CAPÍTULO VII

Polinomios en varias variables. Polinomios simétricos. Resultante y discriminante

En la primera sección de este capítulo se introducen nociones generales y resultados básicos sobre polinomios en varias variables, lo que incluye en particular las Fórmulas de Cardano-Vieta y la demostración del Teorema de representación de los polinomios simétricos. Utilizamos este teorema en la sección segunda para definir y estudiar algunas propiedades de la resultante y el discriminante, que empleamos para presentar una demostración del Teorema de los ceros de Hilbert que sólo usa argumentos de Álgebra Lineal.

1. Generalidades. Polinomios simétricos

Comenzamos esta sección introduciendo el concepto de *anillo de polinomios en varias variables* con coeficientes en un anillo A y estudiando algunas propiedades básicas.

Definición y Proposición VII.1.1 Sea A un anillo conmutativo y unitario. Denotamos $\mathbb{N}$ el conjunto de los enteros no negativos y sea $A[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ el conjunto de todas las funciones $f : \mathbb{N}^n \to A$ tales que $f(\nu) \neq 0$ tan sólo para una cantidad finita de elementos $\nu \in \mathbb{N}^n$.

(1) $A[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ *es un anillo conmutativo y unitario con las operaciones suma y producto definidas por*

$$(f+g)(\nu) := f(\nu) + g(\nu) \quad \& \quad (fg)(\nu) := \sum_{\mu+\rho=\nu} f(\mu)g(\rho),$$

donde $f, g \in A[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ *y* $\nu, \mu, \rho \in \mathbb{N}^n$.

(2) *La aplicación* $A \hookrightarrow A[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ *dada por* $a \mapsto f_a$, *donde* $f_a(0) = a$ *y* $f_a(\nu) = 0$ *para* $\nu \neq 0$, *es un monomorfismo de anillos.*

Demostración. (1) La comprobación de que $A[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ es un anillo conmutativo y unitario es rutinaria y pesada; por eso la omitimos. Señalemos que, con las notaciones del apartado (2), el elemento neutro para la suma es la función f_0 y el elemento unidad es f_1.

(2) La comprobación de este apartado es también inmediata.

El anillo $A[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ recibe el nombre de *anillo de polinomios en n indeterminadas* o *variables* sobre A. En virtud de VII.1.1 (2) consideraremos A como subanillo de $A[\mathtt{x}_1, \ldots, \mathtt{x}_n]$, identificando cada $a \in A$ con f_a. □

Observaciones VII.1.2 (1) Si $n = 1$, entonces $A[\mathtt{x}_1]$ es el anillo de polinomios en una variable descrito en V.1.1.

(2) Introducimos una notación más conveniente para tratar los anillos de polinomios en varias variables. Fijado $n \geq 1$, denotamos

$$e_i := (0, \ldots, 0, \overset{i)}{1}, 0, \ldots, 0) \in \mathbb{N}^n.$$

Para cada $k \in \mathbb{N}$ definimos $ke_i := (0, \ldots, 0, \overset{i)}{k}, 0, \ldots, 0)$, y así cada multiíndice $\nu \in \mathbb{N}^n$ se expresa de forma única como $\nu := (\nu_1, \ldots, \nu_n) = \nu_1 e_1 + \cdots + \nu_n e_n$. Se llama *peso* de ν a la suma $|\nu| := \nu_1 + \cdots + \nu_n$.

Sean A un anillo y $n \geq 1$ un entero positivo. Para $1 \leq i \leq n$ consideramos $\mathtt{x}_i \in A[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ dada por

$$\mathtt{x}_i(e_i) = 1 \quad \& \quad \mathtt{x}_i(\nu) = 0 \text{ si } \nu \neq e_i.$$

Además, dados $1 \leq i \leq n$ y $k \in \mathbb{N}$, de la definición de producto se deduce que

$$\mathtt{x}_i^k(ke_i) = 1 \quad \& \quad \mathtt{x}_i^k(\nu) = 0 \text{ si } \nu \neq ke_i.$$

Dado un multiíndice $\nu = (\nu_1, \ldots, \nu_n)$ definimos $\mathtt{x}^\nu := \mathtt{x}_1^{\nu_1} \cdots \mathtt{x}_n^{\nu_n}$, que cumple

$$\mathtt{x}^\nu(\nu) = \mathtt{x}_1^{\nu_1} \cdots \mathtt{x}_n^{\nu_n}(\nu) = 1 \quad \& \quad \mathtt{x}^\nu(\mu) = 0 \quad \forall\, \mu \in \mathbb{N}^n \setminus \{\nu\}.$$

(3) Sean $f \in A[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ y el conjunto finito $\mathcal{F}_f := \{\nu \in \mathbb{N}^n : f(\nu) \neq 0\}$. Denotando $a_\nu := f(\nu)$ para cada $\nu \in \mathcal{F}_f$ se escribe

$$f = \sum_{\nu \in \mathcal{F}_f} a_\nu \mathtt{x}^\nu, \text{ lo que abreviamos } f = \sum_{\nu} a_\nu \mathtt{x}^\nu.$$

Se dice que $\mathtt{x}_1, \ldots, \mathtt{x}_n \in A[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ son las *indeterminadas* o *variables* del anillo de polinomios $A[\mathtt{x}_1, \ldots, \mathtt{x}_n]$. Los elementos a_ν de la expresión precedente son los *coeficientes* de f; por supuesto,

$$\sum_\nu a_\nu \mathtt{x}^\nu = \sum_\nu b_\nu \mathtt{x}^\nu \quad \Longleftrightarrow \quad a_\nu = b_\nu \quad \forall\ \nu.$$

Un polinomio del tipo $a\mathtt{x}^\nu$ para cierto $\nu \in \mathbb{N}^n$ recibe el nombre de *monomio*. Este monomio se dice *nulo* si $a = 0$. Todo polinomio no nulo se escribe de modo único como suma de una cantidad finita de monomios no nulos. Nótese que si $1 \leq i_1 < \cdots < i_r \leq n$, el anillo $A[\mathtt{x}_{i_1}, \ldots, \mathtt{x}_{i_r}]$ se puede interpretar como un subanillo de $A[\mathtt{x}_1, \ldots, \mathtt{x}_n]$; para ello basta considerar las variables $\mathtt{x}_j$ con $j \notin \{i_1, \ldots, i_r\}$ elevadas al exponente 0 en todos los monomios no nulos de los polinomios de $A[\mathtt{x}_{i_1}, \ldots, \mathtt{x}_{i_r}]$.

Definición y Observación VII.1.3 (Evaluación) Sean A y B anillos tales que A es subanillo de B. Sea $b := (b_1, \ldots, b_n) \in B^n$ y consideramos la aplicación

$$\mathrm{ev}_b : A[\mathtt{x}_1, \ldots, \mathtt{x}_n] \to B,\ f = \sum_\nu a_\nu \mathtt{x}^\nu \mapsto f(b) = \sum_\nu a_\nu b^\nu := \sum_\nu a_\nu b_1^{\nu_1} \cdots b_n^{\nu_n}.$$

Se comprueba sin dificultad que la aplicación ev_b es un homomorfismo, que denominaremos *homomorfismo evaluación*, que cumple que $\mathrm{ev}_b\,|_A = \mathrm{id}_A$ y $\mathrm{ev}_b(\mathtt{x}_i) = b_i$. Además, la imagen de ev_b, que denotaremos por $A[b_1, \ldots, b_n]$, es el menor subanillo de B que contiene al anillo A y a $b_1, \ldots, b_n$. Por el Primer Teorema de isomorfía II.2.1 se cumple que

$$A[\mathtt{x}_1, \ldots, \mathtt{x}_n]/\ker \mathrm{ev}_b \cong A[b_1, \ldots, b_n].$$

Corolario VII.1.4 *Sean A un anillo y $n \geq 1$ un entero positivo. Fijado un índice k, donde $1 \leq k \leq n$, existen isomorfismos de anillos*

$$A[\mathtt{x}_1, \ldots, \mathtt{x}_k][\mathtt{x}_{k+1}, \ldots, \mathtt{x}_n] \cong A[\mathtt{x}_1, \ldots, \mathtt{x}_n] \cong A[\mathtt{x}_{k+1}, \ldots, \mathtt{x}_n][\mathtt{x}_1, \ldots, \mathtt{x}_k].$$

Demostración. Veremos que $A[\mathtt{x}_1, \ldots, \mathtt{x}_k][\mathtt{x}_{k+1}, \ldots, \mathtt{x}_n] \cong A[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ pues el otro isomorfismo se obtiene análogamente. Como $A[\mathtt{x}_1, \ldots, \mathtt{x}_k] \subset A[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ existe, por VII.1.3, un homomorfismo de anillos

$$\varphi : A[\mathtt{x}_1, \ldots, \mathtt{x}_k][\mathtt{x}_{k+1}, \ldots, \mathtt{x}_n] \to A[\mathtt{x}_1, \ldots, \mathtt{x}_n]$$

tal que $\varphi|_{A[\mathtt{x}_1, \ldots, \mathtt{x}_k]} = \mathrm{id}_{A[\mathtt{x}_1, \ldots, \mathtt{x}_k]}$ y $\varphi(\mathtt{x}_j) = \mathtt{x}_j$ para $k+1 \leq j \leq n$.

Por otro lado, como $A \subset A[\mathtt{x}_1, \ldots, \mathtt{x}_k][\mathtt{x}_{k+1}, \ldots, \mathtt{x}_n]$ existe, por VII.1.3, un homomorfismo de anillos

$$\psi : A[\mathtt{x}_1, \ldots, \mathtt{x}_n] \to A[\mathtt{x}_1, \ldots, \mathtt{x}_k][\mathtt{x}_{k+1}, \ldots, \mathtt{x}_n]$$

tal que $\psi|_A = \mathrm{id}_A$ y $\psi(\mathtt{x}_j) = \mathtt{x}_j$ para $1 \leq j \leq n$. Nótese que

$$(\psi \circ \varphi)|_A = \mathrm{id}_A \quad \& \quad (\psi \circ \varphi)(\mathtt{x}_j) = \mathtt{x}_j \quad \forall\ 1 \leq j \leq n,$$

y por tanto, $\psi \circ \varphi = \mathrm{id}_{A[\mathtt{x}_1,\ldots,\mathtt{x}_k][\mathtt{x}_{k+1},\ldots,\mathtt{x}_n]}$. Análogamente, $\varphi \circ \psi = \mathrm{id}_{A[\mathtt{x}_1,\ldots,\mathtt{x}_n]}$, luego φ es un isomorfismo. □

En lo sucesivo actuaremos como si los isomorfismos de la Proposición anterior fuesen identidades, por lo que escribiremos

$$\begin{aligned} A[\mathtt{x}_1, \ldots, \mathtt{x}_k][\mathtt{x}_{k+1}, \ldots, \mathtt{x}_n] &= A[\mathtt{x}_1, \ldots, \mathtt{x}_n] \\ &= A[\mathtt{x}_{k+1}, \ldots, \mathtt{x}_n][\mathtt{x}_1, \ldots, \mathtt{x}_k] = A[\mathtt{x}_1][\mathtt{x}_2] \cdots [\mathtt{x}_n]. \end{aligned}$$

Definición y Observaciones VII.1.5 (Grado de un polinomio) (1) Dado un polinomio no nulo $f = \sum_\nu a_\nu \mathtt{x}^\nu \in A[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ se llama *grado,* o *grado total,* de f a $\deg(f) := \max\{|\nu| : a_\nu \neq 0\}$. Si $f = 0$ se conviene que $\deg(f) := -\infty$. El operador grado cumple las siguientes propiedades, en cuya formulación suponemos el convenio habitual:

$$(-\infty) + (-\infty) = -\infty,\ \ (-\infty) + n = -\infty \ \ \& \ \ -\infty \leq n\ \ \forall\ n \in \mathbb{Z}.$$

(1) Si $f, g \in A[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ entonces $\deg(f + g) \leq \max\{\deg(f), \deg(g)\}$, y si $\deg(f) \neq \deg(g)$ entonces $\deg(f + g) = \max\{\deg(f), \deg(g)\}$.

(2) Si $f, g \in A[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ entonces $\deg(fg) \leq \deg(f) + \deg(g)$. Además, si A es un dominio se cumple la igualdad $\deg(fg) = \deg(f) + \deg(g)$.

(3) Para $1 \leq i \leq n$ denotamos $B := A[\mathtt{x}_1, \ldots, \mathtt{x}_{i-1}, \mathtt{x}_{i+1}, \cdots, \mathtt{x}_n]$, luego

$$A[\mathtt{x}_1, \ldots, \mathtt{x}_n] = A[\mathtt{x}_1, \ldots, \mathtt{x}_{i-1}, \mathtt{x}_{i+1}, \cdots, \mathtt{x}_n][\mathtt{x}_i] = B[\mathtt{x}_i],$$

y dado $f \in A[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ se define el *grado de f con respecto a la variable* $\mathtt{x}_i$, que se denota $\deg_{\mathtt{x}_i}(f)$, como su grado como polinomio en $B[\mathtt{x}_i]$, que por tanto cumple las propiedades relativas al grado de los polinomios en una variable descritas en la sección primera del Capítulo V.

(4) Un polinomio $f \in A[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ es *homogéneo* si todos sus monomios no nulos tienen el mismo grado. Por convenio consideramos que también el polinomio nulo es homogéneo. Si f es homogéneo de grado d se tiene la igualdad

$$f(\mathtt{t}\mathtt{x}_1, \ldots, \mathtt{t}\mathtt{x}_n) = \mathtt{t}^d f(\mathtt{x}_1, \ldots, \mathtt{x}_n) \tag{1.1}$$

como polinomios en $A[\mathtt{x}_1, \ldots, \mathtt{x}_n, \mathtt{t}]$. En efecto, cada monomio $g \in A[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ de grado d se escribe como $g := a\mathtt{x}_1^{\nu_1} \cdots \mathtt{x}_n^{\nu_n}$ donde $\nu_1 + \cdots + \nu_n = d$, luego

$$\begin{aligned} g(\mathtt{tx}_1, \ldots, \mathtt{tx}_n) &= a(\mathtt{tx}_1)^{\nu_1} \cdots (\mathtt{tx}_n)^{\nu_n} \\ &= \mathtt{t}^{\nu_1+\cdots+\nu_n} a\mathtt{x}_1^{\nu_1} \cdots \mathtt{x}_n^{\nu_n} = \mathtt{t}^d g(\mathtt{x}_1, \ldots, \mathtt{x}_n). \end{aligned}$$

En consecuencia, si $f = g_1 + \cdots + g_r$ es suma de monomios de grado d se tiene

$$\begin{aligned} f(\mathtt{tx}_1, \ldots, \mathtt{tx}_n) &= \sum_{i=1}^{r} g_i(\mathtt{tx}_1, \ldots, \mathtt{tx}_n) \\ &= \mathtt{t}^d \sum_{i=1}^{r} g_i(\mathtt{x}_1, \ldots, \mathtt{x}_n) = \mathtt{t}^d f(\mathtt{x}_1, \ldots, \mathtt{x}_n). \end{aligned}$$

(5) Cada polinomio $f \in A[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ se escribe, de modo único, como suma $f = \sum_{k=0}^{d} f_k$ donde $d = \deg(f)$ y cada f_k es un polinomio homogéneo de grado k o el polinomio nulo. Los polinomios f_k están determinados por f y reciben el nombre de *componentes homogéneas de* f. La componente f_k, si no es nula, es la suma de los monomios de f de grado k. Por lo visto en (4),

$$f(\mathtt{tx}_1, \ldots, \mathtt{tx}_n) = \sum_{k=0}^{d} f_k(\mathtt{tx}_1, \ldots, \mathtt{tx}_n) = \sum_{k=0}^{d} \mathtt{t}^k f_k(\mathtt{x}_1, \ldots, \mathtt{x}_n),$$

que no coincide con $\mathtt{t}^d f(\mathtt{x}_1, \ldots, \mathtt{x}_n) = \mathtt{t}^d \sum_{k=0}^{d} f_k(\mathtt{x}_1, \ldots, \mathtt{x}_n)$ salvo si $f_k = 0$ para $0 \leq k < d$. Así, la igualdad (1.1) caracteriza, entre los polinomios no nulos, los homogéneos de grado d.

(6) El producto de dos polinomios homogéneos es, bien nulo, bien un polinomio homogéneo. En efecto, si f y g son polinomios homogéneos de grados d y e, respectivamente, su producto $h := fg$ o bien es nulo o bien es homogéneo de grado $d + e$, ya que

$$\begin{aligned} h(\mathtt{tx}_1, \ldots, \mathtt{tx}_n) &= f(\mathtt{tx}_1, \ldots, \mathtt{tx}_n) \cdot g(\mathtt{tx}_1, \ldots, \mathtt{tx}_n) \\ &= \mathtt{t}^d f(\mathtt{x}_1, \ldots, \mathtt{x}_n) \cdot \mathtt{t}^e g(\mathtt{x}_1, \ldots, \mathtt{x}_n) = \mathtt{t}^{d+e} h(\mathtt{x}_1, \ldots, \mathtt{x}_n). \end{aligned}$$

Corolario VII.1.6 *Sean A un anillo y $n \geq 1$. Se cumplen las siguientes propiedades.*

(1) *A es un dominio si y sólo si $A[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ es un dominio.*

(2) *Si A es un dominio, entonces $\mathcal{U}(A) = \mathcal{U}(A[\mathtt{x}_1, \ldots, \mathtt{x}_n])$.*

(3) *A es noetheriano si y sólo si $A[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ es noetheriano.*

(4) *A es un* DFU *si y sólo si $A[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ es un* DFU. *En particular, si K es un cuerpo, entonces $K[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ es un* DFU.

(5) *Las condiciones siguientes son equivalentes.*

(5.1) *$A[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ es un* DE.

(5.2) *$A[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ es un* DIP.

(5.3) *A es un cuerpo y $n = 1$.*

Demostración. Los apartados (1) y (2) se deducen de la Proposición V.1.2 empleando la igualdad $A[\mathtt{x}_1, \ldots, \mathtt{x}_n] = A[\mathtt{x}_1, \ldots, \mathtt{x}_{n-1}][\mathtt{x}_n]$ y argumentando por inducción.

Los apartados (3) y (4) se siguen del Teorema de la base de Hilbert, V.2.15, y del Teorema de Gauss, VI.1.6, argumentando por inducción y utilizando de nuevo que $A[\mathtt{x}_1, \ldots, \mathtt{x}_n] = A[\mathtt{x}_1, \ldots, \mathtt{x}_{n-1}][\mathtt{x}_n]$.

Por último, el apartado (5) se deduce de la Proposición V.1.8 utilizando la igualdad $A[\mathtt{x}_1, \ldots, \mathtt{x}_n] = B[\mathtt{x}_n]$ donde $B := A[\mathtt{x}_1, \ldots, \mathtt{x}_{n-1}]$ es un cuerpo si y sólo si A es un cuerpo y $n = 1$, es decir, no hay variables. □

Definición y Observación VII.1.7 (Funciones polinómicas) (1) Sean A un anillo, $n \geq 1$ y $f \in A[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ un polinomio no nulo. La *función polinómica* asociada a f se define como

$$F : A^n \to A,\ a \mapsto f(a) = \mathrm{ev}_a(f).$$

La función polinómica asociada a un polinomio no nulo puede ser nula. Por ejemplo, si p es un número primo, $A = \mathbb{Z}_p$ y $n = 1$, el polinomio $f = \mathtt{t}^p - \mathtt{t}$ no es nulo, pero la función polinómica asociada a f sí es nula, por el Pequeño Teorema de Fermat, **??** vol. I.

