Universidad de Valladolid

Facultad de Ciencias

Trabajo Fin de Grado

Grado en Matemáticas

Resultantes y teoría de la eliminación

Autor: Sergio Matilla Mayo

Tutor/es: Philippe Thierry Gimenez

Índice general

Introducción

En sus orígenes el álgebra era el arte de resolver ecuaciones. El estudio de sistemas de ecuaciones polinomiales ha pasado de ser una mera manipulación de fórmulas a convertirse en una herramienta crucial para estudiar ciertas estructuras más abstractas. La resolución de estos sistemas no es para nada una tarea trivial, e incluso con el auge de la computación en el último siglo hay ocasiones en las que somos incapaces de encontrar las soluciones exactas, teniendo que recurrir a técnicas de aproximación. En este trabajo se presentará la teoría de la eliminación como una herramienta para resolver dichos sistemas polinomiales. Es una herramienta que ya se empezó a usar en el siglo XVII cuando Newton planteó el problema de, dadas dos curvas, encontrar sus puntos de intersección. Su solución fue eliminar una de las incógnitas de una de las ecuaciones y el grado de la ecuación resultante sería el producto de los grados de las anteriores. Esto nos recuerda al conocido Teorema de Bézout, planteado en el siglo XVIII. Ya en el siglo XIX, primero Poisson, en 1802, y más tarde Netto y Le Vavasseur escribieron articulos hablando ya explícitamente de la teoría de la eliminación. Fue en este periodo cuando la matriz de Sylvester apareció por primera vez, se hablaba de su determinante pero fue Cayley quien le dió mas tarde el nombre de resultante. En la última parte del siglo XIX se publicaron muchos artículos sobre resultantes, con contribucciones tan relevantes como las de Brill (1880), Kronecker (1882) y Mertens (1886). Esto continuó en la primera parte del siglo XX con Macaulay, primero en un artículo (1902) y luego en el clásico libro [9]. La mayoría de los artículos estaban focalizados principalmente en polinomios homogéneos y fue Kronecker quién les dió un papel crucial en la teoría de la eliminación. En el siglo XX, más concretamente en los años 60, con la aparición de las bases de Gröbner, las resultantes dejaron de tener tanta importancia en la teoría de la eliminación. A finales del siglo XX, Jouanolou escribió varios artículos sobre resultantes, no solo creando una nueva teoría sobre estas, también relacionándolas íntimamente con el álgebra conmutativa. Ya en el siglo XXI han ido apareciendo nuevos tipos de resultantes como por ejemplo *Reduced resultants*, *Sparse resultants* o *Parametric resultants*. En cuanto a la teoría

de eliminación, en este siglo está jugando un papel muy importante en problemas de implicitación, por ejemplo los métodos que usan *moving curves*, e incluso tiene su parte de importancia en el álgebra tropical.
En este trabajo se dará una introducción a los conceptos básicos de la teoría de la eliminación y el uso de las resultantes.

1. En el primer capítulo se da una breve introducción a los órdenes monomiales y bases de Gröbner necesaria para luego poder abordar los teoremas de eliminación y extensión. También se da una relación entre el álgebra conmutativa y la geometría algebraica que será de utilidad para poder aplicar los conceptos de la eliminación en problemas de geometría.

2. En el segundo capítulo se presentan las resultantes en una variable como una herramienta para determinar cuando dos polinomios tienen un factor en común. Para ello se introduce la matriz de Sylvester, definiendo la resultante como su determinante, y se dan ciertas propiedades clásicas de la resultante en una variable.

3. En el tercer capítulo se generaliza el concepto de resultante para n polinomios homogéneos en n variables. Se dan una serie de propiedades, que serán en su mayoría la generalización de las vistas en el capítulo anterior, y se muestra una forma de poder calcular dichas resultantes usando determinantes. La resultante de polinomios homogéneos tendrá un papel fundamental en la implicitación de superficies, como se verá en el capítulo 5.

4. En el cuarto capítulo se dan las pruebas de los teoremas de eliminación y extensión usando bases de Gröbner. También se da una prueba alternativa del teorema de extensión usando las resultates vistas en los capítulos anteriores.

5. En el quinto capítulo se ven ciertas aplicaciones de la teoría expuesta en los capítulos anteriores. Se da una forma de resolver sistemas de ecuaciones polinomiales usando bases de Gröbner y los teoremas de eliminación y extensión, y otras dos alternativas usando resultantes. Las dos últimas tienen la ventaja de que son mejores computacionalmente hablando ya que no requieren de cálculos de bases de Gröbner, una tarea muy costosa. También se expone como se puede aplicar esta teoría en geometría, resolviendo problemas de implicitación, de estudio de puntos singulares y de cálculo de envolventes de curvas.

Capítulo 1

Preliminares

1.1. Bases de Gröbner

En este apartado vamos a dar la definición y una serie de propiedades sobre las bases de Gröbner necesarias para poder demostrar los teoremas de eliminación y extensión. Para una información más detallada se puede consultar [2, Ch.2].
Antes de introducir las bases de Gröbner hay que hablar primero sobre órdenes monomiales los cuales nos van a permitir ordenar los monomios del anillo $K[x_1, \ldots, x_n]$, siendo K un cuerpo. Además, como nuestro objetivo es estudiar la teoría de eliminación también vamos a introducir los órdenes de eliminación, que serán esenciales para poder estudiar y aplicar el teorema de eliminación en el capítulo 4.

Notación 1.1.1. Usaremos la notación $\underline{x}^\alpha$ para referirnos a monomios en $K[x_1, \ldots, x_n]$, esto es $\underline{x}^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$, donde $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$.

Definición 1.1.2. Una relación de orden sobre el conjunto de los monomios de $K[x_1, \ldots, x_n]$ se llama un orden monomial si cumple las siguientes propiedades:

1. Es un orden total, es decir, dados dos monomios $\underline{x}^\alpha, \underline{x}^\beta \in K[x_1, \ldots, x_n]$ distintos, se tiene que $\underline{x}^\alpha > \underline{x}^\beta$ ó $\underline{x}^\beta > \underline{x}^\alpha$.

2. El orden es compatible con el producto de monomios, es decir, si $\underline{x}^\alpha > \underline{x}^\beta$ y tomamos otro monomio $\underline{x}^\gamma \in K[x_1, \ldots, x_n]$, entonces $\underline{x}^\gamma \underline{x}^\alpha > \underline{x}^\gamma \underline{x}^\beta$.

3. Es un buen orden, es decir, que todo conjunto no vacío de monomios admite un mínimo.

Notación 1.1.3. Dado $f \in K[x_1, \ldots, x_n]$ y fijado un orden monomial, denotaremos por $\text{in}(f)$ al mayor monomio de f respecto del orden monomial fijado.

