades de las expresiones que les afecten obviaremos siempre el signo. Dado que $R(s_1,\ldots,s_q)$ pertenece al ideal generado por $N(s_1,\ldots,s_q,t)$ y $N'(s_1,\ldots,s_q,t)$ (ver nota 1.3.1) se tiene que $\Delta_{\rm o}(n,I)$ divide a $\Delta(n,I)$.

El teorema siguiente muestra en particular que $\Delta(n,I)$ es no nulo si y solo si lo es también $\Delta_{\rm o}(n,I)$, puesto que ambas condiciones equivalen a la existencia de algún contraejemplo a la conjetura de Casas-Alvero de un determinado tipo.

Teorema 5.6.2. *Para un grado n y un conjunto de exponentes I dados, son condiciones equivalentes las siguientes:*

(i) $U_{n,I}\big(\mathbb{C}\big)=\emptyset$

(ii) $\Delta(n,I)\neq 0$

(iii) $\Delta_{o}(n,I)\neq 0$.

Demostración. Según la proposición 5.5.4, $U_{n,I}\big(\mathbb{C}\big)=\emptyset$ equivale a que el sistema

$$R(s_1,\ldots,s_q)=N_1(s_1,\ldots,s_q)=\ \cdots\ =N_q(s_1,\ldots,s_q)=0$$

carezca de soluciones sobre $\mathbb{C}$. Por el teorema de los ceros de Hilbert, ello equivale a su vez a que el ideal $\mathcal{J}(n,I)_{\mathbb{C}}$ coincida con $\mathbb{C}[s_1,\ldots,s_q]$, esto es, a que se tenga

$$1=B_0\,R+\sum_{l=1}^{q}B_l\,N_l,\quad \text{con}\ \ B_l\in\mathbb{C}[s_1,\ldots,s_q]\ \ \text{para}\ l=0,1,\ldots,q. \tag{5.22}$$

Argumentando de igual modo que se hizo en la demostración de 3.0.3 se concluye que, en caso de darse una igualdad como la anterior, los polinomios B_l involucrados pueden elegirse con todos sus coeficientes racionales; entonces, tomando el mínimo común múltiplo m de todos sus denominadores y multiplicando por él, (5.22) se reescribe como

$$m=(mB_0)\,R+\sum_{l=1}^{q}(mB_l)\,N_l,\quad \text{con}\ \ mB_l\in\mathbb{Z}[s_1,\ldots,s_q]\ \ \text{para}\ l=0,1,\ldots,q.$$

La existencia de un entero $m\neq 0$ que responda a la expresión anterior caracteriza que $\mathcal{J}(n,I)\cap\mathbb{Z}$ no sea el ideal nulo o, equivalentemente, que su generador $\Delta(n,I)$ sea diferente de cero.

Hemos demostrado $(i)\Leftrightarrow(ii)$; la prueba de $(i)\Leftrightarrow(iii)$ es totalmente paralela, empleando esta vez el sistema (5.20) y los ideales $\mathcal{J}_{\rm o}(n,I)_{\mathbb{C}}$ y $\mathcal{J}_{\rm o}(n,I)$. □

Corolario 5.6.3. *Para un grado n y un conjunto de exponentes I dados, se verifican las condiciones equivalentes del teorema anterior si y solo si, al aplicar el algoritmo de Buchberger al sistema de generadores $\{R, N_1, \ldots, N_q\}$ del ideal $\mathcal{J}(n,I)_{\mathbb{Q}}$ —cualquiera que sea el orden monomial considerado—, se obtiene en alguna de las etapas un polinomio m con multigrado nulo, esto es, $m \in \mathbb{Q}\text{-}\{0\}$.*

Demostración. Se desprende de la demostración del teorema anterior. Cabe destacar que, si la aplicación del algoritmo de Buchberger se atiene a la descripción dada en la subsección 1.3.3, entonces el número racional m que —en su caso— ha de obtenerse es, de hecho, un entero. Se sigue que m pertenece al ideal $\mathcal{J}(n,I) \cap \mathbb{Z}$ y que, por tanto, es un múltiplo del discriminante $\Delta(n,I)$. □