(2) Veremos a continuación que si A es un dominio infinito la situación es distinta.

Proposición VII.1.8 *Sean A un dominio infinito y $f \in A[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ un polinomio no nulo. Entonces, la función polinómica $F : A^n \to A$ asociada a f es no nula.*

Demostración. Supongamos, por reducción al absurdo, que F es nula. Procedemos por inducción sobre n. Si $n = 1$, la nulidad de F significa que cada

elemento del dominio infinito A es raíz de f, lo que contradice la Proposición V.2.2. Supongamos el resultado cierto para polinomios en $n-1$ variables y sean $B := A[\mathtt{x}_1, \ldots, \mathtt{x}_{n-1}]$ y f un polinomio en n variables. Como $A[\mathtt{x}_1, \ldots, \mathtt{x}_{n-1}, \mathtt{x}_n] = B[\mathtt{x}_n]$ podemos escribir

$$f = \sum_{k=0}^{m} f_k \mathtt{x}_n^k$$

donde cada $f_k \in B$. Fijamos ahora $a' := (a_1, \ldots, a_{n-1}) \in A^{n-1}$. Para cada $a_n \in A$, tenemos que

$$0 = F(a', a_n) = \sum_{k=0}^{m} f_k(a') a_n^k$$

y, por el caso de una variable ya estudiado, el polinomio $\sum_{k=0}^{m} f_k(a')\mathtt{x}_n^k \in A[\mathtt{x}_n]$ es nulo. Esto significa que $f_k(a') = 0$ para $0 \leq k \leq m$, y cada $a' \in A^{n-1}$. Por hipótesis de inducción, $f_k = 0$ para $0 \leq k \leq m$, luego $f = 0$. □

Observaciones VII.1.9 (1) Por lo anterior, si A es un dominio infinito, podemos identificar los polinomios con sus funciones polinómicas asociadas.

(2) En particular, si A es un dominio de característica cero existe un homomorfismo inyectivo $\mathbb{Z} \hookrightarrow A$, luego A es infinito, por lo que los polinomios de $A[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ se identifican con las funciones polinómicas $A^n \to A$.

Corolario VII.1.10 *Sean A un dominio infinito, y $f, g, h \in A[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ tres polinomios tales que $h \neq 0$. Si $f(a) = g(a)$ para cada $a \in A^n$ tal que $h(a) \neq 0$, entonces $f = g$.*

Demostración. Por hipótesis, la función polinómica asociada a $h_0 := (f-g)h$ es nula, luego se deduce de la Proposición VII.1.8 que $h_0 = 0$, y $A[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ es un dominio por serlo A. Como $h \neq 0$ esto implica que $f - g = 0$, o sea, $f = g$. □

Definición y Observación VII.1.11 (Funciones racionales.) Si A es un dominio y $n \geq 1$, entonces $A[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ es también un dominio, por lo que existe su cuerpo de fracciones $F := \mathrm{qf}(A[\mathtt{x}_1, \ldots, \mathtt{x}_n])$. Por otro lado, si K es el cuerpo de fracciones de A, consideramos el dominio $K[\mathtt{x}_1, \ldots, \mathtt{x}_n]$, que contiene a $A[\mathtt{x}_1, \ldots, \mathtt{x}_n]$. Denotamos por $K(\mathtt{x}_1, \ldots, \mathtt{x}_n)$ al cuerpo de fracciones de $K[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ y vamos a comprobar que coincide con F.

Como el cuerpo F contiene al anillo A también contiene, por 1.a en el Capítulo II, al cuerpo K. Además, cada $\mathtt{x}_i \in A[\mathtt{x}_1, \ldots, \mathtt{x}_n] \subset F$, y por tanto $K[\mathtt{x}_1, \ldots, \mathtt{x}_n] \subset F$. De nuevo por 1.a en el Capítulo II, $K(\mathtt{x}_1, \ldots, \mathtt{x}_n) \subset F$. Por otro lado,

$$A[\mathtt{x}_1, \ldots, \mathtt{x}_n] \subset K[\mathtt{x}_1, \ldots, \mathtt{x}_n] \subset K(\mathtt{x}_1, \ldots, \mathtt{x}_n)$$

con lo que $F \subset K(\mathtt{x}_1, \ldots, \mathtt{x}_n)$ y se da la igualdad anunciada.

1.a. Polinomios simétricos. Fórmulas de Cardano-Vieta. Veremos a continuación las Fórmulas de Cardano-Vieta, que relacionan los coeficientes de un polinomio en una variable con sus raíces. Estas fórmulas hacen entrar en la escena a las formas simétricas elementales, que son relevantes para formular el teorema de representación de los polinomios simétricos.

Definiciones y Observaciones VII.1.12 (Polinomios simétricos)

(1) Sean A un anillo y $n \geq 1$ un entero. El grupo de permutaciones $\mathcal{S}_n$ (véase Capítulo 3, vol. I) actúa sobre el anillo de polinomios $A[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ mediante

$$\mathcal{S}_n \to \mathrm{Biy}(A[\mathtt{x}_1, \ldots, \mathtt{x}_n]),\ \tau \mapsto \widehat{\tau},$$

donde para cada $f \in A[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ se tiene

$$\widehat{\tau}(f)(\mathtt{x}_1, \ldots, \mathtt{x}_n) := f(\mathtt{x}_{\tau(1)}, \ldots, \mathtt{x}_{\tau(n)}).$$

Es inmediato comprobar que la aplicación $\widehat{\tau} : A[\mathtt{x}_1, \ldots, \mathtt{x}_n] \to A[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ es un isomorfismo de anillos cuyo inverso es $\widehat{\tau^{-1}}$.

(2) Se dice que el polinomio f es *simétrico* si $\widehat{\tau}(f) = f$ para cada permutación $\tau \in \mathcal{S}_n$. Se llaman *polinomios simétricos elementales* o también *formas simétricas elementales* en n variables a los polinomios homogéneos

$$\mathtt{s}_1 := \mathtt{x}_1 + \cdots + \mathtt{x}_n, \quad \mathtt{s}_k := \sum_{1 \leq i_1 < \cdots < i_k \leq n} \mathtt{x}_{i_1} \cdots \mathtt{x}_{i_k} \quad \& \quad \mathtt{s}_n := \mathtt{x}_1 \cdots \mathtt{x}_n,$$

donde $2 \leq k \leq n-1$. Nótese que $\deg(\mathtt{s}_k) = k$ para $1 \leq k \leq n$. Además, si denotamos $\mathtt{s}'_1, \ldots, \mathtt{s}'_{n-1}$ los polinomios simétricos elementales en $n-1$ variables se cumple que

$$\begin{aligned} \mathtt{s}_k &= \sum_{1 \leq i_1 < \cdots < i_k \leq n} \mathtt{x}_{i_1} \cdots \mathtt{x}_{i_k} = \sum_{1 \leq i_1 < \cdots < i_k \leq n-1} \mathtt{x}_{i_1} \cdots \mathtt{x}_{i_k} \\ &+ \sum_{1 \leq i_1 < \cdots < i_{k-1} < i_k = n} \mathtt{x}_{i_1} \cdots \mathtt{x}_{i_{k-1}} \mathtt{x}_n = \sum_{1 \leq i_1 < \cdots < i_k \leq n-1} \mathtt{x}_{i_1} \cdots \mathtt{x}_{i_k} \\ &+ \mathtt{x}_n \cdot \Big(\sum_{1 \leq i_1 < \cdots < i_{k-1} \leq n-1} \mathtt{x}_{i_1} \cdots \mathtt{x}_{i_{k-1}} \Big) = \mathtt{s}'_k + \mathtt{x}_n \mathtt{s}'_{k-1}. \end{aligned}$$

En lo sucesivo denotamos $\mathtt{s}'_0 := 1$ y $\mathtt{s}'_n := 0$. Obsérvese que si A es un anillo de característica cero, los polinomios simétricos elementales en n variables son elementos del subanillo $\mathbb{Z}[\mathtt{x}_1, \ldots, \mathtt{x}_n] \subset A[\mathtt{x}_1, \ldots, \mathtt{x}_n]$.

(3) Si $f \in A[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ es un polinomio simétrico y $f = f_0 + \cdots + f_d$ es la expresión de f como suma de sus componentes homogéneas, entonces cada f_k es un polinomio simétrico. En efecto, para cada permutación $\tau \in \mathcal{S}_n$ se tiene

$$0 = f - \widehat{\tau}(f) = (f_0 - \widehat{\tau}(f_0)) + \cdots + (f_d - \widehat{\tau}(f_d)). \tag{1.2}$$

Como el polinomio $\widehat{\tau}(f_k)$ es homogéneo de grado k, cada resta $f_k - \widehat{\tau}(f_k)$ es un polinomio homogéneo de grado k o el polinomio nulo, y como la suma (1.2) es nula se da el segundo caso, es decir, $f_k = \widehat{\tau}(f_k)$, lo que significa que cada componente homogénea f_k de f es un polinomio simétrico.

Teorema VII.1.13 (Fórmulas de Cardano–Vieta) *Sea*

$$f_n := (\mathtt{t} - \mathtt{x}_1) \cdots (\mathtt{t} - \mathtt{x}_n) \in \mathbb{Z}[\mathtt{x}_1, \ldots, \mathtt{x}_n, \mathtt{t}].$$

Entonces

$$f_n = \mathtt{t}^n + \sum_{k=1}^{n} (-1)^k \mathtt{s}_k(\mathtt{x}_1, \ldots, \mathtt{x}_n) \mathtt{t}^{n-k}.$$

Demostración. Procedemos por inducción sobre $n = \deg_{\mathtt{t}}(f_n)$. Para $n = 1$, tenemos

$$f_1 = \mathtt{t} - \mathtt{x}_1 = \mathtt{t} + (-1)\mathtt{s}_1(\mathtt{x}_1).$$

Supongamos el resultado cierto para $n-1$ y veamos que también lo es para n. Por hipótesis de inducción, y denotando $\mathtt{x}' := (\mathtt{x}_1, \ldots, \mathtt{x}_{n-1})$ se tiene

$$f_{n-1} = (\mathtt{t} - \mathtt{x}_1) \cdots (\mathtt{t} - \mathtt{x}_{n-1}) = \mathtt{t}^{n-1} + \sum_{k=1}^{n-1} (-1)^k \mathtt{s}'_k(\mathtt{x}') \mathtt{t}^{n-1-k},$$

donde $\mathtt{s}'_1, \ldots, \mathtt{s}'_{n-1}$ son los polinomios simétricos elementales en $n-1$ variables. Por tanto,

$$\begin{aligned} f_n = f_{n-1} \cdot (\mathtt{t} - \mathtt{x}_n) &= \Big(\mathtt{t}^{n-1} + \sum_{k=1}^{n-1} (-1)^k \mathtt{s}'_k(\mathtt{x}') \mathtt{t}^{n-1-k}\Big)(\mathtt{t} - \mathtt{x}_n) \\ &= \mathtt{t}^n + \sum_{k=1}^{n} (-1)^k \mathtt{s}'_k(\mathtt{x}') \mathtt{t}^{n-k} + \sum_{k=0}^{n-1} (-1)^{k+1} \mathtt{s}'_k(\mathtt{x}') \mathtt{x}_n \mathtt{t}^{n-(k+1)}. \end{aligned}$$

Cambiando de índice en el último sumatorio resulta

$$f_n = \mathtt{t}^n + \sum_{k=1}^{n}(-1)^k \mathtt{s}'_k(\mathtt{x}')\mathtt{t}^{n-k} + \sum_{k=1}^{n}(-1)^k \mathtt{s}'_{k-1}(\mathtt{x}')\mathtt{x}_n\mathtt{t}^{n-k} = \mathtt{t}^n$$
$$+ \sum_{k=1}^{n}(-1)^k \big(\mathtt{s}'_k(\mathtt{x}') + \mathtt{x}_n\mathtt{s}'_{k-1}(\mathtt{x}')\big)\mathtt{t}^{n-k} = \mathtt{t}^n + \sum_{k=1}^{n}(-1)^k \mathtt{s}_k(\mathtt{x}_1,\dots,\mathtt{x}_n)\mathtt{t}^{n-k}.$$

□

1.b. Teorema de representación de los polinomios simétricos. Antes de probar el *Teorema de representación de los polinomios simétricos* veremos dos lemas auxiliares. Fijamos un anillo A y variables $\mathtt{x}_1,\dots,\mathtt{x}_n$.

Lema VII.1.14 *Sea $f \in A[\mathtt{x}_1,\dots,\mathtt{x}_n]$ un polinomio homogéneo y simétrico. Entonces*

$$g(\mathtt{x}_1,\dots,\mathtt{x}_{n-1}) := f(\mathtt{x}_1,\dots,\mathtt{x}_{n-1},0) \in A[\mathtt{x}_1,\dots,\mathtt{x}_{n-1}]$$

es, o el polinomio nulo, o un polinomio homogéneo y simétrico de grado $\deg(f)$.

Demostración. Suponemos que g no es nulo, y por tanto tampoco es nulo f, y denotamos $d := \deg(f)$. Entonces, g es homogéneo de grado d, ya que

$$\begin{aligned} g(\mathtt{tx}_1,\dots,\mathtt{tx}_{n-1}) &= f(\mathtt{tx}_1,\dots,\mathtt{tx}_{n-1},0) = f(\mathtt{tx}_1,\dots,\mathtt{tx}_{n-1},\mathtt{t}\cdot 0) \\ &= \mathtt{t}^d f(\mathtt{x}_1,\dots,\mathtt{x}_{n-1},0) = \mathtt{t}^d g(\mathtt{x}_1,\dots,\mathtt{x}_{n-1}). \end{aligned}$$

Esto demuestra que g es homogéneo de grado $\deg(f)$. Para probar que es simétrico, sea $\sigma \in \mathcal{S}_{n-1}$ y consideramos la permutación $\tau \in \mathcal{S}_n$ definida por

$$\tau(k) := \begin{cases} \sigma(k) & \text{si } k \neq n \\ n & \text{si } k = n \end{cases}$$

Entonces, como f es simétrico se tiene

$$f(\mathtt{x}_{\tau(1)},\dots,\mathtt{x}_{\tau(n-1)},\mathtt{x}_n) = f(\mathtt{x}_{\tau(1)},\dots,\mathtt{x}_{\tau(n)}) = f(\mathtt{x}_1,\dots,\mathtt{x}_n),$$

y evaluando ambos miembros en $\mathtt{x}_n = 0$ resulta

$$\begin{aligned} g(\mathtt{x}_{\sigma(1)},\dots,\mathtt{x}_{\sigma(n-1)}) &= f(\mathtt{x}_{\tau(1)},\dots,\mathtt{x}_{\tau(n-1)},0) \\ &= f(\mathtt{x}_1,\dots,\mathtt{x}_{n-1},0) = g(\mathtt{x}_1,\dots,\mathtt{x}_{n-1}). \end{aligned}$$

□

Lema VII.1.15 *Sean* $\mathtt{s}_1, \ldots, \mathtt{s}_n$ *las formas simétricas elementales en las variables* $\mathtt{x}_1, \ldots, \mathtt{x}_n$. *Entonces, el homomorfismo de anillos*

$$A[\mathtt{x}_1, \ldots, \mathtt{x}_n] \to A[\mathtt{x}_1, \ldots, \mathtt{x}_n],\ f(\mathtt{x}_1, \ldots, \mathtt{x}_n) \mapsto f(\mathtt{s}_1, \ldots, \mathtt{s}_n)$$

es inyectivo.

Demostración. Se trata de demostrar, por inducción sobre n, que el único polinomio $f \in A[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ que cumple que $f(\mathtt{s}_1, \ldots, \mathtt{s}_n) = 0$ es el polinomio nulo. Para $n = 1$ la única forma simétrica elemental es $\mathtt{s}_1 = \mathtt{x}_1$, luego la condición $f(\mathtt{s}_1) = 0$ significa que $f = f(\mathtt{x}_1) = 0$. Supongamos que la afirmación es cierta para polinomios en $n-1$ variables y veamos que también lo es para polinomios en n variables. Escribimos

$$f := \sum_{k=0}^{m} f_k(\mathtt{x}_1, \ldots, \mathtt{x}_{n-1})\mathtt{x}_n^k \tag{1.3}$$

para ciertos $f_k \in A[\mathtt{x}_1, \ldots, \mathtt{x}_{n-1}]$, y hemos de probar que cada f_k es nulo. Procedemos por inducción sobre $m := \deg_{\mathtt{x}_n}(f)$. Denotamos $\mathtt{x}' := (\mathtt{x}_1, \ldots, \mathtt{x}_{n-1})$ y $\mathtt{x} := (\mathtt{x}', \mathtt{x}_n)$. Vimos en la Observación VII.1.12 (2) que

$$\mathtt{s}_k(\mathtt{x}) = \mathtt{s}'_k(\mathtt{x}') + \mathtt{x}_n\mathtt{s}'_{k-1}(\mathtt{x}')$$

para $1 \leq k \leq n$. Por tanto, $\mathtt{s}_k(\mathtt{x}', 0) = \mathtt{s}'_k(\mathtt{x}')$ para $1 \leq k \leq n-1$. Así, como $f(\mathtt{s}_1, \ldots, \mathtt{s}_n) = 0$, al evaluar $\mathtt{x}_n = 0$ en la fórmula (1.3) se tiene

$$\begin{aligned} 0 &= f(\mathtt{s}_1(\mathtt{x}', 0), \ldots, \mathtt{s}_n(\mathtt{x}', 0)) \\ &= f_0(\mathtt{s}_1(\mathtt{x}', 0), \ldots, \mathtt{s}_{n-1}(\mathtt{x}', 0)) = f_0(\mathtt{s}'_1, \ldots, \mathtt{s}'_{n-1}). \end{aligned}$$

Por la hipótesis de inducción (sobre n) se deduce que $f_0 = 0$. En particular, si $m = 0$ hemos terminado. Supongamos el resultado cierto para polinomios cuyo grado respecto de la variable $\mathtt{x}_n$ es menor que m y sea f un polinomio cuyo grado respecto de $\mathtt{x}_n$ es $\deg_{\mathtt{x}_n}(f) := m$. Como ya hemos demostrado que $f_0 = 0$, podemos escribir

$$f = \sum_{k=1}^{m} f_k(\mathtt{x}')\mathtt{x}_n^k = \mathtt{x}_n \sum_{k=1}^{m} f_k(\mathtt{x}')\mathtt{x}_n^{k-1}.$$

Entonces, $0 = f(\mathtt{s}_1, \ldots, \mathtt{s}_n) = \mathtt{s}_n \sum_{k=1}^{m} f_k(\mathtt{s}_1, \ldots, \mathtt{s}_{n-1})\mathtt{s}_n^{k-1}$. Como $\mathtt{s}_n$ no es divisor de cero en $A[\mathtt{x}_1, \ldots, \mathtt{x}_n]$, resulta

$$\sum_{k=1}^{m} f_k(\mathtt{s}_1, \ldots, \mathtt{s}_{n-1})\mathtt{s}_n^{k-1} = 0. \tag{1.4}$$

El grado respecto de $\mathtt{x}_n$ del polinomio $g := \sum_{k=1}^{m} f_k(\mathtt{x}')\mathtt{x}_n^{k-1}$ es $\leq m-1$ luego, por la hipótesis de inducción (sobre m), se sigue de la igualdad (1.4) que $g = 0$, así que $f = \mathtt{x}_n g = 0$. □

Teorema VII.1.16 (Representación de los polinomios simétricos) *Sea $f \in A[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ un polinomio simétrico. Entonces, existe un único polinomio $g \in A[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ tal que $f = g(\mathtt{s}_1, \ldots, \mathtt{s}_n)$.*

Demostración. La unicidad es, exactamente, lo que dice el Lema VII.1.15, pues si existiesen dos polinomios $g_1, g_2 \in A[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ tales que

$$g_1(\mathtt{s}_1, \ldots, \mathtt{s}_n) = f = g_2(\mathtt{s}_1, \ldots, \mathtt{s}_n),$$

el polinomio $g := g_1 - g_2$ cumpliría que

$$g(\mathtt{s}_1, \ldots, \mathtt{s}_n) = g_1(\mathtt{s}_1, \ldots, \mathtt{s}_n) - g_2(\mathtt{s}_1, \ldots, \mathtt{s}_n) = f - f = 0,$$

luego por el Lema VII.1.15 $g = 0$, es decir, $g_1 = g_2$.