Esto se refiere al monomio mayor sin constante. Para hablar del término mayor de f con constante usaremos $\mathrm{lt}(f)$ y a dicha constante la denotaremos por $\mathrm{lc}(f)$, es decir, $\mathrm{lt}(f) = \mathrm{lc}(f) \cdot \mathrm{in}(f)$.

Definición 1.1.4. Consideramos un anillo de polinomios con coeficientes en un cuerpo K, separamos las variables en dos bloques y para ello escribimos $K[x_1, \ldots, x_t, y_1, \ldots, y_m]$. Supongamos que tenemos un orden monomial fijado sobre $K[x_1, \ldots, x_t]$ que denotaremos por $>_x$, y otro sobre $K[y_1, \ldots, y_m]$ que denotaremos por $>_y$. Cada monomio $f \in K[x_1, \ldots, x_t, y_1, \ldots, y_m]$ lo podemos escribir como $f = f_x f_y$ donde $f_x \in K[x_1, \ldots, x_t]$, $f_y \in K[y_1, \ldots, y_m]$. Entonces definimos el orden de eliminación sobre $K[x_1, \ldots, x_t, y_1, \ldots, y_m]$ asociado a $>_x$ y $>_y$ como:

$$f_x f_y > g_x g_y \Longleftrightarrow \begin{cases} f_x >_x g_x. \\ \text{o} \\ f_x = g_x \text{ y } f_y >_y g_y. \end{cases}$$

En este caso se tiene que $x_i > y_j$, para todo $i = 1, \ldots, t$, $j = 1, \ldots, m$, debido a que primero se evalúa el orden en las variables x_i y solo en el caso de que sea igual, se evalúa el orden en las variables y_j.

Ejemplo 1.1.5. Definimos el orden lexicográfico como: dados dos monomios $\underline{x}^{\alpha}$, $\underline{x}^{\beta}$, donde α y β son multi-índices,

$\underline{x}^{\alpha} > \underline{x}^{\beta} \Longleftrightarrow$ el primer elemento no nulo por la izquierda en α-β es positivo.

Depende del orden de las variables, previamente hay que fijar el orden de las mismas, es decir, el orden lexicográfico con $x_1 > \ldots > x_n$ es diferente al orden lexicográfico con $x_n > \ldots > x_1$.
El lexicográfico es un orden monomial que además es de eliminación. Computacionalmente es muy malo, pero como veremos en la sección 5.1 a veces es muy útil.

Introducidos los órdenes monomiales ya podemos hablar sobre bases de Gröbner. El siguiente resultado demostrado en la asignatura de Álgebra Conmutativa y Computacional será muy útil, como se verá en la definiciones posteriores, ya que nos permitirá asegurar que todo ideal tiene base de Gröbner.

Teorema 1.1.6 (Teorema de la base de Hilbert)**.** *Todo ideal $I \subseteq K[x_1, \ldots, x_n]$ tiene un sistema de generadores finito. Esto es, $I = \langle g_1, \ldots, g_t \rangle$ para ciertos $g_1, \ldots, g_t \in I$.*

Definición 1.1.7. Sea K un cuerpo y consideramos el anillo $K[x_1, \ldots, x_n]$. Si $I \subseteq K[x_1, \ldots, x_n]$ es un ideal, y fijado un orden monomial sobre el conjunto de los monomios de $K[x_1, \ldots, x_n]$, el ideal inicial de I respecto del orden monomial fijado, que denotaremos por $\mathrm{in}(I)$, es el ideal monomial engendrado por todos los $\mathrm{in}(f)$ con $f \in I$. Por el teorema de la base de Hilbert, $\mathrm{in}(I)$ es finitamente generado, es decir, existen $g_1, \ldots, g_t \in I$ tal que:

$$\mathrm{in}(I) = \langle \mathrm{in}(f), f \in I \rangle = \langle \mathrm{in}(g_1), \ldots, \mathrm{in}(g_t) \rangle.$$

Definición 1.1.8. Una base de Gröbner del ideal I respecto de un orden monomial fijado es un subconjunto finito de I, $G = \{g_1, \ldots, g_t\}$ tal que $\{\mathrm{in}(g_1), \ldots, \mathrm{in}(g_t)\}$ genera $\mathrm{in}(I)$.

El siguiente resultado, también demostrado en la asignatura de Álgebra Conmutativa y Computacional, se puede encontrar en [2, Ch.2,Sec.5,Coro.6].

Proposición 1.1.9. *Toda base de Gröbner de I es un sistema de generadores de I.*

1.2. Diccionario Álgebra-Geometría

En este apartado vamos a hacer una pequeña introducción sobre la relación entre ideales y variedades que nos será de utilidad en la teoría de la eliminación. Información más detallada se puede encontrar en [2, Ch.4].

Definición 1.2.1. Dado K un cuerpo y $V \subseteq K^n$ una variedad afín, definimos el ideal:

$$\mathrm{I}(V) = \{f \in K[x_1, \ldots, x_n] \ : f(a) = 0, \ \forall a \in V\}.$$

De forma recíproca, dado un ideal $I \subseteq K[x_1, \ldots, x_n]$ definimos:

$$\mathrm{V}(I) = \{a \in K^n \ : f(a) = 0, \ \forall f \in I\},$$

además, es claro que si $I = \langle f_1, \ldots, f_t \rangle$ se tiene que

$$\mathrm{V}(I) = \mathrm{V}(f_1, \ldots, f_t) = \{a \in K^n \ : f_i(a) = 0, \ \forall i \in \{1, \ldots, t\}\}.$$

Es claro que para todo ideal I de $K[x_1, \ldots, x_n]$, $\mathrm{V}(I)$ es una variedad afín y que dada una variedad afín $V \subseteq K^n$, $\mathrm{I}(V)$ es un ideal de $K[x_1, \ldots, x_n]$. Esto nos permite dar dos aplicaciones entre ideales y variedades:

$$\begin{array}{rcc} \textit{ideales} & \longrightarrow & \textit{variedades afines} \\ I & \longrightarrow & \mathrm{V}(I) \\ \mathrm{I}(V) & \longleftarrow & V \end{array}$$

Esta identificación es la que da el nombre de la sección, ya que nos permite movernos entre la geometría y el álgebra. Pero hay que tener cuidado ya que no son operaciones inversas la una de la otra.
Vamos a exponer el teorema de los ceros de Hilbert primero en su versión débil, aunque ambas son equivalentes. Este teorema ha tenido tanto impacto que incluso en la actualidad se le sigue llamando por su nombre original en alemán.

Teorema 1.2.2 (The weak Nullstellensatz)**.** *Sea K es un cuerpo algebraicamente cerrado y dado $I \in K[x_1, \ldots, x_n]$ un ideal tal que $V(I) = \emptyset$. Entonces $I = K[x_1, \ldots, x_n]$.*

Teorema 1.2.3 (Hilbert's Nullstellensatz)**.** *Sea K un cuerpo algebraicamente cerrado y sea $I \subseteq K[x_1, \ldots, x_n]$ un ideal, dado $f \in K[x_1, \ldots, x_n]$ entonces:*

$$f \in \mathrm{I}(\mathrm{V}(I)) \text{ si y solo si } f^m \in I,$$

para algún $m \geq 1$.