Observación 5.6.4. La eventual existencia de un primo p tal que $\Delta(n,I) \not\equiv 0 \mod p$ garantizaría, no solo que es $U_{n,I}(\mathbb{C}) = \emptyset$ (por el teorema anterior), sino también que es $U_{n,I}(\overline{\mathbb{F}}_p) = \emptyset$. En efecto, también para el cuerpo $\mathbb{K} = \overline{\mathbb{F}}_p$ el teorema de los ceros de Hilbert proporciona la equivalencia entre las condiciones $U_{n,I}(\mathbb{K}) = \emptyset$ y $1 \in \mathcal{J}(n,I)_{\mathbb{K}}$. Entonces, basta tomar una igualdad del tipo

$$\Delta(n,I) = C_0 R + \sum_{l=1}^{q} C_l N_l, \quad \text{con } C_0, C_l \in \mathbb{Z}[s_1, \ldots, s_q]$$

—cuya existencia viene garantizada por la definición de $\Delta(n,I)$— y reducirla módulo p, obteniendo

$$\overline{\Delta}(n,I) = \overline{C}_0 R + \sum_{l=1}^{q} \overline{C}_l N_l, \quad \text{con } \overline{C}_0, \overline{C}_l \in \overline{\mathbb{F}}_p[s_1, \ldots, s_q].$$

Puesto que, por hipótesis, $\overline{\Delta}(n,I) \in \mathcal{J}(n,I)_{\overline{\mathbb{F}}_p}$ es un elemento no nulo de $\overline{\mathbb{F}}_p$, se concluye que 1 pertenece a $\mathcal{J}(n,I)_{\overline{\mathbb{F}}_p}$ y que, por tanto, es $U_{n,I}(\overline{\mathbb{F}}_p) = \emptyset$.

Definición 5.6.5. Para un conjunto de cardinal 1, $I = \{i\}$, definimos el discriminante asociado a los datos (n,I) como el número entero $\Delta(n,I) = 1 - \binom{n}{i}$. Observemos que la condición $\Delta(n,I) \not\equiv 0 \mod p$ es necesaria y suficiente para que $U_{n,I}(\overline{\mathbb{F}}_p) = S_{n,I}(\overline{\mathbb{F}}_p)$ sea vacío, puesto que el esquema sintético $S_{n,\{i\}}$ (cuyos puntos, si los tiene, cumplirán necesariamente $s_1 \neq 0$) viene definido por la ecuación $\left(1 - \binom{n}{i}\right) s_1^n = 0$. La imposibilidad de que ocurra $\Delta(n,I) = 0$ se corresponde con el hecho de que $S_{n,\{i\}}(\mathbb{C})$ es vacío para todo par de grados n, i.

Si existiera un contraejemplo a la conjetura de Casas-Alvero de grado n, para el conjunto I de los grados de los términos distintos del líder con coeficiente no nulo se cumpliría $S_{n,I}(\mathbb{C}) \neq \emptyset$ y también $U_{n,I}(\mathbb{C}) \neq \emptyset$. Más aún, siendo i el mínimo de tales grados y

considerando el conjunto de exponentes $I_i = \{i, i+1, \ldots, n-2\}$, se tendría $U_{n,I_i}(\mathbb{C}) \neq \emptyset$. En consecuencia, el problema de Casas-Alvero en grado n tiene respuesta afirmativa si y solo si se cumple $U_{n,I_i}(\mathbb{C}) = \emptyset$ para todo $i = 1 \ldots, n-2$. El teorema que acabamos de probar traduce esta condición en que sean no nulos todos los discriminantes $\Delta(n, I_i)$ para $i = 1, \ldots, n-2$, esto es, que no se anule el producto de todos ellos. En consecuencia, es válida la siguiente formulación:

Conjetura de Casas-Alvero. *Para cada n se verifica $D_n \neq 0$, siendo $D_n = \prod_{i=1}^{n-2} \Delta(n, I_i)$, según definiciones previas.*

Queda así demostrado, en particular, lo siguiente:

Teorema 5.6.6. *La conjetura de Casas-Alvero admite una formulación en términos de naturaleza aritmética.* □