En cuanto a la existencia, basta probarla para polinomios homogéneos. En efecto, supongamos esto probado, y sea $f \in A[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ un polinomio simétrico. Denotamos $f_0, \ldots, f_d$ sus componentes homogéneas, que por la Observación VII.1.12 (3) son también polinomios simétricos y, por supuesto, homogéneos. Existen entonces polinomios $g_k \in A[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ tales que $f_k = g_k(\mathtt{s}_1, \ldots, \mathtt{s}_n)$ para $0 \leq k \leq d$. Así, $g = g_0 + \cdots + g_d \in A[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ cumple

$$f = \sum_{k=0}^{d} f_k = \sum_{k=0}^{d} g_k(\mathtt{s}_1, \ldots, \mathtt{s}_n) = g(\mathtt{s}_1, \ldots, \mathtt{s}_n).$$

Es por tanto suficiente demostrar el resultado para polinomios homogéneos y simétricos, y de hecho vamos a probar lo siguiente:

Para todo polinomio simétrico y homogéneo $f \in A[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ existe un polinomio $g \in A[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ tal que $g(\mathtt{x}_1, \mathtt{x}_2^2, \ldots, \mathtt{x}_n^n)$ es un polinomio homogéneo de grado $\deg(f)$ *y $f = g(\mathtt{s}_1, \ldots, \mathtt{s}_n)$.*

Procedemos por inducción sobre n. Si $n = 1$, entonces $\mathtt{s}_1 = \mathtt{x}_1$ y por ello $f = f(\mathtt{x}_1) = f(\mathtt{s}_1)$, luego $g := f$ nos vale. Supongamos el resultado cierto para polinomios en $n-1$ variables y veamos que también es cierto para polinomios en n variables.

Para ello argumentamos por inducción sobre el grado (total) $\deg(f)$. Si $\deg(f) = 0$ basta tomar $g := f$. Supongamos que la afirmación es cierta para

polinomios cuyo grado total es menor que d y veamos que también lo es si $\deg(f) = d$. Denotamos $\mathtt{x}' := (\mathtt{x}_1, \ldots, \mathtt{x}_{n-1})$ y $F_0 := f(\mathtt{x}', 0) \in A[\mathtt{x}_1, \ldots, \mathtt{x}_{n-1}]$ que, por el Lema VII.1.14, es nulo o simétrico y homogéneo de grado $\deg(f)$.

Por la hipótesis de inducción sobre el número de variables existe un polinomio $G_0 \in A[\mathtt{x}_1, \ldots, \mathtt{x}_{n-1}]$ tal que $F_0 = G_0(\mathtt{s}'_1, \ldots, \mathtt{s}'_{n-1})$ y $G_0(\mathtt{x}_1, \mathtt{x}_2^2, \ldots, \mathtt{x}_{n-1}^{n-1})$ es, bien nulo si $G_0 = 0$, bien homogéneo de grado $\deg(F_0) = \deg(f)$. En consecuencia, el polinomio $G_0(\mathtt{s}_1, \ldots, \mathtt{s}_{n-1})$ es homogéneo de grado $\deg(f)$ o nulo. Consideramos el polinomio homogéneo y simétrico de grado $\deg(f)$:

$$h := f - G_0(\mathtt{s}_1, \ldots, \mathtt{s}_{n-1}).$$

Si $h = 0$ hemos terminado; por tanto, podemos suponer que $h \neq 0$. Como

$$h(\mathtt{x}_1, \ldots, \mathtt{x}_{n-1}, 0) = F_0 - G_0(\mathtt{s}'_1, \ldots, \mathtt{s}'_{n-1}) = F_0 - F_0 = 0,$$

deducimos que $\mathtt{x}_n$ divide a h y, por tanto, dado que h es simétrico, todas las variables $\mathtt{x}_1, \ldots, \mathtt{x}_{n-1}$ dividen a h. Así, $\mathtt{s}_n = \mathtt{x}_1 \cdots \mathtt{x}_n$ divide a h, luego existe un polinomio simétrico y homogéneo h_1 de grado $\deg(h) - n = \deg(f) - n$ tal que $h := \mathtt{s}_n h_1$.

Por la hipótesis de inducción sobre el grado existe $G_1 \in A[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ tal que $G_1(\mathtt{x}_1, \mathtt{x}_2^2, \ldots, \mathtt{x}_n^n)$ es homogéneo de grado $\deg(f) - n$ y $h_1 = G_1(\mathtt{s}_1, \ldots, \mathtt{s}_n)$. De este modo,

$$f = G_0(\mathtt{s}_1, \ldots, \mathtt{s}_{n-1}) + \mathtt{s}_n G_1(\mathtt{s}_1, \ldots, \mathtt{s}_n).$$

Sea $g := G_0 + \mathtt{x}_n G_1$. Se cumple que $f = g(\mathtt{s}_1, \ldots, \mathtt{s}_n)$ y que

$$g(\mathtt{x}_1, \mathtt{x}_2^2, \ldots, \mathtt{x}_n^n) = G_0(\mathtt{x}_1, \mathtt{x}_2^2, \ldots, \mathtt{x}_{n-1}^{n-1}) + \mathtt{x}_n^n G_1(\mathtt{x}_1, \mathtt{x}_2^2, \ldots, \mathtt{x}_n^n)$$

es un polinomio homogéneo de grado $\deg(f)$. □

La demostración anterior es constructiva si, en lugar de aplicar la hipótesis de inducción, repetimos en cada etapa el paso inicial, aunque el proceso es laborioso.

En ocasiones un análisis del polinomio involucrado nos permite encontrar "atajos" que simplifican el procedimiento. En el siguiente ejemplo empleamos, en primer lugar, el argumento introducido en la demostración y vemos después cómo utilizar un procedimiento alternativo que siplifica considerablemente los cálculos involucrados..

Ejemplos VII.1.17 (1) Consideramos el polinomio homogéneo y simétrico

$$f := (\mathtt{x}_1^2 + \mathtt{x}_2^2)(\mathtt{x}_1^2 + \mathtt{x}_3^2)(\mathtt{x}_2^2 + \mathtt{x}_3^2).$$

Buscamos un polinomio $g \in \mathbb{Z}[\mathtt{u}_1, \mathtt{u}_2, \mathtt{u}_3]$ tal que $f = g(\mathtt{s}_1, \mathtt{s}_2, \mathtt{s}_3)$ donde $\mathtt{s}_1, \mathtt{s}_2, \mathtt{s}_3$ son las formas simétricas elementales en las variables $\mathtt{x}_1, \mathtt{x}_2, \mathtt{x}_3$. Sean $\mathtt{s}'_1 := \mathtt{x}_1 + \mathtt{x}_2$ y $\mathtt{s}'_2 := \mathtt{x}_1\mathtt{x}_2$ las formas simétricas elementales en las variables $\mathtt{x}_1$ y $\mathtt{x}_2$. Nótese que

$$\mathtt{x}_1^2 + \mathtt{x}_2^2 = (\mathtt{x}_1 + \mathtt{x}_2)^2 - 2\mathtt{x}_1\mathtt{x}_2 = \mathtt{s}_1'^2 - 2\mathtt{s}'_2,$$

y por tanto se cumple

$$\begin{aligned} F_0 :&= f(\mathtt{x}_1, \mathtt{x}_2, 0) = (\mathtt{x}_1^2 + \mathtt{x}_2^2)\mathtt{x}_1^2\mathtt{x}_2^2 \\ &= (\mathtt{x}_1\mathtt{x}_2)^2(\mathtt{x}_1^2 + \mathtt{x}_2^2) = \mathtt{s}_2'^2(\mathtt{s}_1'^2 - 2\mathtt{s}'_2) = G_0(\mathtt{s}'_1, \mathtt{s}'_2), \end{aligned}$$

con $G_0(\mathtt{u}_1, \mathtt{u}_2) = \mathtt{u}_2^2(\mathtt{u}_1^2 - 2\mathtt{u}_2)$. Así, $F_1 := f - G_0(\mathtt{s}_1, \mathtt{s}_2) = -\mathtt{x}_1\mathtt{x}_2\mathtt{x}_3 F_2$, donde

$$F_2 : \mathtt{x}_1\mathtt{x}_2\mathtt{x}_3 + 2\mathtt{x}_1^3 + 2\mathtt{x}_2^2\mathtt{x}_1 + 2\mathtt{x}_3^2\mathtt{x}_1 + 2\mathtt{x}_1^2\mathtt{x}_2 + 2\mathtt{x}_2^3 + 2\mathtt{x}_3^2\mathtt{x}_2 + 2\mathtt{x}_1^2\mathtt{x}_3 + 2\mathtt{x}_2^2\mathtt{x}_3 + 2\mathtt{x}_3^2.$$

Ahora reiniciamos el proceso con este polinomio F_2, es decir, calculamos

$$\begin{aligned} F_2(\mathtt{x}_1, \mathtt{x}_2, 0) &= 2(\mathtt{x}_1^3 + \mathtt{x}_2^2\mathtt{x}_1 + \mathtt{x}_1^2\mathtt{x}_2 + \mathtt{x}_2^3) = 2(\mathtt{x}_1^3 + 3\mathtt{x}_2^2\mathtt{x}_1 + 3\mathtt{x}_1^2\mathtt{x}_2 + \mathtt{x}_2^3) \\ &\quad - 4(\mathtt{x}_1^2\mathtt{x}_2 + \mathtt{x}_2^2\mathtt{x}_1) = 2\big((\mathtt{x}_1 + \mathtt{x}_2)^3 - 2\mathtt{x}_1\mathtt{x}_2(\mathtt{x}_1 + \mathtt{x}_2)\big) \\ &= 2(\mathtt{s}_1'^3 - 2\mathtt{s}'_1\mathtt{s}'_2) = 2G_1(\mathtt{s}'_1, \mathtt{s}'_2), \end{aligned}$$

donde $G_1(\mathtt{u}_1, \mathtt{u}_2) := \mathtt{u}_1^3 - 2\mathtt{u}_1\mathtt{u}_2$. Así, $F_3 := F_2 - 2G_1(\mathtt{s}_1, \mathtt{s}_2) = \mathtt{x}_1\mathtt{x}_2\mathtt{x}_3 = \mathtt{s}_3$, y por tanto $F_2 = \mathtt{s}_3 + 2G_1(\mathtt{s}_1, \mathtt{s}_2)$. Sustituyendo los valores obtenidos resulta

$$f = G_0(\mathtt{s}_1, \mathtt{s}_2) - \mathtt{s}_3 F_2 = G_0(\mathtt{s}_1, \mathtt{s}_2) - \mathtt{s}_3^2 - 2\mathtt{s}_3 G_1(\mathtt{s}_1, \mathtt{s}_2).$$

Finalmente, $f = g(\mathtt{s}_1, \mathtt{s}_2, \mathtt{s}_3)$, donde

$$\begin{aligned} g(\mathtt{u}_1, \mathtt{u}_2, \mathtt{u}_3) &= G_0(\mathtt{u}_1, \mathtt{u}_2) - \mathtt{u}_3\big(\mathtt{u}_3 + 2G_1(\mathtt{u}_1, \mathtt{u}_2)\big) \\ &= \mathtt{u}_2^2(\mathtt{u}_1^2 - 2\mathtt{u}_2) - \mathtt{u}_3^2 - 2\mathtt{u}_3\mathtt{u}_1(\mathtt{u}_1^2 - 2\mathtt{u}_2) \\ &= (\mathtt{u}_1^2 - 2\mathtt{u}_2)(\mathtt{u}_2^2 - 2\mathtt{u}_1\mathtt{u}_3) - \mathtt{u}_3^2. \end{aligned}$$

Ya señalamos que en ocasiones existen métodos alternativos que permiten acortar los cálculos. En el ejemplo anterior introducimos la variable auxiliar $\mathtt{t} := \mathtt{x}_1^2 + \mathtt{x}_2^2 + \mathtt{x}_3^2$, y así,

$$\mathtt{x}_1^2 + \mathtt{x}_2^2 = \mathtt{t} - \mathtt{x}_3^2, \quad \mathtt{x}_1^2 + \mathtt{x}_3^2 = \mathtt{t} - \mathtt{x}_2^2 \quad \& \quad \mathtt{x}_2^2 + \mathtt{x}_3^2 = \mathtt{t} - \mathtt{x}_1^2,$$

por lo que, empleando las Fórmulas de Cardano-Vieta, VII.1.13, resulta

$$\begin{aligned} f :&= (\mathtt{x}_1^2+\mathtt{x}_2^2)(\mathtt{x}_1^2+\mathtt{x}_3^2)(\mathtt{x}_2^2+\mathtt{x}_3^2) = (\mathtt{t}-\mathtt{x}_3^2)(\mathtt{t}-\mathtt{x}_2^2)(\mathtt{t}-\mathtt{x}_1^2) = \mathtt{t}^3 \\ &- (\mathtt{x}_1^2+\mathtt{x}_2^2+\mathtt{x}_3^2)\mathtt{t}^2 + (\mathtt{x}_3^2\mathtt{x}_2^2+\mathtt{x}_3^2\mathtt{x}_1^2+\mathtt{x}_1^2\mathtt{x}_2^2)\mathtt{t} - \mathtt{x}_3^2\mathtt{x}_2^2\mathtt{x}_1^2 = \mathtt{t}^3 - \mathtt{t}^3 \\ &+ (\mathtt{x}_3^2\mathtt{x}_2^2+\mathtt{x}_3^2\mathtt{x}_1^2+\mathtt{x}_1^2\mathtt{x}_2^2)\mathtt{t} - \mathtt{x}_3^2\mathtt{x}_2^2\mathtt{x}_1^2 = (\mathtt{x}_3^2\mathtt{x}_2^2+\mathtt{x}_3^2\mathtt{x}_1^2+\mathtt{x}_1^2\mathtt{x}_2^2)\mathtt{t} - \mathtt{s}_3^2. \end{aligned}$$

Por otro lado, expresamos

$$\begin{aligned} \mathtt{x}_3^2\mathtt{x}_2^2+\mathtt{x}_3^2\mathtt{x}_1^2+\mathtt{x}_1^2\mathtt{x}_2^2 &= (\mathtt{x}_1\mathtt{x}_2+\mathtt{x}_1\mathtt{x}_3+\mathtt{x}_2\mathtt{x}_3)^2 - 2(\mathtt{x}_1^2\mathtt{x}_2\mathtt{x}_3+\mathtt{x}_2^2\mathtt{x}_1\mathtt{x}_3+\mathtt{x}_3^2\mathtt{x}_1\mathtt{x}_2) \\ &= \mathtt{s}_2^2 - 2\mathtt{s}_3(\mathtt{x}_1+\mathtt{x}_2+\mathtt{x}_3) = \mathtt{s}_2^2 - 2\mathtt{s}_1\mathtt{s}_3, \end{aligned}$$

mientras que la variable auxiliar introducida es también un polinomio simétrico, que escribimos

$$\mathtt{t} = \mathtt{x}_1^2+\mathtt{x}_2^2+\mathtt{x}_3^2 = (\mathtt{x}_1+\mathtt{x}_2+\mathtt{x}_3)^2 - 2(\mathtt{x}_1\mathtt{x}_2+\mathtt{x}_1\mathtt{x}_3+\mathtt{x}_2\mathtt{x}_3) = \mathtt{s}_1^2 - 2\mathtt{s}_2.$$

Al reemplazar estos valores en la expresión de f obtenida anteriormente resulta

$$f = (\mathtt{s}_2^2 - 2\mathtt{s}_1\mathtt{s}_3)(\mathtt{s}_1^2 - 2\mathtt{s}_2) - \mathtt{s}_3^2,$$

o sea, el polinomio $g(\mathtt{u}_1,\mathtt{u}_2,\mathtt{u}_3) := (\mathtt{u}_2^2 - 2\mathtt{u}_1\mathtt{u}_3)(\mathtt{u}_1^2 - 2\mathtt{u}_2) - \mathtt{u}_3^2$ cumple que $f = g(\mathtt{s}_1,\mathtt{s}_2,\mathtt{s}_3)$.