Las demostraciones de estos dos teoremas no tienen que ver con el motivo de este trabajo, se pueden encontrar en [2, Ch.4,Sec.1].

Capítulo 2

La resultante en una variable

En este capítulo vamos a definir y dar algunas propiedades sobre la resultante en una variable. También nos servirá de introducción para ver en el capítulo 3 las resultantes multivariadas, que son una generalización de lo que veremos en este capítulo. Aunque en apariencia no tenga mucha relación con la teoría de eliminación, veremos que las resultantes son una herramienta muy potente para resolver sistemas de ecuaciones. A mayores, nos permitirá dar una demostración alternativa del teorema de extensión.

2.1. Definición

En este apartado vamos a introducir la resultante en una variable como una herramienta para determinar cuando dos polinomios tienen un factor común. Es decir, dado K un cuerpo y dados dos polinomios $f, g \in K[x]$ de grado positivo y no nulos, los esribimos como:

$$f(x) = \sum_{i=0}^{l} c_i x^i, \;\; g(x) = \sum_{i=0}^{m} d_i x^i, \tag{2.1}$$

donde $c_i, d_i \in K$ para todo i, $c_l, d_m \neq 0$. El siguiente lema va a dar una condición equivalente a que f, g tengan un factor común, la cual nos va a permitir linealizar el problema de determinar cuando dos polinomios tienen un factor común.

Lema 2.1.1. *Sean $f, g \in K[x]$ polinomios como en (2.1). Entonces f y g tienen un factor común en $K[x]$ si y solo si existen polinomios $A, B \in K[x]$ tales que:*

1. *$A \neq 0$ ó $B \neq 0$.*

2. $\deg(A) \leq m-1$ *y* $\deg(B) \leq l-1$.

3. $Af + Bg = 0$.

Demostración. $\Leftarrow$) Razonando por reducción al absurdo, si f y g no tienen factores comunes, entonces $\mathrm{mcd}(f,g) = 1$. Por tanto, existen polinomios $P, Q \in K[x]$ tales que $Pf + Qg = 1$. De la propiedad (1), se puede suponer que $B \neq 0$, entonces multiplicando por B y usando la propiedad (3), tenemos que:

$$B = B(Pf + Qg) = PBf + QBg = PBf - QAf = (PB - QA)f.$$

Como B y f no son nulos, implica que $PB - QA \neq 0$, y por tanto, como $\deg(f) = l$, se tiene que $\deg(B) \geq l$, lo que contradice la propiedad (2).

$\Rightarrow$) Si f y g tienen un factor común $h \in K[x]$, existen polinomios $f_1, g_1 \in K[x]$ con $\deg(f_1) \leq l-1$ y $\deg(g_1) \leq m-1$ tales que $f = hf_1$ y $g = hg_1$. Además, como los grados de f y g son estrictamente mayores que 0, tanto f_1 como g_1 son no nulos. Entonces,

$$g_1 f + (-f_1)g = g_1 h f_1 - f_1 h g_1 = 0.$$

Tomando $A = g_1$, $B = -f_1$, se tiene lo que se pide. □

Por tanto, el problema de determinar cuando dos polinomios f y g tienen un factor común se reduce a determinar cuándo existen polinomios A y B con las propiedades del lema anterior. Para ver esto, si denotamos por S_l al espacio vectorial de los polinomios de grado a lo sumo l, construimos la siguiente aplicación lineal entre K-espacios vectoriales de dimensión $(l+m)$:

$$\begin{array}{rccc} \phi\colon & S_{m-1} \times S_{l-1} & \longrightarrow & S_{l+m-1} \\ & (A,B) & \longmapsto & Af + Bg \end{array} \tag{2.2}$$

Proposición 2.1.2. *La aplicación ϕ es un isomorfismo si y solo si f y g no tienen un factor común.*

Demostración. $\Rightarrow$) Razonando por contrarecíproco, suponemos que f y g tienen un factor común. Por el lema anterior, existen $A \in S_{m-1}, B \in S_{l-1}$ tales que $(A,B) \neq (0,0)$ y $\phi((A,B)) = 0$. Por tanto ϕ no es inyectiva, luego tampoco es un isomorfismo.

$\Leftarrow$) Para ver la inyectividad, razonando por reducción al absurdo, dados $(h_1, h_2) \in S_{m-1} \times S_{l-1}$, $(h_1, h_2) \neq (0,0)$, si

$$\phi((h_1, h_2)) = h_1 f + h_2 g = 0.$$

Por el lema anterior, f y g tendrían un factor común, lo que es absurdo. La sobreyectividad se deduce de que es una aplicación lineal inyectiva entre espacios de la misma dimensión. □

Fijamos las siguientes bases monomiales en los espacios vectoriales de los polinomios:

$$B(S_{m+l-1}) = \{1, x, \ldots, x^{m+l-1}\},$$
$$B(S_{m-1} \times S_{l-1}) = \{(1,0), (x,0), \ldots, (x^{m-1},0), (0,1), \ldots, (0,x^{l-1})\}.$$

Definimos la resultante de dos polinomios de la siguiente manera.

Definición 2.1.3. Dados dos polinomios $f, g \in K[x]$, como en (2.1), la matriz de la apliación ϕ en las bases monomiales anteriores se llama la matriz de Sylvester y la denotaremos por $\mathrm{Syl}(f,g)$. Es decir, es la siguiente matriz de tamaño $(l+m) \times (l+m)$:

$$\mathrm{Syl}(f,g) = \begin{pmatrix} c_0 & & & & d_0 & & & \\ c_1 & c_0 & & & d_1 & d_0 & & \\ c_2 & c_1 & \ddots & & \vdots & d_1 & \ddots & \\ \vdots & c_2 & \ddots & c_0 & & \vdots & \ddots & d_0 \\ & \vdots & & c_1 & d_m & & & d_1 \\ c_l & & & \vdots & & d_m & & \vdots \\ & c_l & & & & & \ddots & \\ & & & c_l & & & & d_m \end{pmatrix}, \tag{2.3}$$

donde los espacios en blanco son ceros.

Definición 2.1.4. Definimos la resultante de f y g, denotada por $\mathrm{Res}(f,g)$ como el determinante de la matriz de Sylvester. Esto es:

$$\mathrm{Res}(f,g) = \det(\mathrm{Syl}(f,g)).$$

Nota 2.1.5. Hemos definido la resultante para polinomios de grado mayor que 0. También se puede extender esta definición si el grado de alguno de los dos polinomios es 0 de la siguiente manera:

$$\begin{aligned} &\mathrm{Res}(c_0, g) = c_0^m, \text{ si } c_0 \in K \setminus \{0\} \text{ y } \deg(g) = m > 0. \\ &\mathrm{Res}(f, d_0) = d_0^l, \text{ si } d_0 \in K \setminus \{0\} \text{ y } \deg(f) = l > 0. \\ &\mathrm{Res}(c_0, d_0) = 1 \text{ si, } c_0, d_0 \in K \setminus \{0\}. \end{aligned} \tag{2.4}$$

Esto tiene sentido con la definición que hemos dado ya que $\mathrm{Syl}(c_0, g)$ es una matriz diagonal de tamaño $m \times m$ con c_0 en la diagonal. Ocurre algo similiar para $\mathrm{Syl}(f, d_0)$.