Nota 5.6.7. El producto de los $n-2$ discriminantes, D_n, puede ser llamado *superdiscriminante*, o discriminante absoluto. Puesto que sabemos, por 2.2.3 y 2.3.4, que no existen contraejemplos a la conjetura con menos de tres términos adicionales al líder, tenemos garantía de que $\Delta(n, I_{n\text{-}2})$ y $\Delta(n, I_{n\text{-}3})$ son siempre distintos de cero. Siendo $n \geq 5$ también es inmediato probar que es $\Delta(n, I_{n\text{-}4}) \neq 0$, pues siempre existe un primo p tal que $\left(I_{n\text{-}4}\right)_p = \emptyset$, deduciéndose entonces del teorema de resolución por interpretación 3.3.1 que tampoco se tienen contraejemplos para $i = n-4$. El primo que nos sirve a este fin es cualquier $p \geq 5$ que divida, bien a n, bien a $n-1$, si es que existe; en caso contrario servirá $p = 2$ o bien $p = 3$, pues entonces n habrá de ser de la forma 2^a o 3^a, dado que necesita ser primo con $n-1$, a su vez de la forma 3^b o 2^b.

Por otra parte, si n es de la forma $p^r + 1$ o $2p^r + 1$, se desprende del teorema 3.6.2 que entonces la sola condición $\Delta(n, I_1) \neq 0$ equivale a que la conjetura de Casas-Alvero sea cierta, pues no son viables contraejemplos sin término de grado 1.

Quiere esto decir que, en general, el rango de valores i para los que la condición $\Delta(n, I_i) \neq 0$ es necesaria para asegurar la conjetura es mucho más pequeño que el del intervalo de números naturales $[1, n-5]$, y se reduce para n general o específico en función del avance de los resultados sobre la conjetura. Con los de esta Memoria se puede, por ejemplo, mejorar también la cota general $n-5$, de modo que el anterior enunciado en términos del superdiscriminante D_n puede afinarse empleando un valor $\widetilde{D}_n$ con bastantes factores menos. De hecho, un *superdiscriminante dinámico* $\widetilde{D}_n$ podría definirse en cada momento como el resultado de suprimir en D_n aquellos factores de quienes hayamos obtenido constancia, por cualquier vía, de que son distintos de cero.

Independientemente de esta posibilidad, el énfasis recae ahora en el hecho de haber descrito para cada n un número cuyo cálculo es en principio factible y tal que su anulación o no equivale a la existencia o no de contraejemplos a la conjetura de Casas-Alvero.

Revisión del caso $r=2$. En el segundo capítulo de esta Memoria se encuentran los resultados 2.2.2 y 2.3.3, que reducen la resolución del I-problema parcial para $r=1$ y $r=2$ a verificar respectivamente que se cumplen las condiciones $1-a\neq 0$ y $(1-a)(1-b)\,\Delta\neq 0$, donde

$$\Delta = a^{\,\rho}\,(b-c)^{\rho}(b-ac)^{\sigma} - (-1)^{\sigma}(a-1)^{\rho+\sigma}(b-1)^{\rho} \tag{5.23}$$

para los enteros a, b, c, ρ, σ en 2.3.3 asociados a la terna n, i, j. Recordemos que la prueba de $\Delta\neq 0$ es existencial; consiste en demostrar que existen primos p tales que $\Delta\not\equiv 0 \mod p$. A continuación se muestra la relación entre este Δ de (5.23) y el discriminante $\Delta\big(n;\{i,j\}\big)$ cuya no anulación caracteriza, en virtud de 5.6.2 y 5.5.4, la no existencia de soluciones para el sistema de ecuaciones $N(t)=N'(t)=0$ que proporciona las coordenadas afines de aquellos puntos de la variedad proyectiva $S_{n,\{i,j\}}\big(\mathbb{C}\big)$ ubicados en la carta local $s_2\neq 0$; esto es, la no existencia de $\{i,j\}$-contraejemplos con $a_{n\text{-}i}\neq 0$ para el problema de Casas-Alvero de grado n.