(2) Por su interés al calcular la resolvente cúbica de un polinomio de grado 4, que abordamos en **??** vol. III, vamos a desarrollar otros ejemplos. Denotamos $\mathtt{x} := (\mathtt{x}_1,\mathtt{x}_2,\mathtt{x}_3,\mathtt{x}_4)$ y consideramos los polinomios

$$\begin{aligned} &h_1(\mathtt{x}) = (\mathtt{x}_1+\mathtt{x}_2)(\mathtt{x}_3+\mathtt{x}_4), \quad h_2(\mathtt{x}) = (\mathtt{x}_1+\mathtt{x}_3)(\mathtt{x}_2+\mathtt{x}_4) \quad \& \\ &h_3(\mathtt{x}) = (\mathtt{x}_1+\mathtt{x}_4)(\mathtt{x}_2+\mathtt{x}_4), \end{aligned}$$

que no son simétricos. Pero sí lo son los polinomios

$$f_1 := h_1+h_2+h_3, \quad f_2 = h_1h_2+h_1h_3+h_2h_3 \quad \& \quad f_3 = h_1h_2h_3,$$

y vamos a expresar estos tres polinomios como polinomios en las formas simétricas elementales $\mathtt{s}_1,\mathtt{s}_2,\mathtt{s}_3$ y $\mathtt{s}_4$ en las variables $\mathtt{x}_1,\mathtt{x}_2,\mathtt{x}_3$ y $\mathtt{x}_4$. Denotamos

$$\mathtt{s}'_1 := \mathtt{x}_1+\mathtt{x}_2+\mathtt{x}_3, \quad \mathtt{s}'_2 := \mathtt{x}_1\mathtt{x}_2+\mathtt{x}_1\mathtt{x}_3+\mathtt{x}_2\mathtt{x}_3 \quad \& \quad \mathtt{s}'_3 := \mathtt{x}_1\mathtt{x}_2\mathtt{x}_3$$

las formas simétricas elementales en las variables $\mathtt{x}_1,\mathtt{x}_2$ y $\mathtt{x}_3$. En primer lugar,

$$\begin{aligned} f_1 &= (\mathtt{x}_1+\mathtt{x}_2)(\mathtt{x}_3+\mathtt{x}_4) + (\mathtt{x}_1+\mathtt{x}_3)(\mathtt{x}_2+\mathtt{x}_4) + (\mathtt{x}_1+\mathtt{x}_4)(\mathtt{x}_2+\mathtt{x}_3) \\ &= 2(\mathtt{x}_1\mathtt{x}_2+\mathtt{x}_1\mathtt{x}_3+\mathtt{x}_1\mathtt{x}_4+\mathtt{x}_2\mathtt{x}_3+\mathtt{x}_2\mathtt{x}_4+\mathtt{x}_3\mathtt{x}_4) = 2\mathtt{s}_2. \end{aligned} \tag{1.5}$$

Para f_2 procedemos como en la prueba del Teorema VII.1.16, es decir, consideramos el polinomio simétrico en tres variables

$$\begin{aligned}F_2 :&= f_2(\mathtt{x}_1,\mathtt{x}_2,\mathtt{x}_3,0) = \mathtt{x}_3(\mathtt{x}_1+\mathtt{x}_2)\mathtt{x}_2(\mathtt{x}_1+\mathtt{x}_3)+\mathtt{x}_3(\mathtt{x}_1+\mathtt{x}_2)\mathtt{x}_1\mathtt{x}_2\\
&+\mathtt{x}_2(\mathtt{x}_1+\mathtt{x}_3)\mathtt{x}_1\mathtt{x}_2 = (\mathtt{x}_1+\mathtt{x}_3)(\mathtt{s}_3'+\mathtt{x}_2^2\mathtt{x}_3)+(\mathtt{x}_2+\mathtt{x}_3)(2\mathtt{s}_3'+\mathtt{x}_1^2\mathtt{x}_2+\mathtt{x}_1^2\mathtt{x}_3)\\
&=(\mathtt{x}_1+\mathtt{x}_3)\mathtt{s}_3'+\mathtt{x}_2\mathtt{s}_3'+\mathtt{x}_2^2\mathtt{x}_3^2+2(\mathtt{x}_2+\mathtt{x}_3)s_3'+\mathtt{x}_1^2\mathtt{x}_2^2+\mathtt{x}_1\mathtt{s}_3'+\mathtt{x}_1\mathtt{s}_3'\\
&+\mathtt{x}_1^2\mathtt{x}_3^2 = 3(\mathtt{x}_1+\mathtt{x}_2+\mathtt{x}_3)\mathtt{s}_3'+\mathtt{x}_1^2\mathtt{x}_2^2+\mathtt{x}_1^2\mathtt{x}_3^2+\mathtt{x}_2^2\mathtt{x}_3^2 = 3\mathtt{s}_1'\mathtt{s}_3'\\
&+(\mathtt{x}_1\mathtt{x}_2+\mathtt{x}_1\mathtt{x}_3+\mathtt{x}_2\mathtt{x}_3)^2-2(\mathtt{x}_1^2\mathtt{x}_2\mathtt{x}_3+\mathtt{x}_1\mathtt{x}_2^2\mathtt{x}_3+\mathtt{x}_1\mathtt{x}_2\mathtt{x}_3^2)\\
&=3\mathtt{s}_1'\mathtt{s}_3'+\mathtt{s}_2'^2-2\mathtt{s}_1'\mathtt{s}_3' = \mathtt{s}_1'\mathtt{s}_3'+\mathtt{s}_2'^2.\end{aligned}$$

Esto implica que la diferencia $f_2-(\mathtt{s}_1\mathtt{s}_3+\mathtt{s}_2^2)$ es múltiplo de $\mathtt{x}_4$ y, como es simétrico, lo es de cada variable $\mathtt{x}_i$. Como $\mathbb{Z}[\mathtt{x}_1,\mathtt{x}_2,\mathtt{x}_3,\mathtt{x}_4]$ es un DFU el producto $\mathtt{s}_4=\mathtt{x}_1\mathtt{x}_2,\mathtt{x}_3\mathtt{x}_4$ divide a $f_2-(\mathtt{s}_1\mathtt{s}_3+\mathtt{s}_2^2)$, y un cálculo largo pero directo muestra que $f_2-(\mathtt{s}_1\mathtt{s}_3+\mathtt{s}_2^2)=-4\mathtt{s}_4$. En conclusión,

$$f_2=(\mathtt{s}_1\mathtt{s}_3+\mathtt{s}_2^2)-4\mathtt{s}_4. \tag{1.6}$$

Por último introducimos el polinomio

$$\begin{aligned}F_3 :&= f_3(\mathtt{x}_1,\mathtt{x}_2,\mathtt{x}_3,0) = \mathtt{x}_3(\mathtt{x}_1+\mathtt{x}_2)\mathtt{x}_2(\mathtt{x}_1+\mathtt{x}_3)\mathtt{x}_1(\mathtt{x}_2+\mathtt{x}_3)\\
&=\mathtt{s}_3'(\mathtt{s}_1'-\mathtt{x}_3)(\mathtt{s}_1'-\mathtt{x}_2)(\mathtt{s}_1'-\mathtt{x}_1) = \mathtt{s}_3'(\mathtt{s}_1'^3-\mathtt{s}_1'\mathtt{s}_1'^2+\mathtt{s}_2'\mathtt{s}_1'-\mathtt{s}_3')\\
&=\mathtt{s}_1'\mathtt{s}_2'\mathtt{s}_3'-\mathtt{s}_3'^2.\end{aligned}$$

Por ello, $f_3-(\mathtt{s}_1\mathtt{s}_2\mathtt{s}_3-\mathtt{s}_3^2)$ es múltiplo de $\mathtt{x}_4$, luego también lo es del producto $\mathtt{s}_4=\mathtt{x}_1\mathtt{x}_2\mathtt{x}_3\mathtt{x}_4$. Al desarrollar la resta $f_3-(\mathtt{s}_1\mathtt{s}_2\mathtt{s}_3-\mathtt{s}_3^2)$ y sacar factor común a $\mathtt{s}_4$ se obtiene $f_3-(\mathtt{s}_1\mathtt{s}_2\mathtt{s}_3-\mathtt{s}_3^2)=-\mathtt{s}_1^2\mathtt{s}_4$, así que

$$f_3=\mathtt{s}_1\mathtt{s}_2\mathtt{s}_3-\mathtt{s}_3^2-\mathtt{s}_1^2\mathtt{s}_4. \tag{1.7}$$

2. Resultante y discriminante. Teorema de los ceros

En esta sección A es un dominio de característica 0, luego contiene una copia de $\mathbb{Z}$. El primer objetivo es obtener un procedimiento, la anulación de la resultante, para determinar si dos polinomios en una variable con coeficientes en un dominio de factorización única A comparten un factor irreducible en $A[\mathtt{t}]$ de grado ≥ 1. Dicho procedimiento nos permitirá determinar también, mediante el discriminante, si un polinomio tiene raíces múltiples. Probaremos además el Teorema de los ceros de Hilbert empleando argumentos que sólo involucran a la resultante, que como veremos es una herramienta que únicamente utiliza Álgebra Lineal.

Lema VII.2.1 *Sean A un* DFU *y $f, g \in A[\mathtt{t}]$ dos polinomios de grado ≥ 1. Las siguientes afirmaciones son equivalentes:*

(1) *Los polinomios f y g comparten en $A[\mathtt{t}]$ un factor irreducible de grado ≥ 1.*

(2) *Existen polinomios no nulos $p, q \in A[\mathtt{t}]$ tales que*

$$\deg(p) \leq \deg(f) - 1, \quad \deg(q) \leq \deg(g) - 1 \quad \& \quad fq = gp.$$

Demostración. (1) $\Longrightarrow$ (2) Sea $h \in A[\mathtt{t}]$ un factor irreducible común de f y g en $A[\mathtt{t}]$ de grado mayor o igual que 1. Existen por tanto $p, q \in A[\mathtt{t}]$ de grados $\deg(p) \leq \deg(f) - 1$ y $\deg(q) \leq \deg(g) - 1$ tales que $f = ph$ y $g = qh$. Por tanto, $qf = qph = pg$.

(2) $\Longrightarrow$ (1) Suponemos, por reducción al absurdo, que f y g no tienen ningún factor irreducible común en $A[\mathtt{t}]$ de grado mayor o igual que 1, es decir, $\mathrm{mcd}\,(f, g) = a \in A \setminus \{0\}$. Escribimos $f = af_1$ y $g = ag_1$ donde $f_1, g_1 \in A[\mathtt{t}]$ y $\mathrm{mcd}(f_1, g_1) = 1$. Entonces $af_1q = ag_1p$, así que $f_1q = g_1p$, luego $f_1 | g_1p$. Como $A[\mathtt{t}]$ es un DFU y $\mathrm{mcd}(f_1, g_1) = 1$, esto implica que que $f_1 | p$, lo que es absurdo ya que $\deg(p) \leq \deg(f) - 1 = \deg(f_1) - 1$. □

2.a. Resultante. (1) Si A es un DFU, el Lema anterior VII.2.1 nos dice que para determinar si dos polinomios en $A[\mathtt{t}]$

$$f(\mathtt{t}) := \sum_{i=0}^{n} a_i \mathtt{t}^i \quad \& \quad g(\mathtt{t}) := \sum_{j=0}^{m} b_j \mathtt{t}^j$$

de grados $n, m \geq 1$ comparten un factor irreducible en $A[\mathtt{t}]$ es suficiente que existan polinomios no nulos $p(\mathtt{t}) := \sum_{k=0}^{n-1} A_k \mathtt{t}^k$ y $-q(\mathtt{t}) := \sum_{\ell=0}^{m-1} B_\ell \mathtt{t}^\ell$ en $A[\mathtt{t}]$ tales que $gp = fq$ o, equivalentemente,

$$0 = gp - fq = \sum_{d=0}^{n+m-1} \Big(\sum_{i+\ell=d} a_i B_\ell + \sum_{j+k=d} b_j A_k \Big) \mathtt{t}^d. \tag{2.8}$$

(2) Antes de analizar lo anterior en toda su generalidad veamos qué significa para polinomios de grados pequeños, por ejemplo $n = 3$ y $m = 2$. La igualdad (2.8) se escribe ahora

$$\sum_{d=0}^{4} \Big(\sum_{i+\ell=d} a_i B_\ell + \sum_{j+k=d} b_j A_k \Big) \mathtt{t}^d \quad \Longrightarrow \quad \sum_{i+\ell=d} a_i B_\ell + \sum_{j+k=d} b_j A_k = 0$$

para $0 \leq d \leq 4$. Esto equivale a que la upla $(B_0, B_1, A_0, A_1, A_2)$ es solución no trivial del sistema homogéneo de ecuaciones lineales

$$\left\{\begin{array}{lllllllllll} a_0B_0 & & & + & b_0A_0 & & & & & = & 0 \\ a_1B_0 & + & a_0B_1 & + & b_1A_0 & + & b_0A_1 & & & = & 0 \\ a_2B_0 & + & a_1B_1 & + & b_2A_0 & + & b_1A_1 & + & b_0A_2 & = & 0 \\ a_3B_0 & + & a_2B_1 & & & + & b_2A_1 & + & b_1A_2 & = & 0 \\ & & a_3B_1 & & & & & + & b_2A_2 & = & 0 \end{array}\right.$$

Por el Teorema de Rouché-Frobenius, la existencia de una solución no trivial del sistema de ecuaciones lineales anterior equivale a que sea nulo el determinante de su matriz de coeficientes, esto es,

$$\det \begin{pmatrix} a_0 & 0 & b_0 & 0 & 0 \\ a_1 & a_0 & b_1 & b_0 & 0 \\ a_2 & a_1 & b_2 & b_1 & b_0 \\ a_3 & a_2 & 0 & b_2 & b_1 \\ 0 & a_3 & 0 & 0 & b_2 \end{pmatrix} = 0.$$

Como una matriz cuadrada y su traspuesta tienen el mismo determinante la igualdad anterior se suele escribir, de modo equivalente, como

$$\det \begin{pmatrix} a_0 & a_1 & a_2 & a_3 & 0 \\ 0 & a_0 & a_1 & a_2 & a_3 \\ b_0 & b_1 & b_2 & 0 & 0 \\ 0 & b_0 & b_1 & b_2 & 0 \\ 0 & 0 & b_0 & b_1 & b_2 \end{pmatrix} = 0.$$

(3) Volviendo al caso general, la igualdad (2.8) equivale a que

$$\sum_{j+k=d} b_j A_k + \sum_{i+\ell=d} a_i B_\ell = 0$$

para todo $0 \leq d \leq n+m-1$. Así, $(B_0, \ldots, B_{m-1}, A_0, \ldots, A_{n-1}) \in A^{m+n}$ es una solución no nula del sistema de ecuaciones lineales

$$(B_0, \ldots, B_{m-1}, A_0, \ldots, A_{n-1}) \cdot M = (0, \ldots, 0),$$

donde M es la siguiente matriz de orden $n+m$ con coeficientes en A:

$$M := \left[\begin{array}{cccccccc} a_0 & a_1 & \cdots & a_n & 0 & 0 & \cdots & 0 \\ 0 & a_0 & a_1 & \cdots & a_n & 0 & \cdots & 0 \\ \vdots & & \vdots & & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & a_0 & a_1 & a_2 & \cdots & a_n \\ b_0 & b_1 & \cdots & b_{m-1} & b_m & 0 & \cdots & 0 \\ 0 & b_0 & b_1 & \cdots & b_{m-1} & b_m & \cdots & 0 \\ \vdots & \vdots & & & \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 & b_0 & b_1 & \cdots & b_m \end{array}\right] \begin{array}{l} \left.\begin{array}{l}\\\\\\\end{array}\right\} m \text{ filas} \\ \left.\begin{array}{l}\\\\\\\end{array}\right\} n \text{ filas} \end{array}$$

El sistema anterior es homogéneo y, por tanto, tiene una solución no idénticamente nula si y sólo si $\det(M) = 0$.

Se define la *resultante* $\mathrm{Res}(f,g) \in A$ de f, g como $\mathrm{Res}(f,g) := \det(M)$, y el Lema VII.2.1 se reformula del siguiente modo.

(∗) *Si A es un* DFU *y $f, g \in A[\mathtt{t}]$ son dos polinomios de grado ≥ 1, entonces f y g comparten en $A[\mathtt{t}]$ un factor de grado ≥ 1 si y sólo si* $\mathrm{Res}(f,g) = 0$.

Ejemplos VII.2.2 (1) Dados los polinomios

$$f(\mathtt{x},\mathtt{y}) := \mathtt{x}^2 - 5\mathtt{y}^2 - 2\mathtt{xy} - 3\mathtt{x} + 3\mathtt{y} + 2 \quad \& \quad g(\mathtt{x},\mathtt{y}) := \mathtt{x}^2 - 7\mathtt{y}^2 - 3\mathtt{x} - 5\mathtt{y} + 2$$

vamos a encontrar todos los puntos de corte de las cónicas afines

$$C_1 := \{(x,y) \in \mathbb{C}^2 : f(x,y) = 0\} \quad \& \quad C_2 := \{(x,y) \in \mathbb{C}^2 : g(x,y) = 0\}.$$

Sea $(x,b) \in C_1 \cap C_2$. Entonces x es raíz común de los polinomios

$$f_b(\mathtt{x}) := \mathtt{x}^2 - (2b+3)\mathtt{x} + (2+3b-5b^2) \quad \& \quad g_b(\mathtt{x}) := \mathtt{x}^2 - 3\mathtt{x} + (2-5b-7b^2),$$

luego el polinomio $\mathtt{x} - x$ divide a $f_b(\mathtt{x})$ y $g_b(\mathtt{x})$ en $\mathbb{C}[\mathtt{x}]$, por lo que la resultante $\mathrm{Res}(f_b, g_b)$ de f_b y g_b ha de ser nula. Pero

$$\begin{aligned} \mathrm{Res}(f_b,g_b) &= \det \begin{pmatrix} 1 & -(2b+3) & 2+3b-5b^2 & 0 \\ 0 & 1 & -(2b+3) & 2+3b-5b^2 \\ 1 & -3 & 2-5b-7b^2 & 0 \\ 0 & 1 & -3 & 2-5b-7b^2 \end{pmatrix} \\ &= -24b^2(b^2-1), \end{aligned}$$

luego $b = 0, 1, -1$. Para $b = 0$, $f_0 = \mathtt{x}^2 - 3\mathtt{x} + 2 = (\mathtt{x} - 1)(\mathtt{x} - 2) = g_0$, cuyas raíces son $x = 1$ y $x = 2$, y obtenemos dos puntos de corte $p_1 = (1, 0)$ y $p_2 = (2, 0)$ de C_1 y C_2. Para $b = -1$, la única raíz común de los polinomios

$$f_{-1} = \mathtt{x}^2 - \mathtt{x} - 6 = (\mathtt{x} + 2)(\mathtt{x} - 3) \quad \& \quad g_{-1} = \mathtt{x}^2 - 3\mathtt{x} = \mathtt{x}(\mathtt{x} - 3),$$

es $x = 3$. Así $p_3 = (3, -1) \in C_1 \cap C_2$. Por último, para $b = 1$,

$$f_1 = \mathtt{x}^2 - 5\mathtt{x} = \mathtt{x}(\mathtt{x} - 5) \quad \& \quad g_1(\mathtt{x}) = \mathtt{x}^2 - 3\mathtt{x} - 10 = (\mathtt{x} + 2)(\mathtt{x} - 5),$$

cuya raíz común es $x = 5$. Así también $p_4 = (5, 1) \in C_1 \cap C_2$, y en conclusión

$$C_1 \cap C_2 = \{p_1 = (1, 0),\ p_2 = (2, 0),\ p_3 = (3, -1),\ p_4 = (5, 1)\}.$$

A continuación, veremos algunas propiedades de la resultante.

Proposición VII.2.3 *Sean A un dominio y $f, g \in A[\mathtt{t}]$ polinomios de grado positivo. Entonces, existen polinomios $p, q \in A[\mathtt{t}]$ tales que* $\mathrm{Res}(f, g) = fp + gq$.