Notación 2.1.6. Escribiremos $\mathrm{Syl}(f, g, x)$ y $\mathrm{Res}(f, g, x)$ cuando queramos recalcar la variable en la que estamos trabajando. Esto servirá más adelante cuando trabajemos con polinomios en varias variables.

Ejemplo 2.1.7. Sean $f, g \in K[x]$ polinomios de grado dos genéricos:

$$f = c_0 + c_1 x + c_2 x^2,\ g = d_0 + d_1 x + d_2 x^2,$$

entonces la matriz de Sylvester de f y g es:

$$\mathrm{Syl}(f, g) = \begin{pmatrix} c_0 & 0 & d_0 & 0 \\ c_1 & c_0 & d_1 & d_0 \\ c_2 & c_1 & d_2 & d_1 \\ 0 & c_2 & 0 & d_2 \end{pmatrix},$$

y la resultante de f y g es:

$$\mathrm{Res}(f, g) = d_2^2 c_0^2 - 2 d_2 c_0 c_2 d_0 + c_2^2 d_0^2 - d_1 d_2 c_1 c_0 - d_1 c_1 c_2 d_0 + c_2 d_1^2 c_0 + d_0 d_2 c_1^2.$$

2.2. Propiedades

En este apartado vamos a dar una serie de propiedades sobre la resultante. Sean f, g polinomios como en (2.1).

Proposición 2.2.1. *Las resultantes* $\mathrm{Res}(f, g)$ *y* $\mathrm{Res}(g, f)$ *coinciden salvo el signo. Además, se tiene que:*

$$\mathrm{Res}(f, g) = (-1)^{lm} \mathrm{Res}(g, f).$$

Demostración. Se deduce de la definición de $\mathrm{Res}(f, g)$ como el determinante de la matriz de Sylvester y de que al intercambiar dos columnas el determinante cambia de signo. Más concretamente en 2.3, empezando con $\mathrm{Syl}(f, g)$, si $l = m$ intercambiando la columna i con la columna $(l+i)$ para $i = 1, \ldots, l$, con l intercambios ya tendríamos $\mathrm{Syl}(g, f)$, pero como $(-1)^l = (-1)^{l^2}$, tendríamos el resultado. Ahora, si $l \neq m$, suponemos $l > m$.
Para llevar la columna $(l+i)$-ésima a la posición i-ésima, tenemos que hacer l intercambios, y este proceso hay que hacerlo para $i = 1, \ldots, m$, por tanto tenemos que hacer lm intercambios de columnas para llegar a $\mathrm{Syl}(g, f)$. Si $l < m$ se hace de forma análoga. □

Proposición 2.2.2. $\mathrm{Res}(f, g) \in \mathbb{Z}[c_0, \ldots, c_l, d_0, \ldots, d_m]$. *De manera más precisa tenemos que* $\mathrm{Res}(f, g)$ *es un polinomio entero homogéneo de grado* $l + m$ *en los coeficientes de* f *y* g.

Demostración. Si f o g tienen grado cero, de las expresiones (2.4) es claro el resultado. Si ahora suponemos que ambos tienen grado positivo, la primera afirmación se deduce de la definición de $\mathrm{Res}(f,g)$ como el determinante de la matriz de Sylvester es decir, escribiendo $\mathrm{Syl}(f,g) = (a_{ij})_{1\leq i,j\leq l+m}$, tenemos que:

$$\mathrm{Res}(f,g) = \sum_{\sigma\in S_{l+m}} sgn(\sigma) a_{1,\sigma(1)} \cdot a_{2,\sigma(2)} \cdots a_{l+m,\sigma(l+m)},$$

donde S_{l+m} son las permutaciones de $\{1,\ldots,l+m\}$ y $sgn(\sigma)$ es 1 (respectivamente -1) si σ intercambia un número par (respectivamente impar) de elementos de $\{1,\ldots,l+m\}$. Además, cada a_i no nulo es un coeficiente de f o g. Además, $sgn(\sigma)$ hace el papel de los coeficientes, es decir siempre son ± 1. Luego es claro que $\mathrm{Res}(f,g) \in \mathbb{Z}[c_o,\ldots,c_l,d_o,\ldots,d_m]$. También de esta expresión se deduce que es un polinomio homogéneo ya que cada monomio que lo forma está formado por el producto de $l+m$ elementos de $\mathrm{Syl}(f,g)$. □

Los siguientes resultados son los que nos permitirán usar la resultante como una herramienta para determinar cuando dos polinomios tienen un factor común en $K[x]$, o equivalentemente, una raíz común en un cuerpo algebraicamente cerrado que contenga a K.

Proposición 2.2.3. *Se tiene que* $\mathrm{Res}(f,g) = 0$ *si y solo si* f *y* g *tienen un factor común en* $K[x]$*. Además, si* $\mathbb{K}$ *es un cuerpo algebraicamente cerrado que contiene a* K *y* $f,g \in K[x]$*, entonces* $\mathrm{Res}(f,g) = 0$ *si y solo si* f *y* g *tienen una raíz común en* $\mathbb{K}$*.*

Demostración. La primera afirmación se deduce de la proposición 2.1.2, y de un conocido resultado de álgebra lineal que dice que una aplicación lineal es un isomorfismo si y solo si el determinante de la matriz de la aplicación es distinto de 0.
La segunda afirmación se deduce de que como $\mathbb{K}$ es un cuerpo algebraicamente cerrado y $K \subseteq \mathbb{K}$, es equivalente la existencia de un factor común a la de una raíz común en $\mathbb{K}$. □

Esta propiedad es la que nos permitirá relacionar las resultantes con la teoría de eliminación ya que cuando tengamos un ideal I y queramos calcular $\mathrm{V}(I)$, esta propiedad nos permitirá eliminar ciertas variables e ir calculándolo poco a poco. Esto se verá con mas detalle en capítulos posteriores.
Vamos a dar un ejemplo en el cual se vea la diferencia entre factor y raíz común, dependiendo si estamos trabajando sobre un cuerpo algebraicamente cerrado o no.