Teorema 5.6.8. *Para $I=\{i,j\}$ se tiene la igualdad*

$$\Delta(n,I) = (a-1)^{\,i}\,(e-1)^{n\text{-}j}\;\Delta^{d},$$

donde $e=\binom{j}{i}$, $d=\text{m.c.d.}(n-j,j-i)$, *y* Δ *obedece a la expresión (5.23).*

Demostración. Siendo en este caso $q=0$, se tiene $\mathcal{J}(n,I)=\langle R\rangle$ con $R=\text{Res}\big(N(t),N'(t)\big)\in\mathbb{Z}$, de modo que el discriminante $\Delta(n,I)$ no es otro que el número R. Como puede comprobarse, se cumple

$$N(t)=t^{\,i}\cdot\widetilde{N}(t),\quad \text{con}\quad \widetilde{N}(t)=(1-e)\,t^{\,n\text{-}i}+(a-1)\,t^{\,j\text{-}i}+(e-a);$$

mientras que es $N'(t)=b(1-e)\,t^{\,n-j}+(a-1)$ (debe advertirse que este polinomio no es la derivada del anterior). Así pues,

$$R=\text{Res}\big(t,N'(t)\big)^{\,i}\cdot\text{Res}\big(\widetilde{N}(t),N'(t)\big)=(a-1)^{\,i}\cdot\text{Res}\big(\widetilde{N}(t),N'(t)\big).$$

El cálculo $\text{Res}\big(\widetilde{N}(t),N'(t)\big)$ se conduce, mediante la sustracción de las $n-j$ primeras filas multiplicadas por b a las $n-j$ filas siguientes en la matriz correspondiente, y el desarrollo del determinante por las primeras $n-j$ columnas (ya con un único elemento no nulo) a una situación en la que procede aplicar el lema 2.3.1. Teniendo en cuenta que $(-1)^{\rho\sigma+\rho}$ coincide necesariamente con $(-1)^{\sigma+1}$ (pues solo diferirían en caso de ser pares tanto ρ como σ, algo imposible por ser primos entre sí) se obtiene de inmediato

$$\mathrm{Res}\big(\widetilde{N}(t), N'(t)\big) = (e-1)^{n\text{-}j}\ \Delta^d,$$

tal como se requiere para la verificación del teorema. □

Caso particular $r=3$. Para un conjunto de exponentes $I=\{i,j,k\}$ se tiene $q=r-2=1$, y el sistema (5.21) toma la forma $N_1(s_1)=R(s_1)=0$. Podemos comprobar que es

$$N_1(s_1) = \Big(1-\tbinom{j}{i}\Big)\Big(1-\tbinom{n}{k}\Big)\, s_1^n + (\text{términos de menor grado}),$$
$$R(s_1) = \mathrm{Res}_t\big(N(s_1,t)\,,\, N'(s_1,t)\big),$$

donde, a su vez,

$$N(s_1,t) = \Big(1-\tbinom{j}{i}\Big)\, t^n + (\text{términos de menor grado en } t) \in \mathbb{Z}[s_1][t]$$
$$N'(s_1,t) = \Big(1-\tbinom{j}{i}\Big)\tbinom{n}{j}\, t^{n\text{-}j} + (\text{términos de menor grado en } t) \in \mathbb{Z}[s_1][t].$$

Además del discriminante $\Delta(n,I)$, generador del ideal principal $\big\langle N_1(s_1), R(s_1)\big\rangle \cap \mathbb{Z}$, nos interesará considerar el valor

$$\delta(n,I) = \mathrm{Res}_{s_1}\big(R(s_1), N_1(s_1)\big).$$

Observación 5.6.9. Las desigualdades $\Delta(n,I)\neq 0$ y $\delta(n,I)\neq 0$ son dos caracterizaciones independientes de la inexistencia de $\{i,j,k\}$-contraejemplos al problema de Casas-Alvero de grado n. Así lo establecen las proposiciones 5.6.2 y 5.5.4 (pues $\delta(n,I)\neq 0$ equivale a que $N_1(s_1)=R(s_1)=0$ carezca de soluciones en $\mathbb{C}$), y el hecho de que $S_{n,I}\big(\mathbb{C}\big)$ no admita puntos que queden fuera de $U_{n,I}\big(\mathbb{C}\big)$, ya que corresponderían a contraejemplos con solo dos términos adicionales al líder.

En particular, $\Delta(n,I)$ será nulo si y solo si lo es $\delta(n,I)$. A diferencia de lo que ocurre con $\Delta(n,I)$, para calcular $\delta(n,I)$ disponemos de una fórmula explícita.