Demostración. Por definición, tenemos

$$\mathrm{Res}(f,g) := \det \begin{bmatrix} a_0 & a_1 & \cdots & a_n & 0 & 0 & \cdots & 0 \\ 0 & a_0 & a_1 & \cdots & a_n & 0 & \cdots & 0 \\ \vdots & & \vdots & & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & a_0 & a_1 & a_2 & \cdots & a_n \\ b_0 & b_1 & \cdots & b_{m-1} & b_m & 0 & \cdots & 0 \\ 0 & b_0 & b_1 & \cdots & b_{m-1} & b_m & \cdots & 0 \\ \vdots & \vdots & & & \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 & b_0 & b_1 & \cdots & b_m \end{bmatrix} \begin{matrix} \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} m \text{ filas} \\ \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} n \text{ filas} \end{matrix}$$

El determinante anterior no varía si a la primera columna le sumamos $\mathtt{t}$ veces la segunda, $\mathtt{t}^2$ veces la tercera, ..., $\mathtt{t}^{j-1}$ veces la j-ésima, ..., y $\mathtt{t}^{n+m-1}$ veces la $(n+m)$-ésima. Por tanto

$$\mathrm{Res}(f,g) = \det \begin{bmatrix} f & a_1 & \cdots & a_n & 0 & 0 & \cdots & 0 \\ f\mathtt{t} & a_0 & a_1 & \cdots & a_n & 0 & \cdots & 0 \\ \vdots & & \vdots & & \vdots & \vdots & & \vdots \\ f\mathtt{t}^{m-1} & \cdots & 0 & a_0 & a_1 & a_2 & \cdots & a_n \\ g & b_1 & \cdots & b_{m-1} & b_m & 0 & \cdots & 0 \\ g\mathtt{t} & b_0 & b_1 & \cdots & b_{m-1} & b_m & \cdots & 0 \\ \vdots & \vdots & & & \vdots & \vdots & & \vdots \\ g\mathtt{t}^{n-1} & 0 & \cdots & 0 & b_0 & b_1 & \cdots & b_m \end{bmatrix} \begin{matrix} \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} m \text{ filas} \\ \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} n \text{ filas} \end{matrix}$$

Desarrollando este determinante por la primera columna obtenemos polinomios $p, q \in A[\mathtt{t}]$ tales que $\mathrm{Res}(f,g) = fp + gq$. □

Teorema VII.2.4 *Sean n, m enteros positivos y consideremos indeterminadas*

$$\mathtt{v} := (\mathtt{v}_0, \ldots, \mathtt{v}_n),\ \ \mathtt{w} := (\mathtt{w}_0, \ldots, \mathtt{w}_m),\ \ \mathtt{x} := (\mathtt{x}_1, \ldots, \mathtt{x}_n),\ \ \mathtt{y} := (\mathtt{y}_1, \ldots, \mathtt{y}_m)\ \&\ \mathtt{t}$$

y los polinomios

$$\begin{aligned} f_{\mathtt{v}} &:= \mathtt{v}_n(\mathtt{t}-\mathtt{x}_1)\cdots(\mathtt{t}-\mathtt{x}_n) = \mathtt{v}_0 + \mathtt{v}_1\mathtt{t} + \cdots + \mathtt{v}_n\mathtt{t}^n, \\ g_{\mathtt{w}} &:= \mathtt{w}_m(\mathtt{t}-\mathtt{y}_1)\cdots(\mathtt{t}-\mathtt{y}_m) = \mathtt{w}_0 + \mathtt{w}_1\mathtt{t} + \cdots + \mathtt{w}_m\mathtt{t}^m. \end{aligned}$$

Se cumple que $\mathrm{Res}(f_{\mathtt{v}}, g_{\mathtt{w}}) = (-1)^{nm}\mathtt{v}_n^m\mathtt{w}_m^n \prod_{i=1}^n \prod_{j=1}^m (\mathtt{x}_i - \mathtt{y}_j)$.

Demostración. En primer lugar, por las Fórmulas de Cardano-Vieta se tiene

$$\begin{aligned} \mathtt{v}_i &= \mathtt{v}_n(-1)^{n-i}\mathtt{s}_{n-i}(\mathtt{x}_1, \ldots, \mathtt{x}_n) \qquad \text{para } \ 0 \le i \le n-1, \\ \mathtt{w}_j &= \mathtt{w}_m(-1)^{m-j}\widehat{\mathtt{s}}_{m-j}(\mathtt{y}_1, \ldots, \mathtt{y}_m) \qquad \text{para } \ 0 \le j \le m-1, \end{aligned} \tag{2.9}$$

donde $\mathtt{s}_1, \ldots, \mathtt{s}_n$ son las formas simétricas elementales en n variables y hemos denotado $\widehat{\mathtt{s}}_1, \ldots, \widehat{\mathtt{s}}_m$ las formas simétricas elementales en m variables. Por definición se tiene

$$\mathrm{Res}(f_{\mathtt{v}}, g_{\mathtt{w}}) = \det \begin{bmatrix} \mathtt{v}_0 & \mathtt{v}_1 & \cdots & \mathtt{v}_n & 0 & 0 & \cdots & 0 \\ 0 & \mathtt{v}_0 & \mathtt{v}_1 & \cdots & \mathtt{v}_n & 0 & \cdots & 0 \\ \vdots & & \vdots & & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & \mathtt{v}_0 & \mathtt{v}_1 & \mathtt{v}_2 & \cdots & \mathtt{v}_n \\ \mathtt{w}_0 & \mathtt{w}_1 & \cdots & \mathtt{w}_{m-1} & \mathtt{w}_m & 0 & \cdots & 0 \\ 0 & \mathtt{w}_0 & \mathtt{w}_1 & \cdots & \mathtt{w}_{m-1} & \mathtt{w}_m & \cdots & 0 \\ \vdots & \vdots & & & \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 & \mathtt{w}_0 & \mathtt{w}_1 & \cdots & \mathtt{w}_m \end{bmatrix} \begin{matrix} \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} m \text{ filas} \\ \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} n \text{ filas} \end{matrix}$$

así que existe un polinomio $H(\mathtt{v}, \mathtt{w}) \in \mathbb{Z}[\mathtt{v}, \mathtt{w}]$ tal que $\mathrm{Res}(f_{\mathtt{v}}, g_{\mathtt{w}}) := H(\mathtt{v}, \mathtt{w})$. Por las propiedades de los determinantes,

$$H(\mathtt{tv}, \mathtt{w}) = \mathtt{t}^m H(\mathtt{v}, \mathtt{w}) \quad \& \quad H(\mathtt{v}, \mathtt{tw}) = \mathtt{t}^n H(\mathtt{v}, \mathtt{w}),$$

lo que implica, por VII.1.5 (5), que H es un polinomio homogéneo en las variables $\mathtt{v}$ de grado m y homogéneo en las variables $\mathtt{w}$ de grado n. Consideremos los

grupos de variables $\mathtt{u} := (\mathtt{u}_1, \dots, \mathtt{u}_n)$ y $\mathtt{z} := (\mathtt{z}_1, \dots, \mathtt{z}_m)$, los anillos $B := \mathbb{Z}[\mathtt{z}]$, $C := \mathbb{Z}[\mathtt{u}]$ y el polinomio

$$F(\mathtt{u}, \mathtt{z}) := H\big((-1)^n \mathtt{u}_n, \dots, -\mathtt{u}_1, 1; (-1)^m \mathtt{z}_m, \dots, -\mathtt{z}_1, 1\big) \in B[\mathtt{u}] = C[\mathtt{z}]$$

de grado total $\leq m$ en $B[\mathtt{u}]$ y de grado total $\leq n$ en $C[\mathtt{z}]$. Si denotamos

$$\mathtt{s} := (\mathtt{s}_1, \dots, \mathtt{s}_n) \quad \& \quad \widehat{\mathtt{s}} := (\widehat{\mathtt{s}}_1, \dots, \widehat{\mathtt{s}}_m),$$

se deduce de las igualdades (2.9) que

$$\begin{aligned} H(\mathtt{v}, \mathtt{w}) &= H\big(\mathtt{v}_n((-1)^n \mathtt{s}_n, \dots, -\mathtt{s}_1, 1), \mathtt{w}_m((-1)^m \widehat{\mathtt{s}}_m, \dots, -\widehat{\mathtt{s}}_1, 1)\big) \\ &= \mathtt{v}_n^m \mathtt{w}_m^n H\big((-1)^n \mathtt{s}_n, \dots, -\mathtt{s}_1, 1; (-1)^m \widehat{\mathtt{s}}_m, \dots, -\widehat{\mathtt{s}}_1, 1\big) \\ &= \mathtt{v}_n^m \mathtt{w}_m^n F(\mathtt{s}, \widehat{\mathtt{s}}). \end{aligned} \tag{2.10}$$

Escribimos $F(\mathtt{s}, \widehat{\mathtt{s}}) := G(\mathtt{x}, \mathtt{y})$, donde $G \in \mathbb{Z}[\mathtt{x}, \mathtt{y}]$. Si hacemos $\mathtt{x}_i := \mathtt{y}_j$, entonces los polinomios $f_{\mathtt{v}}, g_{\mathtt{w}} \in \mathbb{Z}[\mathtt{x}, \mathtt{y}, \mathtt{v}, \mathtt{w}][\mathtt{t}]$ compartirían el factor $(\mathtt{t} - \mathtt{x}_i) = (\mathtt{t} - \mathtt{y}_j)$, y se deduce de la discusión que sigue al Lema VII.2.1 que

$$G(\mathtt{x}_1, \dots, \mathtt{x}_{i-1}, \mathtt{y}_j, \mathtt{x}_{i+1}, \dots, \mathtt{x}_n, \mathtt{y}) = 0.$$

De este modo, por la Regla de Ruffini V.1.11, cada resta $\mathtt{x}_i - \mathtt{y}_j$ divide a G y, como $\mathbb{Z}[\mathtt{x}, \mathtt{y}]$ es un DFU, también el producto $\prod_{i=1}^n \prod_{j=1}^m (\mathtt{x}_i - \mathtt{y}_j)$ divide a G. Por tanto,

$$G(\mathtt{x}, \mathtt{y}) = L(\mathtt{x}, \mathtt{y}) \prod_{i=1}^n \prod_{j=1}^m (\mathtt{x}_i - \mathtt{y}_j)$$

para cierto polinomio $L \in \mathbb{Z}[\mathtt{x}, \mathtt{y}]$. Para terminar es suficiente comprobar que $L = (-1)^{nm}$. Se cumple que

$$F(\mathtt{s}, \widehat{\mathtt{s}}) = L(\mathtt{x}, \mathtt{y}) \prod_{i=1}^n \prod_{j=1}^m (\mathtt{x}_i - \mathtt{y}_j) \in \mathbb{Z}[\mathtt{x}][\mathtt{y}] = \mathbb{Z}[\mathtt{y}][\mathtt{x}]$$

es un polinomio simétrico tanto en las variables $\mathtt{x}$ como en las variables $\mathtt{y}$ (pero no conjuntamente). Como $\prod_{i=1}^n \prod_{j=1}^m (\mathtt{x}_i - \mathtt{y}_j) \in \mathbb{Z}[\mathtt{y}][\mathtt{x}] = \mathbb{Z}[\mathtt{x}][\mathtt{y}]$ es un polinomio simétrico con respecto a las variables $\mathtt{x}$ y a las variables $\mathtt{y}$ se deduce que $L(\mathtt{x}, \mathtt{y})$ también lo es. Por tanto, aplicando dos veces el Teorema VII.1.16, existe un polinomio $L_1 \in \mathbb{Z}[\mathtt{u}, \mathtt{z}]$ tal que $L = L_1(\mathtt{s}, \widehat{\mathtt{s}})$. Consideramos los polinomios

$$\begin{aligned} f^*(\mathtt{t}) &:= (\mathtt{t} - \mathtt{x}_1) \cdots (\mathtt{t} - \mathtt{x}_n) = \mathtt{u}_n + \mathtt{u}_{n-1}\mathtt{t} + \cdots + \mathtt{u}_1 \mathtt{t}^{n-1} + \mathtt{t}^n \quad \& \\ g^*(\mathtt{t}) &:= (\mathtt{t} - \mathtt{y}_1) \cdots (\mathtt{t} - \mathtt{y}_m) = \mathtt{z}_m + \mathtt{z}_{m-1}\mathtt{t} + \cdots + \mathtt{z}_1 \mathtt{t}^{m-1} + \mathtt{t}^m. \end{aligned}$$

Por el Teorema VII.1.13 se cumple que

$$\mathtt{u}_i = (-1)^i \mathtt{s}_i(\mathtt{x}_1, \ldots, \mathtt{x}_n) \quad \& \quad \mathtt{z}_j = (-1)^j \widehat{\mathtt{s}}_j(\mathtt{y}_1, \ldots, \mathtt{y}_m) \tag{2.11}$$

para $1 \leq i \leq n$ y $1 \leq j \leq m$. De este modo,

$$\prod_{i=1}^{n}\prod_{j=1}^{m}(\mathtt{x}_i - \mathtt{y}_j) = \prod_{i=1}^{n} g^*(\mathtt{x}_i) = (-1)^{n+m}\prod_{j=1}^{m} f^*(\mathtt{y}_j).$$

El polinomio $g^* \in \mathbb{Z}[\mathtt{t}][\mathtt{z}]$ tiene grado total 1 como polinomio en las variables $\mathtt{z}'s$, luego el producto $\prod_{i=1}^{n} g^*(\mathtt{x}_i)$ tiene grado n con respecto a $\mathtt{z}$. Por otro lado, $f^* \in \mathbb{Z}[\mathtt{t}][\mathtt{u}]$ tiene grado total 1 como polinomio en las variables $\mathtt{u}'s$ y, por tanto, $(-1)^{n+m}\prod_{j=1}^{m} f^*(\mathtt{y}_j)$ tiene grado m con respecto a $\mathtt{u}$. Vamos a comprobar que

$$F(\mathtt{s},\mathtt{z}) = L_1(\mathtt{s},\mathtt{z})\prod_{i=1}^{n} g^*(\mathtt{x}_i) \quad \& \quad F(\mathtt{u},\widehat{\mathtt{s}}) = L_1(\mathtt{u},\widehat{\mathtt{s}})(-1)^{n+m}\prod_{j=1}^{m} f^*(\mathtt{y}_j). \tag{2.12}$$

En efecto, para demostrar la primera igualdad es suficiente, en virtud del Lema VII.1.15, comprobarla al sustituir $\mathtt{z}$ por $\widehat{s}$, y eso es inmediato:

$$F(\mathtt{s},\widehat{\mathtt{s}}) = L(\mathtt{x},\mathtt{y})\prod_{i=1}^{n}\prod_{j=1}^{m}(\mathtt{x}_i - \mathtt{y}_j) = L_1(\mathtt{s},\widehat{\mathtt{s}})\prod_{i=1}^{n}\prod_{j=1}^{m}(\mathtt{x}_i - \mathtt{y}_j) = L_1(\mathtt{s},\widehat{\mathtt{s}})\prod_{i=1}^{n} g^*(\mathtt{x}_i).$$

En cuanto a la segunda el razonamiento es idéntico. Basta demostrar la igualdad al reemplazar $\mathtt{u}$ por $\mathtt{s}$, y esto es trivialmente cierto, ya que

$$F(\mathtt{s},\widehat{\mathtt{s}}) = L(\mathtt{x},\mathtt{y})\prod_{i=1}^{n}\prod_{j=1}^{m}(\mathtt{x}_i - \mathtt{y}_j) = L_1(\mathtt{s},\widehat{\mathtt{s}})(-1)^{n+m}\prod_{j=1}^{m} f^*(\mathtt{y}_j). \tag{2.13}$$

Nótese que el grado total de $F \in C[\mathtt{z}]$ es menor o igual que n y el grado total de $F \in B[\mathtt{u}]$ es menor o igual que m. Por otro lado, tanto el grado en $\mathtt{z}$ de $g^*(\mathtt{t})$ como el grado en $\mathtt{u}$ de $f^*(\mathtt{t})$ valen 1, luego el grado en $\mathtt{z}$ del producto $\prod_{i=1}^{n} g^*(\mathtt{x}_i)$ es n, mientras que el grado en $\mathtt{z}$ del producto $\prod_{j=1}^{m} f^*(\mathtt{y}_j)$ es m. Por ello, de las igualdades en (2.12) se desprende que $L_1(\mathtt{s},\mathtt{z})$ tiene grado 0 con respecto a $\mathtt{z}$ y $L_1(\mathtt{u},\widehat{\mathtt{s}})$ tiene grado 0 con respecto a $\mathtt{u}$.

Por el Lema VII.1.15, $L_1(\mathtt{u},\mathtt{z}) \in \mathbb{Z}[\mathtt{u},\mathtt{z}]$ tiene grado 0 con respecto a $\mathtt{u}$ y con respecto a $\mathtt{z}$ y, por tanto, es un número entero $L = L_1 \in \mathbb{Z}$, y todo se reduce a comprobar que $L = (-1)^{nm}$. De momento sabemos, por la igualdad (2.13), que

$$F(\mathtt{s},\widehat{\mathtt{s}}) = L\prod_{i=1}^{n}\prod_{j=1}^{m}(\mathtt{x}_i - \mathtt{y}_j).$$

Ahora bien, si hacemos $\mathtt{x}_1 = \cdots = \mathtt{x}_n = -1$, $\mathtt{y}_1 = \cdots = \mathtt{y}_m = 0$ y $\mathtt{v}_n = \mathtt{w}_m = 1$ en las definiciones de $f_{\mathtt{v}}$ y $g_{\mathtt{w}}$ tenemos

$$f_{\mathtt{v}} = (\mathtt{t}+1)^n = \sum_{k=0}^{n} \binom{n}{k} \mathtt{t}^k \quad \& \quad g_{\mathtt{w}} = \mathtt{t}^m,$$

con lo que, para estos valores,

$$\operatorname{Res}(f_{\mathtt{v}}, g_{\mathtt{w}}) = \det \begin{bmatrix} 1 & \mathtt{v}_1 & \cdots & \mathtt{v}_n & 0 & 0 & \cdots & 0 \\ 0 & 1 & \mathtt{v}_1 & \cdots & \mathtt{v}_n & 0 & \cdots & 0 \\ \vdots & & \vdots & & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & 1 & \mathtt{v}_1 & \mathtt{v}_2 & \cdots & \mathtt{v}_n \\ 0 & 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & & & \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 1 \end{bmatrix} = 1.$$

Por otro lado, para esta sustitución se tiene $F(\mathtt{s}, \widehat{\mathtt{s}}) = (-1)^{nm} L$ y, como consecuencia de la igualdad (2.12) y la elección $\mathtt{v}_n = \mathtt{w}_m = 1$, deducimos

$$\begin{aligned} (-1)^{nm} L = F(\mathtt{s}, \widehat{\mathtt{s}}) &= 1^m \cdot 1^n F(\mathtt{s}, \widehat{\mathtt{s}}) \\ &= H(\mathtt{v}_0, \ldots, \mathtt{v}_{n-1}, 1; \mathtt{w}_0, \ldots, \mathtt{w}_{m-1}, 1) = \operatorname{Res}(f_{\mathtt{v}}, g_{\mathtt{w}}) = 1, \end{aligned}$$

es decir, $L = (-1)^{nm}$, como queríamos. □

Corolario VII.2.5 *Sean $A \subset B$ dos dominios tales que A es un subanillo de B. Sean f y g dos polinomios en $A[\mathtt{t}]$ de grado mayor o igual que 1. Supongamos que*

$$\begin{aligned} f(\mathtt{t}) &:= a_n(\mathtt{t}-\alpha_1)\cdots(\mathtt{t}-\alpha_n), \ \textit{donde } a_n \in A \quad \& \quad \alpha_1, \ldots, \alpha_n \in B, \\ g(\mathtt{t}) &:= b_m(\mathtt{t}-\beta_1)\cdots(\mathtt{t}-\beta_m), \ \textit{donde } b_m \in A \quad \& \quad \beta_1, \ldots, \beta_m \in B. \end{aligned}$$

Entonces, f y g comparten alguna raíz en B si y sólo si $\operatorname{Res}(f, g) = 0$.