Ejemplo 2.2.4. Sean $f, g \in \mathbb{R}[x]$ los siguientes polinomios de grado 3 y 2 respectivamente:

$$f(x) = x^3 + 3x^2 + x + 3,\ g(x) = x^2 + 1.$$

Entonces, la matriz de Sylvester asociada a f y g es:

$$\mathrm{Syl}(f,g) = \begin{pmatrix} 3 & 0 & 1 & 0 & 0 \\ 1 & 3 & 0 & 1 & 0 \\ 3 & 1 & 1 & 0 & 1 \\ 1 & 3 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix},$$

y $\mathrm{Res}(f,g) = \det(\mathrm{Syl}(f,g)) = 0$. Y efectivamente, f y g tienen un factor común, $h(x) = x^2 + 1 \in \mathbb{R}[x]$, pero no tienen raíces comunes en $\mathbb{R}$, pero en $\mathbb{C}$, que es un cuerpo algebraicamente cerrado (y que contiene a $\mathbb{R}$), tienen las raíces comunes $\pm i$.

En esta memoria se ha dado una definición constructiva de la resultante de dos polinomios en una variable, también es usual dar la definición mediante el siguiente teorema.

Teorema 2.2.5. *Existe un único polinomio (salvo signo) irreducible llamado la resultante,* $\mathrm{Res} \in \mathbb{Z}[c_0, \ldots, c_l, d_0, \ldots, d_m]$*, que verifica que* $\mathrm{Res}(f,g) = 0$ *si y solo si* f *y* g *tienen un factor común en* $K[x]$*.*

Nota 2.2.6. Se recomienda consultar la primera parte del capítulo 3 para entender mejor lo que significa que $\mathrm{Res} \in \mathbb{Z}[c_0, \ldots, c_l, d_0, \ldots, d_m]$.

La existencia está vista en resultados anteriores ya que hemos construido un polinomio que cumple dichas propiedades. La irreduciblidad del determinante de la matriz de Sylvester se puede encontrar en [9, Ch.1,Sec.2]. El motivo de dar la definición de esta forma es que la resultante multivariada se definirá de esta manera en el siguiente capítulo, quedando claro que la resultante multivariada generaliza a esta.

Proposición 2.2.7. *Existen polinomios* $A, B \in K[x]$*, tales que:*

$$Af + Bg = \mathrm{Res}(f,g).$$

Además, si f *y* g *tienen grado positivo, es decir* $l > 0$ *y* $m > 0$*, los coeficientes de* A *y* B *son polinomios enteros en los coeficientes de* f *y* g*, con grados* $m-1$ *y* $l-1$ *respectivamente. Es decir, se puede escribir* $A = \sum_{i=0}^{m-1} a_i x^i$*, donde* $a_i \in \mathbb{Z}[c_0, \ldots, c_l, d_0, \ldots, d_m], \forall i \in \{1, \ldots, m-1\}$*, y de forma similar para* B*.*

Demostración. Si $\text{Res}(f,g) = 0$, tomando $A = B = 0$ el resultado es cierto. Ahora, si $f = c_0 \in K$, $g = d_0 \in K$, se tiene que f, g no tienen ningún factor común en $K[x]$, luego existen polinomios A, B tales que

$$Af + Bg = 1 = \text{Res}(c_0, d_0).$$

Si $f = c_0 \in K$ y $\deg(g) = m > 0$, por (2.4) tenemos que:

$$\text{Res}(f,g) = c_0^m = c_0 \cdot c_0^{m-1} = c_0^{m-1} \cdot f + 0 \cdot g,$$

y el caso en el que $g = d_0 \in K$ y $\deg(f) = l > 0$ se hace de manera similar, por tanto el resultado es cierto en estos casos. Supongamos ahora que f y g tienen grado positivo y $\text{Res}(f,g) \neq 0$. Ahora, si en $\text{Syl}(f,g)$ sumamos a la primera fila, la segunda multiplicada por x, la tercera multiplicada por x^2, etc, llegamos a una matriz con entradas en $K[x]$, $\text{Syl}'(f,g)$, en la que en la primera fila tenemos el vector

$$(f, xf, x^2f, \ldots, x^{m-1}f, g, xg, x^2g, \ldots, x^{l-1}g),$$

además, por las propiedades del determinante,

$$\text{Res}(f,g) = \det(\text{Syl}(f,g)) = \det(\text{Syl}'(f,g)).$$

Ahora, desarrollando el determinante por la primera fila de la matriz $\text{Syl}'(f,g)$, llegamos a una expresión de la forma:

$$\text{Res}(f,g) = \sum_{i=1}^{m} a_i x^{i-1} f + \sum_{j=1}^{l} b_j x^{j-1} g = (\sum_{i=1}^{m} a_i x^{i-1}) f + (\sum_{j=1}^{l} b_j x^{j-1}) g,$$

donde los a_i's, b_j's, son los determinantes de tamaño $(l+m-1) \times (l+m-1)$ que salen al desarrollar por la primera fila (los consideramos incluyendo el factor -1 cuando corresponda, que viene del desarollo del determinante). Por tanto $a_i, b_j \in \mathbb{Z}[c_o, \ldots, c_l, d_o, \ldots, d_m], \forall i \in \{1, \ldots, m\}$, $\forall j \in \{1, \ldots, l\}$. Tomando $A = \sum_{i=1}^{m} a_i x^{i-1}$ y $B = \sum_{j=1}^{l} b_j x^{j-1}$, se tiene lo que se pide. □

El siguiente resultado proporciona fórmulas para la resultante en función de las raíces de los polinomios.

Proposición 2.2.8 (Fórmula de Poisson)**.** *Dados $f, g \in K[x]$, con grados respectivos l y m, llamando $f_1, \ldots, f_l$ y $g_1, \ldots, g_m$ las raíces de f y g respectivamente (puede ocurrir que las raíces estén en un cuerpo $\mathbb{K}$ algebraicamente cerrado que contenga a K), se tiene que:*

$$\text{Res}(f,g) = c_l^m d_m^l \prod_{i=1}^{l} \prod_{j=1}^{m} (f_i - g_j) = c_l^m \prod_{i=1}^{l} g(f_i) = (-1)^{lm} d_m^l \prod_{j=1}^{m} f(g_j).$$

Demostración. Las dos últimas igualdades se deben a que podemos escribir f y g de la siguiente manera

$$f(x) = c_l \prod_{i=1}^{l}(x - f_i),$$
$$g(x) = d_m \prod_{j=1}^{m}(x - g_j).$$

Entonces para ver la primera igualdad, definimos el polinomio

$$R(c_0, \ldots, c_l, d_0, \ldots, d_m) = R(c, d) = c_l^m \prod_{i=1}^{l} g(f_i) = \prod_{i=1}^{l}(\sum_{j=0}^{m} d_j f_i^j).$$