Dados cualesquiera dos polinomios $f(s), g(s)\in\mathbb{Z}[s]$ de grado positivo, los enteros $\Delta_{f,g}$ y $\delta_{f,g}$ definidos por $\big\langle \Delta_{f,g}\big\rangle = \big\langle f(s), g(s)\big\rangle \cap \mathbb{Z}$ y $\delta_{f,g}=\mathrm{Res}\big(f(s),g(s)\big)$ no son necesariamente iguales, aunque sabemos por 1.3.1 que $\Delta_{f,g}$ siempre divide a $\delta_{f,g}$; así por ejemplo, siendo $f(s)=3s+2$, $g(s)=3s+4$ se tiene $\Delta_{f,g}=2$ ya que $2=-f(s)+g(s)$, mientras que es $\delta_{f,g}=6$. En general se verifica, además, el resultado siguiente:

Lema 5.6.10. *Sea μ el máximo común divisor de los coeficientes líderes de $f(s)$ y de $g(s)$, y sea p un primo arbitrario. Se cumple la doble implicación*

$$p\,|\,\delta_{f,g} \iff p\,|\,\mu \ \text{ o bien } \ p\,|\,\Delta_{f,g}$$

Demostración. Por simplicidad se omiten los subíndices f,g en la escritura de esta prueba. La implicación hacia la izquierda es obvia; veamos su recíproca. Por la definición de Δ

existen $h(s), q(s) \in \mathbb{Z}[s]$ tales que $\Delta = f(s)\,h(s) + g(s)\,q(s)$. Sean n, m, u, v los respectivos grados de f, g, h y q, y sean a_0 y b_0 los coeficientes líderes de f y de g, de modo que sobre el cuerpo adecuado se puede escribir $f(s) = a_0 \prod_{i=1}^{n}(s-\alpha_i)$ y $g(s) = b_0 \prod_{i=1}^{m}(s-\beta_i)$. Empleando esta factorización, y gracias al comportamiento multiplicativo de la resultante, se obtiene

$$\begin{aligned}\operatorname{Res}\big(f(s)\cdot h(s), g(s)\big) = \operatorname{Res}\big(\Delta - g(s)\,q(s), g(s)\big) &= b_0^{n+u} \prod_{i=1}^{m} \operatorname{Res}\big(\Delta - g(s)\,q(s), s-\beta_i\big) = \\ &= b_0^{n+u} \prod_{i=1}^{m} \big[\Delta - g(\beta_i)\,q(\beta_i)\big];\end{aligned}$$

esto es, en definitiva,

$$\begin{aligned}\delta \cdot \operatorname{Res}\big(h(s), g(s)\big) &= b_0^{n+u}\,\Delta^m \quad \text{y, de forma simétrica,} \\ \delta \cdot \operatorname{Res}\big(q(s, f(s)\big) &= a_0^{m+v}\,\Delta^n.\end{aligned} \tag{5.24}$$

Sea p un divisor primo de δ; si p no divide a μ entonces no divide a a_0, o bien no divide a b_0. De (5.24) se deduce que entonces p divide a Δ, como se quería probar. □

Teorema 5.6.11. *Sea $I = \{i, j, k\}$; sean $\Delta(n, I)$ y $\delta(n, I)$ según definiciones previas. Entonces, para todo primo p se verifica*

$$\delta(n, I) \not\equiv 0 \mod p \quad \Longleftrightarrow \quad \Delta(n, I) \not\equiv 0 \mod p \;\; y \;\; \mu \not\equiv 0 \mod p,$$

siendo μ el máximo común divisor de los coeficientes de los términos líder de $R(s_1)$ y $N_1(s_1)$.

Demostración. Es aplicación directa del lema anterior a los polinomios $R(s_1)$ y $N_1(s_1)$. □

Siguiendo la misma táctica que en 2.3.4, para probar que $\delta(n, I)$ es distinto de cero bastaría demostrar la existencia de un número primo p tal que $\delta(n, I) \not\equiv 0 \bmod p$, y lo mismo puede decirse respecto de $\Delta(n, I)$. El teorema anterior garantiza que el conjunto de primos útiles a dicho fin es el mismo en ambos casos, excepción hecha de los divisores primos de μ (quienes, por otra parte, no están incontrolados pues son, en particular, divisores de $\left(1 - \binom{j}{i}\right) \cdot \left(1 - \binom{n}{k}\right)$, coeficiente líder de $N_1(s_1)$).