Demostración. En la Proposición VII.2.3 probamos que existen $p, q \in A[\mathtt{t}]$ tales que

$$\operatorname{Res}(f, g) = f(\mathtt{t})p(\mathtt{t}) + g(\mathtt{t})q(\mathtt{t}).$$

Supongamos que f y g tienen una raíz común $b \in B$. Entonces, evaluando esta igualdad en b resulta $\operatorname{Res}(f, g) = f(b)p(b) + g(b)q(b) = 0$, lo que demuestra una implicación. Para la otra, deducimos del Teorema VII.2.4 que

$$0 = \operatorname{Res}(f, g) = (-1)^{nm} a_n^m b_m^n \prod_{i=1}^{n} \prod_{j=1}^{m} (\alpha_i - \beta_j).$$

Como A es dominio, el producto $(-1)^{nm}a_n^m b_m^n \neq 0$, luego $\alpha_i = \beta_j$ para ciertos $1 \leq i \leq n$ y $1 \leq j \leq m$, y ésta es una raíz común de f y g en B. □

Antes de probar algunas propiedades relevantes de la resultante enunciamos un resultado que demostraremos en el vol. III, y que hasta entonces emplearemos libremente.

Proposición VII.2.6 Dados un cuerpo K y un polinomio $f \in K[\mathtt{t}]$ de grado al menos 1, existen un cuerpo F que contiene a K como subcuerpo, enteros positivos $m_1, \ldots, m_r$, un elemento $a \in K$ y $\alpha_1, \ldots, \alpha_r \in F$ tales que

$$f(\mathtt{t}) = a \prod_{i=1}^{r} (\mathtt{t} - \alpha_i)^{m_i}.$$

Se dice que *f factoriza en $F[\mathtt{t}]$ como producto de factores de grado* 1.

Observaciones VII.2.7 (1) Si K es un subcuerpo del cuerpo $\mathbb{C}$ de los números complejos, el Teorema Fundamental del Álgebra afirma que podemos elegir el cuerpo F de la Proposición anterior como subcuerpo de $\mathbb{C}$.

(2) Si A es un dominio y $f \in A[\mathtt{t}]$ de grado $n \geq 1$, se tiene $\operatorname{Res}(f, \mathtt{t} - c) = f(c)$.

En efecto, sean $K := \operatorname{qf}(A)$ y F un cuerpo que contiene a K como subcuerpo y tal que f factoriza en $F[\mathtt{t}]$ como producto de factores de grado 1. Existen por tanto $a \in A$ y $\alpha_1, \ldots, \alpha_n \in F$ no necesariamente distintos tales que $f(\mathtt{t}) = a(\mathtt{t} - \alpha_1) \cdots (\mathtt{t} - \alpha_n)$. Por el Teorema VII.2.4 tenemos

$$\operatorname{Res}(f, \mathtt{t} - c) = (-1)^n a(\alpha_1 - c) \cdots (\alpha_n - c) = a_n(c - \alpha_1) \cdots (c - \alpha_n) = f(c).$$

(3) Sean A un dominio y $f, g, h \in A[\mathtt{t}]$ polinomios de grado ≥ 1. Entonces,

$$\operatorname{Res}(f, gh) = \operatorname{Res}(f, g) \operatorname{Res}(f, h).$$

En efecto, sean $K := \operatorname{qf}(A)$ y F un cuerpo que contiene a K como subcuerpo y tal que el producto fgh factoriza en $F[\mathtt{t}]$ como producto de factores de grado 1. Esto implica que f, g y h factorizan en $F[\mathtt{t}]$ como producto de factores de grado 1, luego existen

$$\alpha_1, \ldots, \alpha_n,\ \beta_1, \ldots, \beta_m,\ \gamma_1, \ldots, \gamma_r \in F \quad \& \quad a_n, b_m, c_r \in A$$

tales que

$$f(\mathtt{t}) = a_n(\mathtt{t} - \alpha_1) \cdots (\mathtt{t} - \alpha_n), \quad g(\mathtt{t}) = b_m(\mathtt{t} - \beta_1) \cdots (\mathtt{t} - \beta_m) \quad \&$$
$$h(\mathtt{t}) = c_r(\mathtt{t} - \gamma_1) \cdots (\mathtt{t} - \gamma_r).$$

Además,

$$gh = b_m c_r(\mathtt{t} - \beta_1)\cdots(\mathtt{t} - \beta_m)(\mathtt{t} - \gamma_1)\cdots(\mathtt{t} - \gamma_r).$$

Por tanto, aplicando el Teorema VII.2.4 se deduce que

$$\begin{aligned}\operatorname{Res}(f, gh) &= (-1)^{n(m+r)} a_n^{m+r} (b_m c_r)^n \prod_{i=1}^{n}\prod_{j,k}(\alpha_i - \beta_j)(\alpha_i - \gamma_k)\\ &= \Big((-1)^{nm} a_n^m b_m^n \prod_{i=1}^{n}\prod_{j=1}^{m}(\alpha_i - \beta_j)\Big)\Big((-1)^{nr} a_n^r c_r^n \prod_{i=1}^{n}\prod_{k=1}^{r}(\alpha_i - \gamma_k)\Big)\\ &= \operatorname{Res}(f, g)\operatorname{Res}(f, h).\end{aligned}$$

Observación VII.2.8 (Especialización) Sean $A \subset B$ dos dominios tales que A es un subanillo de B y sean $f, g \in A[\mathtt{x}_1, \ldots, \mathtt{x}_r]$ dos polinomios cuyos grados $\deg_{\mathtt{x}_r}(f) = n$ y $\deg_{\mathtt{x}_r}(g) = m$ con respecto a $\mathtt{x}_r$ son mayores o iguales a 1. Escribimos

$$f := \sum_{i=0}^{n} a_i \mathtt{x}_r^i \quad \& \quad g := \sum_{j=0}^{m} b_j \mathtt{x}_r^j,$$

donde cada $a_i, b_j \in A[\mathtt{x}_1, \ldots, \mathtt{x}_{r-1}]$. Se define la *resultante de f, g con respecto a la variable $\mathtt{x}_r$* como

$$\operatorname{Res}_{\mathtt{x}_r}(f, g) = \operatorname{Res}(f, g) \in A[\mathtt{x}_1, \ldots, \mathtt{x}_{r-1}],$$

es decir, viendo f y g como polinomios en la variable $\mathtt{x}_r$ con coeficientes en el anillo $A[\mathtt{x}_1, \ldots, \mathtt{x}_{r-1}]$. Sea $c := (c_1, \ldots, c_{r-1}) \in B^{r-1}$ tal que $a_n(c), b_m(c) \neq 0$. Entonces,

$$\operatorname{Res}_{\mathtt{x}_r}(f, g)(c) = \operatorname{Res}(f(c, \mathtt{x}_r), g(c, \mathtt{x}_r)),$$

donde $f(c, \mathtt{x}_r), g(c, \mathtt{x}_r) \in B[\mathtt{x}_r]$.

Este hecho es consecuencia del Teorema VII.2.4, que muestra que la resultante de dos polinomios de grados $n, m \geq 1$ es el resultado de sustituir los coeficientes de los polinomios en una fórmula polinómica con variables $\mathtt{v}_0, \mathtt{v}_1, \ldots, \mathtt{v}_n$ y $\mathtt{w}_0, \mathtt{w}_1, \ldots, \mathtt{w}_m$ y con coeficientes en $\mathbb{Z}$. Es decir, que la resultante es una *fórmula universal* que sólo depende de los grados de los polinomios de los que queramos calcularla, y no del valor de dichos coeficientes. La hipótesis $a_n(c) \neq 0 \neq b_m(c)$ garantiza que estos grados se preservan.

2.b. Discriminante de un polinomio. A continuación, dado un dominio A de característica 0, buscamos un procedimiento para detectar, a partir únicamente de sus coeficientes, si un polinomio $f \in A[\mathtt{t}]$ de grado ≥ 2 tiene raíces múltiples en algún cuerpo F que contenga como subcuerpo al cuerpo de fracciones K del dominio A. Por la Proposición V.2.5 esto significa que f y f' compartan alguna raíz en F, lo que equivale, por el Corolario VII.2.5, a que $\mathrm{Res}(f, f') = 0$. Por su utilidad en el vol. III, introducimos ahora el *discriminante* $\Delta(f)$ de f como el elemento de K que cumple la igualdad

$$a_n\Delta(f) = (-1)^{\frac{n(n-1)}{2}}\,\mathrm{Res}(f,f')$$
$$= (-1)^{\frac{n(n-1)}{2}}\det\begin{bmatrix} a_0 & a_1 & \cdots & a_n & 0 & 0 & \cdots & 0\\ 0 & a_0 & a_1 & \cdots & a_n & 0 & \cdots & 0\\ \vdots & & \vdots & & \vdots & \vdots & & \vdots\\ 0 & \cdots & 0 & a_0 & a_1 & a_2 & \cdots & a_n\\ a_1 & 2a_2 & \cdots & (n-1)a_{n-1} & na_n & 0 & \cdots & 0\\ 0 & a_1 & 2a_2 & \cdots & (n-1)a_{n-1} & na_n & \cdots & 0\\ \vdots & \vdots & & & \vdots & \vdots & & \vdots\\ 0 & 0 & \cdots & 0 & a_1 & 2a_2 & \cdots & na_n \end{bmatrix}$$

donde $f(\mathtt{t}) := \sum_{j=0}^{n} a_j\mathtt{t}^j$ y $a_n \neq 0$. Observando la última columna del determinante anterior deducimos que dicho determinante es múltiplo en A de a_n y, por tanto, $\Delta(f) \in A$. Además, definimos por convenio $\Delta(f) := 1$ si $\deg(f) = 1$.

Resumimos a continuación parte de la información anterior.

Corolario VII.2.9 *Sean A un dominio, $f \in A[\mathtt{t}]$ un polinomio de grado ≥ 2 y F un cuerpo que contiene al cuerpo de fracciones K de A como subcuerpo tal que f factoriza en $F[\mathtt{t}]$ como producto de factores de grado uno. Las siguientes afirmaciones son equivalentes:*

(1) *El polinomio f tiene una raíz múltiple en F.*

(2) *El discriminante $\Delta(f)$ de f es nulo.*

(3) *La resultante $\mathrm{Res}(f, f') = 0$.*

Teorema VII.2.10 *Sea n un entero positivo y consideremos los grupos de variables $\mathtt{t}$, $\mathtt{v} := (\mathtt{v}_0, \ldots, \mathtt{v}_n)$ y $\mathtt{x} := (\mathtt{x}_1, \ldots, \mathtt{x}_n)$, y el polinomio*

$$f_{\mathtt{v}}(\mathtt{t}) := \mathtt{v}_n(\mathtt{t} - \mathtt{x}_1)\cdots(\mathtt{t} - \mathtt{x}_n) = \mathtt{v}_0 + \mathtt{v}_1\mathtt{t} + \cdots + \mathtt{v}_n\mathtt{t}^n \in \mathbb{Z}[\mathtt{v}][\mathtt{t}].$$

Entonces, se cumple que

$$\Delta(f_{\mathtt{v}}) = \mathtt{v}_n^{2n-2}\prod_{1\leq i<j\leq n}(\mathtt{x}_i - \mathtt{x}_j)^2.$$

Demostración. La derivada de $f_{\mathtt{v}}$ con respecto a $\mathtt{t}$ es

$$f'_{\mathtt{v}}(\mathtt{t}) = \mathtt{v}_1 + 2\mathtt{v}_2\mathtt{t} + \cdots + n\mathtt{v}_n\mathtt{t}^{n-1} = n\mathtt{v}_n(\mathtt{t}-\mathtt{y}_1)\cdots(\mathtt{t}-\mathtt{y}_{n-1}).$$

Por el Teorema VII.2.4 deducimos que

$$\operatorname{Res}(f_{\mathtt{v}}, f'_{\mathtt{v}}) = (-1)^{n(n-1)}\mathtt{v}_n^{n-1}\mathtt{v}_n^n n^n \prod_{i=1}^{n}\prod_{j=1}^{n-1}(\mathtt{x}_i - \mathtt{y}_j).$$

Nótese que $n(n-1)$ es un número par y que $n\mathtt{v}_n\prod_{j=1}^{n-1}(\mathtt{x}_i-\mathtt{y}_j) = f'_{\mathtt{v}}(\mathtt{x}_i)$. De este modo,

$$\operatorname{Res}(f_{\mathtt{v}}, f'_{\mathtt{v}}) = \mathtt{v}_n^{n-1}\prod_{i=1}^{n} f'_{\mathtt{v}}(\mathtt{x}_i).$$

Como $f_{\mathtt{v}}(\mathtt{t}) = \mathtt{v}_n\prod_{i=1}^{n}(\mathtt{t}-\mathtt{x}_i)$, tenemos que $f'_{\mathtt{v}}(\mathtt{t}) = \mathtt{v}_n\sum_{i=1}^{n}\prod_{k\neq i}(\mathtt{t}-\mathtt{x}_k)$ y, por tanto,

$$f'_{\mathtt{v}}(\mathtt{x}_i) = \mathtt{v}_n\prod_{k\neq i}(\mathtt{x}_i - \mathtt{x}_k).$$

Así, al sustituir resulta

$$\begin{aligned}\operatorname{Res}(f_{\mathtt{v}}, f'_{\mathtt{v}}) = \mathtt{v}_n^{n-1}\prod_{i=1}^{n}\Big(\mathtt{v}_n\prod_{k\neq i}(\mathtt{x}_i-\mathtt{x}_k)\Big) &= \mathtt{v}_n^{2n-1}\prod_{i=1}^{n}\prod_{k\neq i}(\mathtt{x}_i-\mathtt{x}_k)\\ &= (-1)^{\frac{n(n-1)}{2}}\mathtt{v}_n^{2n-1}\prod_{1\leq i<k\leq n}(\mathtt{x}_i-\mathtt{x}_k)^2.\end{aligned}$$

Concluimos por tanto que $\Delta(f_{\mathtt{v}}) = \mathtt{v}_n^{2n-2}\prod_{1\leq i<j\leq n}(\mathtt{x}_i-\mathtt{x}_j)^2$. □

Proposición VII.2.11 *Sean A un dominio y $f, g \in A[\mathtt{t}]$ dos polinomios de grado ≥ 1. Entonces,*

(1) *Para cada $a \in A$ se tiene la igualdad $\Delta(f) = \Delta(f(\mathtt{t}+a))$.*

(2) $\Delta(fg) = \Delta(f)\Delta(g)\operatorname{Res}(f,g)^2$.

Demostración. Fijamos un cuerpo F que contiene como subcuerpo al cuerpo de fracciones de A y tal que el producto fg factoriza en $F[\mathtt{t}]$ como producto de factores de grado uno. Así, tanto f como g factorizan en $F[\mathtt{t}]$ como producto de factores de grado uno.

(1) Si $\deg(f) = 1$ los dos miembros de la igualdad a probar valen 1. Supongamos que $\deg(f) = n \geq 2$ y sean $b \in A$ y $\alpha_1, \ldots, \alpha_n \in F$, no necesariamente distintos, tales que $f(\mathtt{t}) = b(\mathtt{t} - \alpha_1) \cdots (\mathtt{t} - \alpha_n)$, por lo que

$$f(\mathtt{t} + a) = b(\mathtt{t} - \beta_1) \cdots (\mathtt{t} - \beta_n),$$

donde cada $\beta_k := \alpha_k - a$. En particular, $\alpha_i - \alpha_k = \beta_i - \beta_k$ para $1 \leq i < j \leq n$, y se deduce de VII.2.10 que

$$\Delta\big(f(\mathtt{t} + a)\big) = b^{2n-2} \prod_{1 \leq i < k \leq n} (\beta_i - \beta_k)^2 = b^{2n-2} \prod_{1 \leq i < k \leq n} (\alpha_i - \alpha_k)^2 = \Delta(f).$$

(2) Sean $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m \in F$ y $a_n, b_m \in A$, tales que

$$f(\mathtt{t}) = a_n(\mathtt{t} - \alpha_1) \cdots (\mathtt{t} - \alpha_n) \quad \& \quad g(\mathtt{t}) = b_m(\mathtt{t} - \beta_1) \cdots (\mathtt{t} - \beta_m),$$

y por tanto

$$f(\mathtt{t})g(\mathtt{t}) = a_n b_m(\mathtt{t} - \alpha_1) \cdots (\mathtt{t} - \alpha_n)(\mathtt{t} - \beta_1) \cdots (\mathtt{t} - \beta_m).$$

Se deduce de los Teoremas VII.2.10 y VII.2.4 que

$$\begin{aligned}
\Delta(fg) &= (a_n b_m)^{2(n+m)-2} \prod_{i<k} (\alpha_i - \alpha_k)^2 \prod_{j<\ell} (\beta_j - \beta_\ell)^2 \prod_{i=1}^{n} \prod_{j=1}^{m} (\alpha_i - \beta_j)^2 \\
&= \Big(a_n^{2n-2} \prod_{i<k} (\alpha_i - \alpha_k)^2\Big) \Big(b_m^{2m-2} \prod_{j<\ell} (\beta_j - \beta_\ell)^2\Big) \\
&\cdot \Big(a_n^m b_m^n \prod_{i=1}^{n} \prod_{j=1}^{m} (\alpha_i - \beta_j)\Big)^2 = \Delta(f)\Delta(g)\operatorname{Res}(f, g)^2.
\end{aligned}$$

□

Ejemplos VII.2.12 (1) Sea $f(\mathtt{t}) = a_2\mathtt{t}^2 + a_1\mathtt{t} + a_0$ un polinomio de grado 2. Entonces

$$\Delta(f) = a_1^2 - 4a_2a_0.$$

En particular, $\Delta(\mathtt{t}^2 + b\mathtt{t} + c) = b^2 - 4c$.

(2) Sea $f(\mathtt{t}) = a_3\mathtt{t}^3 + a_2\mathtt{t}^2 + a_1\mathtt{t} + a_0$ un polinomio de grado 3. Desarrollando el determinante que aparece en 2.b resulta

$$\Delta(f) = -4a_1^3a_3 + a_1^2a_2^2 + 18a_0a_1a_2a_3 - 4a_0a_2^3 - 27a_0^2a_3^2.$$

En particular, $\Delta(\mathtt{t}^3 + p\mathtt{t} + q) = -4p^3 - 27q^2$.

(3) Empleando directamente la definición que proporciona 2.b se obtienen los siguientes discriminantes:

(3.1) $\Delta(\mathtt{t}^4 + p\mathtt{t}^2 + q\mathtt{t} + r) = 256r^3 - 128p^2r^2 + 144pq^2r + 16p^4r - 4p^3q^2 - 27q^4$.