De la segunda igualdad se deduce que R depende polinómicamente de los coeficientes de g. Gracias a la primera parte de la demostración se tiene que

$$R(c, d) = (-1)^{lm} d_m^l \prod_{j=1}^{m} f(g_j) = (-1)^{lm} d_m^l \prod_{j=1}^{m}(\sum_{i=0}^{l} c_i g_j^i),$$

de donde se deduce que también depende polinómicamente de los coeficientes de f, luego $R \in \mathbb{Z}[c_0, \ldots, c_l, d_0, \ldots, d_m]$. Además se tiene que $R(c, d) = 0$ si y solo si f y g tienen al menos una raíz común en $\mathbb{K}$. Como Res es un polinomio irreducible, existe $c \in \mathbb{K}$ tal que Res $= cR$. Si ahora especializamos $f = x^l$, $g = 1$, tenemos que $\mathrm{Res}(f, g) = 1$ y necesariamente $c = 1$. □

Corolario 2.2.9. *Sean $f_1, f_2, g \in K[x]$, entonces:*

$$\mathrm{Res}(f_1 f_2, g) = \mathrm{Res}(f_1, g) \cdot \mathrm{Res}(f_2, g),$$
$$\mathrm{Res}(g, f_1 f_2) = \mathrm{Res}(g, f_1) \cdot \mathrm{Res}(g, f_2).$$

Demostración. Llamando h_1, h_2 a los grados de f_1, f_2 respectivamente se tiene que

$$\mathrm{Res}(f_1, g) \cdot \mathrm{Res}(f_2, g) = \left((-1)^{h_1 m} d_m^{h_1} \prod_{j=1}^{m} f_1(g_j)\right)\left((-1)^{h_2 m} d_m^{h_2} \prod_{j=1}^{m} f_2(g_j)\right)$$
$$= (-1)^{(h_1+h_2)m} d_m^{h_1+h_2} \prod_{j=1}^{m} f_1(g_j) f_2(g_j) = \mathrm{Res}(f_1 f_2, g).$$

La segunda fórmula se obtiene de la primera aplicando la proposición 2.2.1. □

Vamos a dar otra fórmula para la resultante que nos será útil en los capítulos posteriores. Consideramos el anillo cociente $A_f = K[x]/\langle f\rangle$. Como todo polinomio de $K[x]$ tiene la misma clase en A_f que el resto de su división por f, podemos identificarlo con el conjunto de los polinomios de grado estrictamente menor que l. Definimos la aplicación multiplicación por g como

$$\begin{array}{rccc} m_g\colon & A_f & \longrightarrow & A_f \\ & [h] & \longmapsto & [g]\cdot[h] = [gh]\,. \end{array}$$

Podemos calcular $\mathrm{Res}(f,g)$ en términos de la aplicación m_g de la siguiente manera.

Proposición 2.2.10. *Si M_g es la matriz de la aplicación m_g respecto de alguna base de A_f, entonces* $\mathrm{Res}(f,g) = c_l^m \det(M_g)$.

Demostración. De la interpretación de A_f como los restos de la división por f, se tiene que es un K-espacio vectorial de dimensión l y además, la aplicación m_g es una aplicación lineal gracias a propiedades generales de anillos cociente. Por tanto, lo que vamos a probar es que si $f_1,\dots,f_r$ son las raíces de f con multiplicidades $a_1,\dots,a_r$, entonces $\det(M_g) = \prod_{i=1}^r g(f_i)^{a_i}$ y por la proposición 2.2.8 tendríamos lo que queremos. Definimos la aplicación

$$T\colon A_f \longrightarrow K[x]/\langle (x-f_1)^{a_1})\rangle \oplus \cdots \oplus K[x]/\langle (x-f_r)^{a_r})\rangle,$$

que a cada $[h]\in A_f$ lo envía a $([h]_1,\dots,[h]_r)$, donde $[h]_i$ es la clase de h en $K[x]/\langle (x-f_i)^{a_i})\rangle$. Está bien definida ya que para cualquier $h'\in[h]$ se tienen las siguientes igualdades

$$\begin{aligned} h &= qf + R, \\ h' &= q'f + R, \end{aligned}$$

donde q, q' son los cocientes de la división por f y R el resto. De aquí se deduce que $R = h - qf$ y por tanto

$$h' = f(q'-q) + h.$$

Ahora, como $(x-f_i)^{a_i}$ divide a f, se tiene que el resto de la división de h' por $(x-f_i)^{a_i}$ es el mismo que el resto de la división de h por $(x-f_i)^{a_i}$ y por tanto $[h']_i = [h]_i$ para todo i. Además, conserva la suma y el producto, ya que si tenemos $h, p\in K[x]$, al dividirlos por cada $(x-f_i)^{a_i}$ tenemos una expresión de la forma

$$\begin{aligned} h &= (x-f_i)^{a_i} q_i + R_i, \\ p &= (x-f_i)^{a_i} q_i' + R_i', \end{aligned}$$

donde q_i, q_i' son los cocientes y R_i, R_i' los restos. Con estas expresiones es claro que

$$T([h+p]) = (R_1 + R_1', \ldots, R_r + R_r') = T([h]) + T([p]),$$
$$T([hp]) = (R_1R_1', \ldots, R_rR_r') = T([h])T([p]).$$

Además tenemos que es una aplicación inyectiva ya que si tenemos $h \in K[x]$ no nulo tal que $T([h]) = (0, \ldots, 0)$, entonces para cada i se tiene que

$$h = (x - f_i)^{a_i} q_i,$$

es decir, necesariamente se tiene que

$$h = (x - f_1)^{a_1} \cdots (x - f_r)^{a_r} q = \frac{q}{c_l} f,$$

y por tanto $[h] = 0$. Además como las dimensiones son iguales se puede concluir que T es un isomorfismo de anillos. En cada $K[x]/\langle (x - f_i)^{a_i} \rangle$ consideramos la base dada por $\{1, (x - f_i), \ldots, (x - f_i)^{a_i - 1}\}$ y escribimos g como

$$g(x) = b_m(x - f_i)^m + \ldots + b_1(x - f_i) + b_0,$$

donde lo que se ha hecho es reemplazar x por $(x - f_i) + f_i$ y usar el bimomio de Newton para dejarlo en términos de $(x - f_i)$. Ahora si en esta expresión evaluamos $x = f_i$ se tiene que $g(f_i) = b_0$. Si consideramos la aplicación multiplicación por g definida y con llegada en cada $K[x]/\langle (x - f_i)^{a_i} \rangle$,

$$\begin{array}{rccc} m_g' \colon K[x]/\langle (x - f_i)^{a_i} \rangle & \longrightarrow & K[x]/\langle (x - f_i)^{a_i} \rangle \\ [h] & \longmapsto & [g] \cdot [h] = [gh]\,, \end{array}$$

tenemos que si $0 \leq z \leq a_i - 1$ entonces

$$m_g'((x - f_i)^z) = [g][(x - f_i)^z] = g(f_i)(x - f_i)^z,$$

por tanto la matriz de esa aplicación, que llamaremos M_g', es diagonal con $g(f_i)$ en la diagonal y por tanto $\det(M_g') = g(f_i)^{a_i}$. Ahora consideramos la aplicación multiplicación por g, a la que llamaremos m_g'' y su matriz asociada M_g'', con origen y llegada en $K[x]/\langle (x - f_1)^{a_1} \rangle \oplus \cdots \oplus K[x]/\langle (x - f_r)^{a_r} \rangle$, entonces $\det(M_g'') = \prod_{i=1}^r g(f_i)^{a_i}$. De aquí se concluye el resultado porque al componer tenemos que $m_g = T \circ m_g'' \circ T^{-1}$, y si llamamos B a la matriz de la aplicación T se tiene que

$$\det(M_g) = \det(B)\det(M_g'')\frac{1}{\det(B)} = \det(M_g'') = \prod_{i=1}^r g(f_i)^{a_i}.$$