Observación 5.6.12. El teorema anterior permite encontrar de modo efectivo los primos ineficaces de nivel 3 para valores asequibles de h. En efecto, con la única posible excepción de aquellos primos que dividan a $1 - \binom{j}{i}$ (los demás divisores de μ, por serlo de $1 - \binom{n}{k}$ se encontrarían en el nivel 1), son primos ineficaces de nivel máximo —si no lo fueran ya

de nivel uno o dos— justamente los divisores primos de $\Delta(n,I)$, o equivalentemente, de $\delta(n,I)$, el cual es computable a través de la fórmula de la resultante. Con este criterio, y si se requiere, las tablas que siguen a la proposición 4.4.6 pueden completarse con el nivel 3 para los primeros valores de h.

Ejemplo. Tomamos $n=5$, $I=\{1,2,3\}$. Entonces se tiene

$$\Delta\big(5;\{3\}\big) = \tbinom{5}{3}-1 = 3^2, \qquad \text{por la definición 5.6.5,}$$

$$\Delta\big(5;\{2,3\}\big) = 2^2\cdot 3^2\cdot 11\cdot 3541, \qquad \text{por el teorema 5.6.8, y}$$

$$\delta\big(5;\{1,2,3\}\big) = 2^{24}\cdot 3^6\cdot 7^3\cdot 131\cdot 193\cdot 599^2\cdot 8009, \quad \text{resultante de } R \text{ y } N_1.$$

Los polinomios R y N_1 en cuestión son

$$\begin{aligned} R(s_1) &= 64\cdot(1-5s_1^2)\cdot(5s_1^2-3)\cdot(2450s_1^4-1445s_1^2+193) \\ N_1(s_1) &= -s_1\,(s_1-1)^2\cdot(9s_1^2-2s_1-3), \end{aligned}$$

y, por tanto, el valor de μ es 1. Del teorema anterior se deduce, pues, que los primos que dividen al discriminante $\Delta\big(5;\{1,2,3\}\big)$ son exactamente los divisores de $\delta\big(5;\{1,2,3\}\big)$, es decir, 2, 3, 7, 131, 193, 599, 8009. Se trata de siete de los nueve primos ineficaces para $n=5$. Los otros dos primos ineficaces con $n=5$, que son 11 y 3541, aparecen en $\Delta\big(5;\{2,3\}\big)$.

En el ejemplo anterior hemos podido observar la coincidencia entre el conjunto de los primos ineficaces con 5 y el conjunto de los primos que dividen al superdiscriminante $D_5=\Delta\big(5;\{3\}\big)\cdot\Delta\big(5;\{2,3\}\big)\cdot\Delta\big(5;\{1,2,3\}\big)$, comportamiento que también se produce con $n=3$ y $n=4$. Un resultado general, en este sentido, es el que garantiza una de las dos inclusiones. Está dado con el siguiente teorema, con el cual concluye esta Memoria.

Teorema 5.6.13. *Sea $n\geq 3$ un número entero, y sea $p\geq n$ un número primo.*

(*a*) *Si p no divide a D_n, entonces p es eficaz para n, y la conjetura de Casas-Alvero es cierta para los grados np^r, con $r\geq 0$.*

(*b*) *Si p no divide a $\widetilde{D}_n$, entonces la conjetura de Casas-Alvero es cierta en grado n.*

Demostración. (*a*): Como p no divide a D_n, tampoco divide al discriminante $\Delta(n,I_i)$ para ningún $i=1,\ldots,n-2$, lo cual implica que todos los conjuntos $U_{n,I_i}\big(\overline{\mathbb{F}}_p\big)$ son igual al vacío (ver observación 5.6.4, y reparar en que, siendo $1-\binom{j}{i}=i<p$, no hay obstrucción a la aplicación de este criterio).

Queda así probado que es $S_{n,J}\big(\overline{\mathbb{F}}_p\big) = \bigcup_{i=1}^{n-2} U_{n,I_i}\big(\overline{\mathbb{F}}_p\big) = \emptyset$ y, por tanto, que p es eficaz para n; basta ahora aplicar el principio de expansión enunciado en 4.3.