(3.2) $\Delta(\mathtt{t}^n - a) = (-1)^{\frac{(n+2)(n-1)}{2}} n^n a^{n-1}$.

(3.3) $\Delta(\mathtt{t}^5 + a\mathtt{t} + b) = 2^8 a^5 + 5^5 b^4$.

2.c. Teorema de los ceros de Hilbert. Dedicamos la última parte de esta sección a enunciar y demostrar el llamado Teorema de los ceros de Hilbert siguiendo la prueba publicada por el profesor Enrique Arrondo en Amer. Math. Monthly **113** no 2, 169-171, (2006), que sólo emplea argumentos de Álgebra Lineal. Necesitamos un resultado preliminar.

Lema VII.2.13 *Sean K un cuerpo infinito y $f \in K[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ un polinomio no nulo de grado d.*

(1) *Si f es homogéneo, existe $(b_1, \ldots, b_{n-1}) \in K^{n-1}$ tal que*

$$f(b_1, \ldots, b_{n-1}, 1) \in K \setminus \{0\}.$$

(2) *Existe $(b_1, \ldots, b_{n-1}) \in K^{n-1}$ tal que el coeficiente de $\mathtt{x}_n^d$ del polinomio*

$$h(\mathtt{x}_1, \ldots, \mathtt{x}_n) := f(\mathtt{x}_1 + b_1\mathtt{x}_n, \ldots, \mathtt{x}_{n-1} + b_{n-1}\mathtt{x}_n, \mathtt{x}_n)$$

es un elemento no nulo de K.

Demostración. (1) Por el Corolario VII.1.10 existe $a := (a_1, \ldots, a_n) \in K^n$ tal que $a_n \neq 0$ y $f(a) \neq 0$. Definimos $b_k := a_k/a_n \in K$ para $1 \leq k \leq n$. Nótese que $b_n = 1$ y, por ser f homogéneo de grado $d := \deg(f)$, se deduce de VII.1.5 (4) que

$$0 \neq f(a) = f(a_n b_1, \ldots, a_n b_n) = a_n^d f(b_1, \ldots, b_{n-1}, 1),$$

luego $f(b_1, \ldots, b_{n-1}, 1) \neq 0$.

(2) Escribimos $f = \sum_{j=0}^{d} f_j$ donde cada f_j es nulo o un polinomio homogéneo de grado j y $f_d \neq 0$. Aplicando a f_d el apartado (1) existe $(b_1, \ldots, b_{n-1}) \in K^{n-1}$ tal que $f_d(b_1, \ldots, b_{n-1}, 1) \neq 0$. Como

$$\begin{aligned} h(\mathtt{x}_1, \ldots, \mathtt{x}_n) &= f(\mathtt{x}_1 + b_1\mathtt{x}_n, \ldots, \mathtt{x}_{n-1} + b_{n-1}\mathtt{x}_n, \mathtt{x}_n) \\ &= \sum_{j=0}^{d} f_j(\mathtt{x}_1 + b_1\mathtt{x}_n, \ldots, \mathtt{x}_{n-1} + b_{n-1}\mathtt{x}_n, \mathtt{x}_n), \end{aligned}$$

el coeficiente en h de la potencia $\mathtt{x}_n^d$ coincide con el coeficiente de $\mathtt{x}_n^d$ en el polinomio $f_d(\mathtt{x}_1 + b_1\mathtt{x}_n, \ldots, \mathtt{x}_{n-1} + b_{n-1}\mathtt{x}_n, \mathtt{x}_n)$. Pero el monomio en $\mathtt{x}_n^d$ de este polinomio es

$$f_d(b_1\mathtt{x}_n, \ldots, b_{n-1}\mathtt{x}_n, \mathtt{x}_n) = f_d(b_1, \ldots, b_{n-1}, 1)\mathtt{x}_n^d,$$

es decir, el coeficiente en cuestión es $f_d(b_1, \ldots, b_{n-1}, 1) \in K \setminus \{0\}$. □

Antes de enunciar el Teorema de los ceros necesitamos introducir una noción que también emplearemos en el vol. III.

Definición y Observación VII.2.14 (1) Se dice que un cuerpo F es *algebraicamente cerrado* si cada polinomio $f \in F[\mathtt{t}]$ de grado mayor o igual que 1 factoriza en $F[\mathtt{t}]$ como producto de factores de grado 1.

(2) El Teorema Fundamental del Álgebra dice que el cuerpo $\mathbb{C}$ de los números complejos es algebraicamente cerrado.

Teorema VII.2.15 (Forma débil del Teorema de los ceros) *Sean K un cuerpo algebraicamente cerrado y $\mathfrak{a}$ un ideal propio del anillo de polinomios $K[\mathtt{x}_1, \ldots, \mathtt{x}_n]$. Entonces, existe $a := (a_1, \ldots, a_n) \in K^n$ tal que $f(a) = 0$ para cada $f \in \mathfrak{a}$.*

Demostración. Probamos el teorema por inducción sobre n. Si $n = 1$ el anillo $K[\mathtt{x}_1]$ es, por la Proposición V.1.8, un dominio de ideales principales, luego existe $g \in \mathfrak{a}$ tal que $\mathfrak{a} = gK[\mathtt{x}_1]$. El polinomio g no es constante ya que $\mathfrak{a}$ es un ideal propio, luego por ser K algebraicamente cerrado existe $a \in K$ tal que $g(a) = 0$. Para cada $f \in \mathfrak{a}$ existe $h \in K[\mathtt{x}_1]$ tal que $f = hg$, y por ello $f(a) = h(a)g(a) = 0$, así que el punto a cumple lo requerido.

Supongamos $n > 1$. El resultado es trivial si $\mathfrak{a}$ es el ideal nulo, así que suponemos que no lo es y, aplicando el Lema VII.2.13 a un polinomio no nulo de $\mathfrak{a}$, existe $(b_1, \ldots, b_{n-1}) \in K^{n-1}$ tal que tras un cambio de variables de la forma

$$(\mathtt{x}_1, \ldots, \mathtt{x}_n) \mapsto (\mathtt{y}_1, \ldots, \mathtt{y}_n) := (\mathtt{x}_1 + b_1\mathtt{x}_n, \ldots, \mathtt{x}_{n-1} + b_{n-1}\mathtt{x}_n, \mathtt{x}_n),$$

que no afecta al enunciado, podemos suponer que el ideal $\mathfrak{a}$ contiene un polinomio g de grado d de la forma

$$g := g_0(\mathtt{x}') + g_1(\mathtt{x}')\mathtt{x}_n + \cdots + g_{d-1}(\mathtt{x}')\mathtt{x}_n^{d-1} + \mathtt{x}_n^d,$$

donde $\mathtt{x}' := (\mathtt{x}_1, \ldots, \mathtt{x}_{n-1})$ y cada $g_j \in A := K[\mathtt{x}_1, \ldots, \mathtt{x}_{n-1}]$.

El ideal $\mathfrak{a}_1 := \mathfrak{a} \cap A \neq A$ porque $1 \notin \mathfrak{a}$. Por la hipótesis de inducción, existe un punto $a' := (a_1, \ldots, a_{n-1}) \in K^{n-1}$ tal que $f(a') = 0$ para cada $f \in \mathfrak{a}_1$. El punto clave en la prueba es demostrar que

$$\mathfrak{b} := \{f(a', \mathtt{x}_n) : \ f \in \mathfrak{a}\}$$

es un ideal propio de $K[\mathtt{x}_n]$. Desde luego $\mathfrak{b} \neq \{0\}$, pues $0 \neq g(a', \mathtt{x}_n) \in \mathfrak{b}$. Además, la comprobación de que $\mathfrak{b}$ es ideal es inmediata, luego se trata de probar que $\mathfrak{b} \neq K[\mathtt{x}_n]$. En caso contrario existiría $f \in \mathfrak{a}$ tal que $1 = f(a', \mathtt{x}_n)$. Si $m = \deg(f)$ escribimos

$$f(\mathtt{x}_1, \ldots, \mathtt{x}_n) = f_0(\mathtt{x}') + f_1(\mathtt{x}')\mathtt{x}_n + \cdots + f_m(\mathtt{x}')\mathtt{x}_n^m,$$

donde cada $f_j \in A$. Como A es dominio se sigue de la Proposición VII.2.3 que existen polinomios $p, q \in A[\mathtt{x}_n]$ tales que $R := \mathrm{Res}_{\mathtt{x}_n}(f, g) = fp + gq \in \mathfrak{a}$. Como, además, $R \in A$ concluimos que $R \in \mathfrak{a}_1$, y por tanto $R(a') = 0$, ya que todos los polinomios del ideal $\mathfrak{a}_1$ se anulan en el punto a'. Sin embargo, como

$$1 = f(a', \mathtt{x}_n) = f_0(a') + f_1(a')\mathtt{x}_n + \cdots + f_m(a')\mathtt{x}_n^m,$$

se tiene $f_0(a') = 1$ y $f_j(a') = 0$ para $1 \leq j \leq m$. Así, al evaluar $R(a')$ obtenemos

$$R(a') = \det \begin{bmatrix} f_0(a') & f_1(a') & \cdots & f_m(a') & 0 & 0 & \cdots & 0 \\ 0 & f_0(a') & f_1(a') & \cdots & f_m(a') & 0 & \cdots & 0 \\ \vdots & & \vdots & & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & f_0(a') & f_1(a') & f_2(a') & \cdots & f_m(a') \\ g_0(a') & g_1(a') & \cdots & g_{d-1}(a') & 1 & 0 & \cdots & 0 \\ 0 & g_0(a') & g_1(a') & \cdots & g_{d-1}(a') & 1 & \cdots & 0 \\ \vdots & \vdots & & & \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 & g_0(a') & g_1(a') & \cdots & 1 \end{bmatrix}$$

$$= \det \begin{bmatrix} 1 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & & \vdots & & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & 1 & 0 & 0 & \cdots & 0 \\ g_0(a') & g_1(a') & \cdots & g_{d-1}(a') & 1 & 0 & \cdots & 0 \\ 0 & g_0(a') & g_1(a') & \cdots & g_{d-1}(a') & 1 & \cdots & 0 \\ \vdots & \vdots & & & \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 & g_0(a') & g_1(a') & \cdots & 1 \end{bmatrix} = 1,$$

y esto contradice que $R(a') = 0$.

Así, $\mathfrak{b}$ es un ideal propio de $K[\mathtt{x}_n]$, luego es un ideal principal generado por un polinomio $h \in K[\mathtt{x}_n] \setminus K$. Por ser K algebraicamente cerrado existe $a_n \in K$ tal que $h(a_n) = 0$. Así, para cada $f \in \mathfrak{a}$ el polinomio $f(a', \mathtt{x}_n) \in \mathfrak{b} = hK[\mathtt{x}_n]$, luego existe $p \in K[\mathtt{x}_n]$ tal que $f(a', \mathtt{x}_n) = h(\mathtt{x}_n)p(\mathtt{x}_n)$, por lo que el punto $a := (a', a_n) \in K^n$ cumple que $f(a) = f(a', a_n) = h(a_n)p(a_n) = 0$. □

Observaciones y Notaciones VII.2.16 (1) En el Teorema anterior la hipótesis de que K sea algebraicamente cerrado es esencial. En efecto, si no lo es existe un polinomio no constante $f \in K[\mathtt{x}_1]$ sin raíces en K, luego no existe ningún punto $a \in K^n$ en el que se anulen todos los polinomios del ideal $\mathfrak{a}$ de $K[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ generado por f.

(2) Para enunciar la forma fuerte del Teorema de los ceros de Hilbert necesitamos introducir más notación. Dados un cuerpo K y un ideal $\mathfrak{a}$ del anillo de polinomios $A := K[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ se define *el conjunto de ceros* de $\mathfrak{a}$ en K^n como

$$\mathcal{Z}(\mathfrak{a}) := \{x \in K^n : \ f(x) = 0 \ \ \forall f \in \mathfrak{a}\}.$$

Los subconjuntos de K^n de la forma $\mathcal{Z}(\mathfrak{a})$, donde $\mathfrak{a}$ es un ideal de A, se denominan *subconjuntos algebraicos de* K^n. Si $\mathfrak{a} := fA$ es un ideal principal se tiene

$$\mathcal{Z}(\mathfrak{a}) = \mathcal{Z}(f) := \{x \in K^n : \ f(x) = 0\}.$$

(3) Dado un subconjunto $M \subset K^n$ se define *el ideal de* M como

$$\mathcal{J}(M) := \{f \in A : \ f(x) = 0 \ \ \forall x \in M\}.$$

Nótese que $\mathcal{J}(M)$ es un ideal radical, véase el Ejercicio I.9, pues si $f^k \in \mathcal{J}(M)$ entonces $f(x)^k = 0$ para cada $x \in M$ y, como K es un dominio, $f(x) = 0$, o sea, $f \in \mathcal{J}(M)$.

Teorema VII.2.17 (Forma fuerte del Teorema de los ceros) *Dados un cuerpo algebraicamente cerrado K y un ideal $\mathfrak{a}$ de $K[\mathtt{x}] := K[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ se cumple la igualdad*

$$\mathcal{J}\big(\mathcal{Z}(\mathfrak{a})\big) = \sqrt{\mathfrak{a}}.$$

Demostración. La inclusión $\mathfrak{a} \subset \mathcal{J}(\mathcal{Z}(\mathfrak{a}))$ es inmediata. De aquí se deduce el contenido $\sqrt{\mathfrak{a}} \subset \mathcal{J}(\mathcal{Z}(\mathfrak{a}))$ pues acabamos de comprobar que el ideal $\mathcal{J}(\mathcal{Z}(\mathfrak{a}))$ es radical. Para demostrar la inclusión recíproca empleamos el denominado truco

de Rabinowitsch. Aunque no es imprescindible utilizamos, por comodidad, el Teorema de la base de Hilbert, V.2.15, en virtud del cual existen polinomios $f_1, \ldots, f_m \in \mathfrak{a}$ tales que $\mathfrak{a} = (f_1, \ldots, f_m)K[\mathtt{x}]$. Ahora, dado $f \in \mathcal{J}(\mathcal{Z}(\mathfrak{a})) \setminus \{0\}$ consideramos el ideal

$$\mathfrak{b} := \big(f_1, \ldots, f_m, (\mathtt{x}_{n+1}f - 1)\big)K[\mathtt{x}, \mathtt{x}_{n+1}].$$

Obsérvese que el conjunto $\mathcal{Z}(\mathfrak{b})$ de ceros de $\mathfrak{b}$ es vacío, pues si contuviese algún punto $(a, a_{n+1}) \in K^n \times K = K^{n+1}$ tendríamos $f_j(a) = 0$ para $1 \leq j \leq m$ y, además, $a_{n+1}f(a) = 1$. Sin embargo, $f(a) = 0$ ya que $a \in \mathcal{Z}(\mathfrak{a})$, lo que contradice la igualdad $1 = a_{n+1}f(a)$. Por tanto, $Z(\mathfrak{b}) = \varnothing$ y esto implica, por la forma débil del Teorema de los ceros, que el ideal $\mathfrak{b}$ es el anillo total $K[\mathtt{x}, \mathtt{x}_{n+1}]$. Así, existen $h_1, \ldots, h_{m+1} \in K[\mathtt{x}, \mathtt{x}_{n+1}]$ tales que

$$1 = f_1h_1 + \cdots + f_mh_m + (\mathtt{x}_{n+1}f - 1)h_{m+1}. \tag{2.14}$$

Denotemos $K(\mathtt{x})$ el cuerpo de fracciones del anillo de polinomios $K[\mathtt{x}]$ y consideramos en $K(\mathtt{x})[\mathtt{x}_{n+1}]$ la evaluación $\mathtt{x}_{n+1} := 1/f$, que efectuada en la igualdad (2.14) nos proporciona

$$1 = f_1(\mathtt{x})h_1(\mathtt{x}, 1/f(\mathtt{x})) + \cdots + f_m(\mathtt{x})h_m(\mathtt{x}, 1/f(\mathtt{x})).$$

Multiplicando los dos miembros de esta igualdad por f^k, donde k es suficientemente grande para eliminar los denominadores, obtenemos una expresión $f^k = f_1g_1 + \cdots + f_mg_m$, donde cada $g_j \in K[\mathtt{x}]$, y por tanto $f \in \sqrt{\mathfrak{a}}$, con lo que concluye la prueba. □

Corolario VII.2.18 *Sean K un cuerpo, n un número entero positivo y denotemos $K[\mathtt{x}] := K[\mathtt{x}_1, \ldots, \mathtt{x}_n]$.*

(1) *Para cada $a := (a_1, \ldots, a_n) \in K^n$ el ideal $\mathfrak{m}_a := (\mathtt{x}_1 - a_1, \ldots, \mathtt{x}_n - a_n)K[\mathtt{x}]$ es el ideal formado por todos los polinomios que se anulan en a. Por ello es maximal y $K[\mathtt{x}]/\mathfrak{m}_a \cong K$.*

(2) *Si $\mathfrak{m}$ es un ideal maximal del anillo de polinomios $K[\mathtt{x}]$ y $a \in \mathcal{Z}(\mathfrak{m})$, entonces $\mathfrak{m} = \mathfrak{m}_a$ y $\mathcal{Z}(\mathfrak{m}) = \{a\}$. En particular, el conjunto $\mathcal{Z}(\mathfrak{m})$ no contiene dos puntos distintos.*

(3) *Si K es algebraicamente cerrado y $\mathrm{Max}(K[\mathtt{x}])$ es el conjunto de ideales maximales de $K[\mathtt{x}]$, la aplicación*

$$\psi : K^n \to \mathrm{Max}(K[\mathtt{x}]),\ a \mapsto \mathfrak{m}_a$$

es una biyección cuya inversa hace corresponder a cada ideal maximal $\mathfrak{m}$ de $K[\mathtt{x}]$ el único punto de K^n en el que se anulan todos los polinomios de $\mathfrak{m}$.

Demostración. (1) El homomorfismo

$$\mathrm{ev}_a : K[\mathtt{x}] \to K,\ f \mapsto f(a)$$

es sobreyectivo, pues cada polinomio constante coincide con su valor en a, y su núcleo es un ideal maximal ya que, por el Primer Teorema de isomorfía, $A/\ker \mathrm{ev}_a \cong K$ es un cuerpo.

Basta por tanto probar que $\mathfrak{m}_a = \ker \mathrm{ev}_a$. Cada resta $\mathtt{x}_i - a_i$ se anula en el punto a, lo que demuestra la inclusión $\mathfrak{m}_a \subset \ker \mathrm{ev}_a$. Probamos el contenido recíproco por inducción sobre n.