□

Capítulo 3

Resultante multivariada

3.1. Definición

En este apartado vamos a generalizar el concepto de resultante visto en el capítulo 2. Solo vamos a abordar el caso en el tengamos $n+1$ polinomios homogéneos de grado positivo $F_0, \ldots, F_n \in \mathbb{K}[x_0, \ldots, x_n]$, donde $\mathbb{K}$ es un cuerpo algebraicamente cerrado. Como en el capítulo 2, lo que vamos a intentar es determinar cuando tienen una raíz común, es decir, resolver el sistema

$$F_0(x_0, \ldots, x_n) = \ldots = F_n(x_0, \ldots, x_n) = 0. \tag{3.1}$$

Como todos los F_i's tienen grado positivo, siempre va a existir la raíz común $x_0 = \ldots = x_n = 0$ a la que llamaremos solución trivial, pero lo que a nosotros realmente nos importa es determinar las raíces comunes en $\mathbb{K}^{n+1}\backslash\{(0, \ldots, 0)\}$. Antes de dar la definición vamos a introducir una pequeña notación. Si suponemos que F_i tiene grado $d_i \geq 1$ podemos escribir:

$$F_i = \sum_{|\alpha|=d_i} c_{i,\alpha} \underline{x}^{\alpha}. \tag{3.2}$$

Para cada par de índices i, α, con $|\alpha| = d_i$, introducimos una nueva variable $u_{i,\alpha}$. Entonces, dado un polinomio $P \in \mathbb{K}[u_{i,\alpha}]$, cuando escribimos $P(F_0, \ldots, F_n)$ nos referimos a evaluar cada variable $u_{i,\alpha}$ de P en el correspondiente coeficiente $c_{i,\alpha}$ de F_i. Tenemos que $P(F_0, \ldots, F_n) \in \mathbb{K}$ y es lo que llamamos un polinomio en los coeficientes de F_i. Aunque la notación sea más pesada es el mismo concepto que introducimos en la proposición 2.2.2 También diremos que un polinomio homogéneo $\mathbf{F}$ es universal si lo escribimos como

$$\mathbf{F} = \sum_{|\alpha|=d} u_{i,\alpha} \underline{x}^{\alpha},$$

y diremos que $\mathbf{F} \in \mathbb{Z}[u_{i,\alpha}][x_0, \ldots, x_n]$. Esto no es más que escribir los polinomios de forma genérica, es decir, si especializamos los coeficientes de $\mathbf{F}$ en los valores $c_{i,\alpha}$, obtenemos los polinomios F_i. También es usual, y es la notación que usaré en algunos ejemplos, cuando estemos trabajando con polinomios universales de un determinado grado usar variables diferentes para cada polinomio en vez de usar las variables $u_{i,\alpha}$, por ejemplo si tenemos un polinomio homogéneo $\mathbf{F}$ universal de grado 2, en vez de escribir

$$\mathbf{F} = u_{i,(2,0)}x^2 + u_{i,(1,1)}xy + u_{i,(0,2)}y^2,$$

para facilitar la notación escribiré

$$\mathbf{F} = a_0x^2 + a_1xy + a_2y^2.$$

Definimos la resultante multivariada mediante el siguiente teorema.

Teorema 3.1.1 (Definición)**.** *Fijados $d_0, \ldots, d_n$ números positivos, existe un único polinomio (salvo signo)* $\mathrm{Res} \in \mathbb{Z}[u_{i,\alpha}]$ *con las siguientes propiedades:*

1. *Si $F_0, \ldots, F_n \in \mathbb{K}[x_0 \ldots, x_n]$ son polinomios homogéneos de grados $d_0, \ldots, d_n$, entonces el sistema 3.1 tiene una solución no trivial en $\mathbb{K}$ si y solo si* $\mathrm{Res}(F_0, \ldots, F_n) = 0$.
2. $\mathrm{Res}(x_0^{d_0}, \ldots, x_n^{d_n}) = 1$.
3. Res *es irreducible.*

La demostración de este teorema requiere un nivel mucho más alto que el de este trabajo, se puede encontrar en [10, Ch.4,Sec.4.2,Teo.4.4].
Cuando sea necesario escribiremos $\mathrm{Res}_{d_0,\ldots,d_n}$ para recalcar los grados, y llamaremos $\mathrm{Res}(F_0, \ldots, F_n)$ a la resultante de los polinomios $F_0 \ldots, F_n$.

Nota 3.1.2. Igual que ocurría para la resultante en una variable, cuando escribimos Res nos referimos al polinomio en el anillo $\mathbb{Z}[u_{i,\alpha}]$, el cual solo depende de los grados $d_0, \ldots, d_n$. Si ahora elegimos $F_0, \ldots, F_n$ polinomios homogéneos en $\mathbb{K}[x_0, \ldots, x_n]$, de grados $d_0, \ldots, d_n$, $\mathrm{Res}(F_0, \ldots, F_n)$ es un elemento de $\mathbb{K}$.

Al igual que pasaba con la resultante en una variable, la primera propiedad del teorema es la que nos va a permitir usar resultantes en teoría de eliminación, lo veremos en detalle en capítulos posteriores.

3.2. Propiedades

En esta sección vamos a dar una serie de propiedades sobre la resultante multivariada, generalizando las vistas para la resultante en una variable. No

voy a hacer ninguna de las demostraciones, se puede encontrar información más detallada en [3, Ch.3,Sec.3], donde deja como referencia los artículos [7] y [8], que aunque sean de un nivel mucho más alto que el de este trabajo, son esenciales en esta teoría. Para toda esta sección fijamos $d_0, \ldots, d_n$ números positivos y llamaremos $\mathrm{Res} = \mathrm{Res}_{d_0,\ldots,d_n}$ al polinomio introducido en el teorema 3.1.1. Primero vamos a dar una propiedad sobre el grado de la resultante.