(b): El valor de $\widetilde{D}_n$ que estemos considerando en determinado momento es el producto, justamente, de aquellos factores $\Delta(n, I_i)$ presentes en D_n para los que no se hubiera establecido previamente la igualdad $U_{n,I_i}\big(\mathbb{C}\big) = \emptyset$, esto es, para los que no se hubiera demostrado que el correspondiente discriminante $\Delta(n, I_i)$ sea un entero distinto de cero. Pero al saber que el primo p no divide a ninguno de tales discriminantes, concluimos que, efectivamente, también para todos ellos es $\Delta(n, I_i) \neq 0$, de donde resulta $S_{n,J}\big(\mathbb{C}\big) = \bigcup_{i=1}^{n-2} U_{n,I_i}\big(\mathbb{C}\big) = \emptyset$; esto prueba Casas-Alvero para el grado n. Obsérvese que, sin embargo, pudiera ocurrir que alguno de los discriminantes $\Delta(n, I_i)$ que estaban ausentes del producto $\widetilde{D}_n$ fuera múltiplo de p; no podemos por tanto, con estas hipótesis, garantizar que p sea un primo eficaz para el grado n. □

Bibliografía

[A-M] Atiyah, M.F.; Macdonald, I.G.: *Introducción al Álgebra Conmutativa*. Reverté (1969)

[BLSW] Bothmer, H.-C.; Labs, O.; Schicho, J.; Woestijne, C.: *The Casas-Alvero Conjecture for infinitely many degrees*. J. Algebra **366**, 224 - 230 (2007).

[Cas] Casas-Alvero, E.: *Higher order polars*. J. of Algebra **240**, 326-377 (2001).

[C-S] Chellali, M.; Salinier, A.: *La conjecture de Casas-Alvero pour degree* 5^e. Preprint 2012.

[CLO-1] Castryck, W.; Lauterveer, R.; Ounaïes, M: *Constraints on counterexamples to the Casas-Alvero conjecture, and verification on degree 12*. ArXiv 1208. 5404v1 [Math.AG]. August 27, 2012.

[CLO-2] Castryck, W.; Lauterveer, R.; Ounaïes, M: *CA bad primes for degree 7*. Avalaible at https://perswww.kuleuven.be./~u0040935/badprimes7.txt

[CLS] Cox, D.; Little, J.; O'Shea, D.: *Ideals, Varieties and Algorithms*. Springer-Verlag (1992)

[C-S] Chellali, M.; Salinier, A.: *La conjecture de Casas-Alvero pour degree* 5^e. Preprint 2012.

[D-G] Díaz-Toca, G.; González-Vega, L.: *On analyzing a conjecture about univariable polynomials and their roots by using Maple*. Proceedings on the Maple Conference 2006. Waterloo (Canada), July 23-26 (2006).

[D-J] Draisma, J.; Jong, J.P.: *On the Casas-Alvero conjecture*. Feature. EMS Newsletter **80**, 29 - 33, June 2011. Erratum avalaible at http://www.win.tue.nl/~jdraisma/

[Fru1] Frutos-Marín, R. : *Sobre polinomios que comparten una raíz con cada una de sus derivadas*. Trabajo presentado para obtener el Diploma de Estudios Avanzados del programa de doctorado en Matemáticas. Universidad de Valladolid (2005)

[Fru2] Frutos-Marín, R. : *Polynomials sharing roots with its derivatives*. Conferencias en "Thematic Seminar on Singularities, Algebraic Geometry, Computing and Information". Segovia 15/10/2009, y en "Seminario de Geometría Tórica, VI", Jarandilla de la Vera, 14/11/2009.

[Jon] Jong, J.P. : *Het Casas-Alvero conjecture*. 19 - 04 - 2010.

[Lan] Lang, S.: *Algebra*. Graduate texts in Mathematics. Springer (2002).

[L-O] Lauterveer, R.; Ounaïes, M : *Constraints on hypothetical counterexamples to the Casas-Alvero conjecture*. ArXiv 1204.0450 [mathCV] (2012).

[Sam] Samuel, P.: *Théorie Algébrique des Nombres*. Herrmann, Paris (1997).

[Ser] Serre, J.P.: *Cours d'Arithmetique*. Presses Universitaires de France, Paris (1995).

[Ver] Verhoeck, H.: *Some remarks about a polynomial conjecture of Casas-Alvero*. Seminaire Bourbakettes, Paris (2009).

[Woe] Woestijne, C. Czech and Slovak International Conference on Number Theory. Slará Lesná, September 6, 2011. Avalaible at http://www.opt.math.tugraz.at/˜cvdwoest/maths/talk-lesna.pdf

Índice alfabético