El caso $n = 1$ es consecuencia de la Regla de Ruffini. Si $n > 1$ y $f \in \ker \mathrm{ev}_a$ dividimos f entre $\mathtt{x}_n - a_n$ en el anillo $A[\mathtt{x}_n]$, donde $A := K[\mathtt{x}_1, \ldots, \mathtt{x}_{n-1}]$. Así, existen $q_n, r_n \in A$ tales que

$$f = (\mathtt{x}_n - a_n)q_n + r_n \quad \& \quad \deg_{\mathtt{x}_n}(r_n) < \deg_{\mathtt{x}_n}(\mathtt{x}_n - a_n) = 1,$$

o sea, $r_n \in A$. Si $a' := (a_1, \ldots, a_{n-1})$ se tiene

$$r_n(a') = r_n(a) = f(a) - (a_n - a_n)q_n(a) = 0$$

y, por hipótesis de inducción, existen polinomios $q_1, \ldots, q_{n-1} \in A$, tales que

$$r_n = \sum_{j=1}^{n-1} (\mathtt{x}_j - a_j)q_j \quad \Longrightarrow \quad f = (\mathtt{x}_n - a_n)q_n + r_n = \sum_{j=1}^{n} (\mathtt{x}_j - a_j)q_j \in \mathfrak{m}_a.$$

(2) Como $a \in \mathcal{Z}(\mathfrak{m})$ cada f de $\mathfrak{m}$ se anula en a, o sea, $\mathfrak{m} \subset \mathfrak{m}_a$. Así, como $\mathfrak{m}$ es maximal, $\mathfrak{m} = \mathfrak{m}_a$, luego si $b := (b_1, \ldots, b_n) \in \mathcal{Z}(\mathfrak{m})$ se tiene $b_j - a_j = 0$ para cada j, es decir, $b = a$.

(3) Por el apartado (1) el ideal $\mathfrak{m}_a$ es maximal, luego ψ está bien definida. La inyectividad se deduce de (2), pues si a y b son puntos de K^n distintos, también lo son $\mathfrak{m}_a$ y $\mathfrak{m}_b$, ya que $\mathcal{Z}(\mathfrak{m}_a) = \{a\} \neq \{b\} = \mathcal{Z}(\mathfrak{m}_b)$.

Para la sobreyectividad, sea $\mathfrak{m}$ un ideal maximal de A. Por la forma débil del Teorema de los ceros existe $a \in \mathcal{Z}(\mathfrak{m})$. Hemos probado en el apartado (2) que esto implica que $\mathfrak{m} = \mathfrak{m}_a$, lo que termina la demostración. □

Observación VII.2.19 Si K no es algebraicamente cerrado la aplicación ψ de VII.2.18 (3) no es sobreyectiva. En efecto, vimos en VII.2.16 que existe un ideal propio $\mathfrak{a}$ de $K[\mathtt{x}]$ tal que $\mathcal{Z}(\mathfrak{a}) = \varnothing$. Por I.2.9 existe un ideal maximal $\mathfrak{m}$ de $K[\mathtt{x}]$ que contiene al ideal $\mathfrak{a}$, luego $\mathcal{Z}(\mathfrak{m})$ es vacío, así que $\mathfrak{m} \neq \mathfrak{m}_a$ para cada $a \in K^n$ pues $\mathcal{Z}(\mathfrak{m}_a) = \{a\}$.

Ejercicios y problemas propuestos

Número VII.1 Sean K un cuerpo y $f_1, f_2 \in K[\mathtt{x},\mathtt{y}]$ dos polinomios homogéneos primos entre sí de grados $d \geq 1$ y $d+1$, respectivamente. Demostrar que el polinomio $f := f_1 + f_2$ es irreducible en $K[\mathtt{x},\mathtt{y}]$.

Número VII.2 Sea $g \in \mathbb{R}[\mathtt{x}_1, \ldots, \mathtt{x}_{n-1}]$ un polinomio no nulo tal que $g(x) \geq 0$ para cada $x \in \mathbb{R}^{n-1}$. Demostrar que el polinomio $f := \mathtt{x}_n^2 + g \in \mathbb{R}[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ es irreducible.

Número VII.3 Estudiar la irreducibilidad en $\mathbb{C}[\mathtt{x},\mathtt{y}]$ de los siguientes polinomios:

$$f_1 := \mathtt{x}^2\mathtt{y}^5 + \mathtt{x}^3 + \mathtt{x}\mathtt{y}^2 + \mathtt{y}^2 + \mathtt{x} - 1, \quad f_2 := \mathtt{x}^2\mathtt{y}^5 + \mathtt{y}\mathtt{x}^3 - \mathtt{x}^2\mathtt{y}^2 + \mathtt{y} - 1,$$
$$f_3 := \mathtt{x}^3 + \mathtt{x}^2\mathtt{y} - 2\mathtt{x}\mathtt{y}^2 + 3\mathtt{x}\mathtt{y}^3 + 3\mathtt{y}^4.$$

Número VII.4 ¿Es irreducible en $\mathbb{R}[\mathtt{x},\mathtt{y}]$ el polinomio

$$f := -\mathtt{x} + \mathtt{y} + \mathtt{x}^2 + \mathtt{x}\mathtt{y} + \mathtt{x}^2\mathtt{y} + \mathtt{x}^2\mathtt{y}^2 + \mathtt{x}^2\mathtt{y}^3 + \mathtt{x}^2\mathtt{y}^4?$$

Número VII.5 (1) Probar que el ideal $\mathfrak{a}$ del anillo $\mathbb{R}[\mathtt{x},\mathtt{y}]$ generado por $f := \mathtt{x}^2 + 1$ y $g := \mathtt{y}^2 + 2$ no es primo y que es intersección de los ideales maximales

$$\mathfrak{m}_1 := (f, \mathtt{y} - \sqrt{2}\mathtt{x})\mathbb{R}[\mathtt{x},\mathtt{y}] \quad \& \quad \mathfrak{m}_2 := (f, \mathtt{y} + \sqrt{2}\mathtt{x})\mathbb{R}[\mathtt{x},\mathtt{y}].$$

(2) ¿Cuáles son los ideales primos de $\mathbb{R}[\mathtt{x},\mathtt{y}]$ que contienen al ideal $\mathfrak{a}$?

Número VII.6 ¿Es primo alguno de los ideales $\mathfrak{a} := (2, \mathtt{x}^2 + 1, \mathtt{y})$, $\mathfrak{b} := (3, \mathtt{x}^2 + 1, \mathtt{y}^2 + 1)$ y $\mathfrak{m} := (3, \mathtt{x}^2 + 1, \mathtt{y})$ del anillo $\mathbb{Z}[\mathtt{x},\mathtt{y}]$? ¿Es maximal alguno de ellos?

Número VII.7 Demostrar que el único polinomio $f \in \mathbb{C}[\mathtt{x},\mathtt{y}]$ que se anula en todos los puntos del producto $\mathbb{Z}^+ \times \mathbb{Z}^+$ es el polinomio nulo.

Número VII.8 ¿Cuánto vale la suma de los inversos de las raíces en $\mathbb{C}$ del polinomio $f(\mathtt{t}) := \mathtt{t}^3 - 2\mathtt{t}^2 + 3\mathtt{t} - 4$? Calcular la suma de los cuadrados de dichas raíces.

Número VII.9 Sean a, b y c tres números reales positivos cuyo producto vale 1 y cuya suma es mayor que la suma de sus inversos. Demostrar que exactamente uno de los tres es mayor que 1.

Número VII.10 Sean $r \in \mathbb{C}$ y $f(\mathtt{t}) := 3\mathtt{t}^2 + 3r\mathtt{t} + r^2 - 1 \in \mathbb{C}[\mathtt{t}]$ cuyas raíces $u, v \in \mathbb{C}$ no son necesariamente distintas. Probar que $f(u^3) = f(v^3)$.

Número VII.11 Hallar los polinomios mónicos de $\mathbb{C}[\mathtt{t}]$ de grado 3 cuyas raíces, no necesariamente distintas, cumplen que dos de sus medias aritméticas son raíces de su derivada.

Número VII.12 Sea $h \in \mathbb{R}[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ un polinomio no nulo. Demostrar que el conjunto $D_h := \{x \in \mathbb{R}^n : h(x) \neq 0\}$ es denso en $\mathbb{R}^n$ con su topología usual.

(2) Sea $f(\mathtt{t}) := \sum_{k=0}^{n} a_k \binom{n}{k} \mathtt{t}^k \in \mathbb{R}[\mathtt{t}]$ un polinomio de grado $n \geq 2$ con n raíces reales distintas. Probar que

$$a_{k-1}a_{k+1} < a_k^2 \text{ para } 1 \leq k \leq n-1.$$

(3) Sean $\mathtt{s}_0 := 1$ y $\mathtt{s}_1, \ldots, \mathtt{s}_n$ los polinomios simétricos elementales en $\mathbb{Z}[\mathtt{x}_1, \ldots, \mathtt{x}_n]$. Demostrar que para $1 \leq k \leq n-1$ el polinomio homogéneo y simétrico

$$g_k := k(n-k)\mathtt{s}_{n-k}^2 - (k+1)(n-k+1)\mathtt{s}_{n-k-1}\mathtt{s}_{n-k+1}$$

es *semidefinido positivo,* es decir, $g_k(x) \geq 0$ para cada $x \in \mathbb{R}^n$.

Número VII.13 Sea $f \in \mathbb{R}[\mathtt{t}]$ un polinomio sin raíces múltiples en $\mathbb{C}$ y que tiene n raíces en $\mathbb{C} \setminus \mathbb{R}$. Probar que el discriminante de f es positivo si y sólo si n es múltiplo de 4.

Número VII.14 Probar que tres números no nulos $x, y, z \in \mathbb{C}$, convenientemente ordenados, son términos consecutivos de una progresión geométrica si y sólo si

$$(xy + xz + yz)^3 = xyz(x + y + z)^3.$$

Número VII.15 Encontrar las soluciones reales del sistema de ecuaciones

$$\begin{cases} \mathtt{xyz} & = & 8 \\ \mathtt{xz}^2 + \mathtt{yx}^2 + \mathtt{zy}^2 & = & 73 \\ \mathtt{x}(\mathtt{y}-\mathtt{z})^2 + \mathtt{y}(\mathtt{x}-\mathtt{z})^2 + \mathtt{z}(\mathtt{x}-\mathtt{y})^2 & = & 98 \end{cases}$$

Número VII.16 Sean $m, n \in \mathbb{C} \setminus \{0\}$ y consideramos los polinomios

$$f(\mathtt{t}) := \mathtt{t}^3 + m\mathtt{t} - n \quad \& \quad g(\mathtt{t}) := n\mathtt{t}^3 - 2m^2\mathtt{t}^2 - 5mn\mathtt{t} - n^2.$$

(1) Demostrar que f y g comparten alguna raíz en $\mathbb{C}$ si y sólo si f posee alguna raíz múltiple en $\mathbb{C}$.

(2) Calcular, suponiendo que f tiene alguna raíz múltiple, las raíces complejas de f y de g.

Número VII.17 (1) Encontrar un polinomio $p \in \mathbb{Z}[\mathtt{u}, \mathtt{v}, \mathtt{w}]$ de modo que el polinomio

$$f(\mathtt{t}) := \mathtt{t}^3 - u\mathtt{t}^2 + v\mathtt{t} - w$$

tenga dos raíces cuya suma sea también raíz de f si y sólo si $p(u, v, w) = 0$

(2) Encontrar las raíces del polinomio $f(\mathtt{t}) := \mathtt{t}^3 - 6\mathtt{t}^2 + 10\mathtt{t} - 3$.

Número VII.18 Consideremos la aplicación

$$\varphi : \mathbb{C}^3 \to \mathbb{C}^3,\ (x, y, z) \mapsto (x + y + z, xy + xz + yz, xyz),$$

y el conjunto $M := \{(x, y, z) \in \mathbb{C}^3 : f(x, y, z) = 0\}$, donde f es el polinomio

$$f(\mathtt{x}, \mathtt{y}, \mathtt{z}) := \mathtt{x}^2(\mathtt{y} - \mathtt{z}) + \mathtt{x}(\mathtt{z}^2 - \mathtt{y}^2) + \mathtt{yz}(\mathtt{y} - \mathtt{z}).$$

(1) Probar que φ es sobreyectiva y calcular la fibra del punto $p := (1,1,1)$. ¿Qué grado tiene la aplicación φ, esto es, cuántos elementos tiene la fibra que más elementos tiene? Encontrar un punto $q \in \mathbb{C}^3$ cuya fibra conste de menos puntos que el grado de φ.

(2) Factorizar f en producto de polinomios irreducibles en $\mathbb{C}[\mathtt{x},\mathtt{y},\mathtt{z}]$.

(3) Encontrar un polinomio $\Delta \in \mathbb{Z}[\mathtt{u},\mathtt{v},\mathtt{w}]$ tal que

$$\varphi(\mathbb{C}^3 \setminus M) = \{(u,v,w) \in \mathbb{C}^3 : \Delta(u,v,w) \neq 0\}.$$

¿Contiene $\varphi(\mathbb{C}^3 \setminus M)$ al punto $(0,-3,2)$?

Número VII.19 Sea $f(\mathtt{t}) = \sum_{j=0}^{n} c_j \mathtt{t}^j \in \mathbb{Z}[\mathtt{t}]$ un polinomio de grado n y denotamos $\alpha_1,\ldots,\alpha_n \in \mathbb{C}$ sus raíces, no necesariamente distintas. Probar que si $\mathtt{s}(\mathtt{x}) \in \mathbb{Z}[\mathtt{x}_1,\ldots,\mathtt{x}_n]$ es un polinomio simétrico de grado d, entonces $c_n^d \mathtt{s}(\alpha_1,\ldots,\alpha_n) \in \mathbb{Z}$.

Número VII.20 Sean $f,g \in \mathbb{C}[\mathtt{t}]$ dos polinomios no constantes, $\mathfrak{a}$ el ideal de $\mathbb{C}[\mathtt{t}]$ generado por f y el cociente $V := \mathbb{C}[\mathtt{t}]/\mathfrak{a}$.

(1) Comprobar que V tiene estructura de espacio vectorial sobre el cuerpo $\mathbb{C}$ con las operaciones definidas mediante: dados $h_1,h_2 \in \mathbb{C}[\mathtt{t}]$ y $\lambda \in \mathbb{C}$,

$$(h_1+\mathfrak{a})+(h_2+\mathfrak{a}) := (h_1+h_2)+\mathfrak{a} \quad \& \quad \lambda\cdot(h_1+\mathfrak{a}) := \lambda h_1 + \mathfrak{a}.$$

Calcular la dimensión de V.

(2) Supongamos que el discriminante $\Delta(f)$ de f es no nulo. Demostrar que entonces la aplicación definida por $g_* : V \to V$, $h+\mathfrak{a} \mapsto gh+\mathfrak{a}$ es un endomorfismo de V y expresar sus autovalores en función de lo que vale g en las raíces de f.

(3) Probar que g_* es isomorfismo de $\mathbb{C}$-espacios vectoriales si y sólo si $\mathrm{Res}(f,g) \neq 0$.

(4) Demostrar que g_* es diagonalizable y expresar la traza de g_* en función de los valores que toma g en las raíces de f.

(5) Calcular la suma de los cubos de las raíces del polinomio $f(\mathtt{t}) := \mathtt{t}^5 - 2\mathtt{t}^2 - 2$.

Número VII.21 Sean K un cuerpo, $n > 0$ un entero y denotemos $K[\mathtt{x}] := K[\mathtt{x}_1,\ldots,\mathtt{x}_n]$.

(1) Demostrar que si $\mathfrak{a}$ y $\mathfrak{b}$ son ideales de $K[\mathtt{x}]$ tales que $\mathfrak{a} \subset \mathfrak{b}$ entonces $\mathcal{Z}(\mathfrak{b}) \subset \mathcal{Z}(\mathfrak{a})$.

(2) Sean M y N subconjuntos de K^n tales que $M \subset N$. Probar que $\mathcal{J}(N) \subset \mathcal{J}(M)$.

(3) Demostrar que K^n, cada punto de K^n y el conjunto vacío son subconjuntos algebraicos de K^n.

(4) Demostrar que la unión finita de subconjuntos algebraicos de K^n y la intersección arbitraria de subconjuntos algebraicos de K^n son subconjuntos algebraicos de K^n.

(5) Probar que $X \subset K^n$ es un subconjunto algebraico de K^n si y sólo si $X = \mathcal{Z}(\mathcal{J}(X))$.

(6) Un subconjunto algebraico X de K^n se dice *reducible* si existen dos subconjuntos algebraicos $Y \subsetneq X$ y $Z \subsetneq X$ de K^n tales que $X = Y \cup Z$. Si X no es reducible se denomina *irreducible*. Demostrar que todo subconjunto algebraico de K^n es unión finita de subconjuntos algebraicos irreducibles de K^n.

(7) Sean X un subconjunto algebraico de K^n y

$$\mathcal{A} := \{X_i : 1 \leq i \leq r\} \quad \& \quad \mathcal{B} := \{Y_i : 1 \leq i \leq s\}$$

dos familias de subconjuntos algebraicos irreducibles de K^n de modo que entre los miembros de cada una de ellas no hay relaciones de inclusión y tales que

$$\bigcup_{i=1}^{r} X_i = X = \bigcup_{i=1}^{s} Y_i.$$

Probar que $r = s$ y existe una biyección $\sigma : \{1, \ldots, r\} \to \{1, \ldots, r\}$ tal que $Y_i = X_{\sigma(i)}$ para $1 \leq i \leq r$. Se dice que $\{X_i : 1 \leq i \leq r\}$ son las *componentes irreducibles* de X.

Número VII.22 Sean K un cuerpo finito y $n > 0$ un entero. ¿Cuáles son los subconjuntos algebraicos de K^n? ¿Cuáles son los irreducibles no vacíos?

Número VII.23 Sean K un cuerpo y X un subconjunto algebraico de K^n. Probar que X es irreducible si y sólo si $\mathcal{J}(X)$ es un ideal primo del anillo de polinomios $K[\mathtt{x}] := K[\mathtt{x}_1, \ldots, \mathtt{x}_n]$.

Número VII.24 Sean K un cuerpo infinito, la aplicación $\varphi : K^2 \to K^3$, $(u, v) \mapsto (uv, v, u^2)$ y el conjunto $M := \varphi(K^2)$.

(1) Demostrar que el ideal $\mathcal{J}(M)$ es principal y encontrar un generador suyo.

(2) Estudiar si M es un subconjunto algebraico de K^3 para $K = \mathbb{C}$ y para $K = \mathbb{R}$.

Número VII.25 Sea K un cuerpo. Demostrar que las siguientes afirmaciones son equivalentes.

(1) El cuerpo K es algebraicamente cerrado.

(2) Para cada entero positivo n y cada polinomio irreducible $f \in K[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ el subconjunto algebraico $\mathcal{Z}(f)$ de K^n es irreducible.

(3) Existe un entero positivo $n > 1$ tal que el subconjunto algebraico $\mathcal{Z}(f)$ de K^n es irreducible para cada polinomio irreducible $f \in K[\mathtt{x}_1, \ldots, \mathtt{x}_n]$.

Número VII.26 Demostrar que el polinomio $f := \mathtt{z}^2 + \mathtt{x}^2\mathtt{y}^4 + \mathtt{x}^4\mathtt{y}^2 - 3\mathtt{x}^2\mathtt{y}^2 + 1$ es irreducible en $\mathbb{R}[\mathtt{x}, \mathtt{y}, \mathtt{z}]$. ¿Es $\mathcal{Z}(f)$ un subconjunto algebraico irreducible de $\mathbb{R}^3$?