Teorema 3.2.1. *Fijamos j entre 0 y n,* Res *es homogéneo en las variables $u_{j,\alpha}$ con $|\alpha| = d_j$, de grado $d_0 \cdots d_{j-1}d_{j+1} \cdots d_n$. En particular, si tenemos polinomios homogéneos $F_0, \ldots, F_n \in \mathbb{K}[x_0, \ldots, x_n]$ de grados $d_0, \ldots, d_n$,*

$$\mathrm{Res}(F_0, \ldots, \lambda F_j, \ldots, F_n) = \lambda^{d_0 \cdots d_{j-1}d_{j+1} \cdots d_n} \mathrm{Res}(F_0, \ldots, F_n).$$

Además, el grado total de Res *es $\sum_{j=0}^{n} d_0 \cdots d_{j-1}d_{j+1} \cdots d_n$.*

El siguiente teorema generaliza las propiedades 2.2.1 y 2.2.9 vistas para las resultantes en una variable.

Teorema 3.2.2. *1. Si $j < i$, entonces*

$$\begin{aligned}&\mathrm{Res}_{d_0,\ldots,d_j\ldots,d_i,\ldots,d_n}(F_0, \ldots, F_j, \ldots, F_i, \ldots, F_n) = \\ &(-1)^{d_0 \cdots d_n} \mathrm{Res}_{d_0,\ldots,d_i,\ldots,d_j,\ldots,d_n}(F_0, \ldots, F_i, \ldots, F_j, \ldots, F_n).\end{aligned}$$

2. Si $F_j = F_j' F_j''$, donde F_j' y F_j'' son polinomios homogéneos de grados d_j' y d_j'', entonces

$$\begin{aligned}&\mathrm{Res}_{d_0,\ldots,d_j,\ldots,d_n}(F_0, \ldots, F_j, \ldots, F_n) = \\ &\mathrm{Res}_{d_0,\ldots,d_j',\ldots,d_n}(F_0, \ldots, F_j', \ldots, F_n) \cdot \mathrm{Res}_{d_0,\ldots,d_j'',\ldots,d_n}(F_0, \ldots, F_j'', \ldots, F_n).\end{aligned}$$

Teorema 3.2.3. *Si denotamos por* $\mathrm{Res} = \mathrm{Res}_{d,\ldots,d}$ *y F_j son polinomios homogéneos de grado d, si consideramos los polinomios $G_i = \sum_{j=0}^{n} a_{ij}F_j$, donde los coeficientes (a_{ij}) forman una matriz invertible con entradas en $\mathbb{K}$, entonces*

$$\mathrm{Res}(G_0, \ldots, G_n) = \det(a_{ij})^{d^n} \mathrm{Res}(F_0, \ldots, F_n).$$

Vamos a generalizar la propiedad 2.2.10 para resultantes multivaradas, introducimos primero la siguiente notación. Si $F_0, \ldots, F_n \in \mathbb{K}[x_0, \ldots, x_n]$ son polinomios homogéneos de grados $d_0, \ldots, d_n$, para todo $i = 0, 1, \ldots, n$, consideramos los siguientes polinomios

$$\begin{aligned}f_i(x_1, \ldots, x_n) &= F_i(1, x_1 \ldots, x_n), \\ \overline{F}_i(x_1, \ldots, x_n) &= F_i(0, x_1 \ldots, x_n).\end{aligned} \tag{3.3}$$

Se tiene que $\overline{F}_0, \ldots, \overline{F}_n$ son polinomios homogéneos en $\mathbb{K}[x_1, \ldots, x_n]$ de grados $d_0, \ldots, d_n$.

Teorema 3.2.4. *Si* $\mathrm{Res}(\overline{F}_1,\ldots,\overline{F}_n)\neq 0$*, entonces el anillo cociente* $A=\mathbb{K}[x_1,\ldots,x_n]/\langle f_1,\ldots,f_n\rangle$ *tiene dimensión* $d_1\cdots d_n$ *visto como espacio vectorial sobre* $\mathbb{K}$*, y*

$$\mathrm{Res}(F_0,\ldots,F_n)=\mathrm{Res}(\overline{F}_1,\ldots,\overline{F}_n)^{d_0}\det(M_{f_0}),$$

donde M_{f_0} *es la matriz de la aplicación multiplicación por* f_0*,*

$$\begin{array}{rccl} m_{f_0}\colon & A & \longrightarrow & A \\ & [h] & \longmapsto & [f_0]\cdot[h]=[f_0h]\,. \end{array}$$

Nota 3.2.5. El resultado también es cierto si suponemos como hipótesis que $\mathrm{Res}(\overline{F}_0,\ldots,\overline{F}_{i-1},\overline{F}_{i+1},\ldots,\overline{F}_n)\neq 0$ y entonces

$$\mathrm{Res}(F_0,\ldots,F_n)=\mathrm{Res}(\overline{F}_0,\ldots,\overline{F}_{i-1},\overline{F}_{i+1},\ldots,\overline{F}_n)^{d_i}\det(M_{f_i}),$$

donde M_{f_i} es la matriz de la aplicación multiplicación por f_i en el anillo

$$A'=\mathbb{K}[x_1,\ldots,x_n]/\langle f_0,\ldots,f_{i-1},f_{i+1},\ldots,f_n\rangle.$$

Más aún, si en las ecuaciones (3.3) en vez de especializar x_0 hubiésemos especializado cualquier otra variable x_i, el resultado sigue siendo cierto, lo único que cambia en el teorema es que la aplicación multiplicación está definida en el anillo

$$A'=\mathbb{K}[x_0,\ldots,x_{i-1},x_{i+1},\ldots,x_n]/\langle f_1,\ldots,f_n\rangle.$$

Corolario 3.2.6. *Con la misma notación del teorema,*

$$\mathrm{Res}(x_0^d,F_1,\ldots,F_n)=\mathrm{Res}(\overline{F}_1,\ldots,\overline{F}_n)^d.$$

Demostración. Escribiendo $F_0=x_0^d$, se tiene que $f_0=1$ y por tanto la matriz de la aplicación m_1 es la identidad y aplicando el teorema anterior se tiene el resultado. □

Nota 3.2.7. Igual que antes, si en las ecuaciones (3.3) hubiésemos especializado x_i en vez de x_0, también se deduce que es cierta la igualdad

$$\mathrm{Res}(x_i^d,F_1,\ldots,F_n)=\mathrm{Res}(\overline{F}_1,\ldots,\overline{F}_n)^d.$$

De este teorema se deduce la siguiente versión del teorema de Bézout.

Teorema 3.2.8 (Teorema de Bézout)**.** *Sean* $f_1,\ldots,f_n$ *definidos como en (3.3) y suponemos que el sistema de ecuaciones* $\overline{F}_1=\cdots=\overline{F}_n=0$ *no tiene soluciones diferentes de la trivial. Entonces el sistema* $f_1=\cdots=f_n=0$ *tiene* $d_1\cdots d_n$ *soluciones (contadas con multiplicidad), y el anillo*

$$A=\mathbb{K}[x_1,\ldots,x_n]/\langle f_1,\ldots,f_n\rangle$$

tiene dimensión $d_1\cdots d_n$ *como espacio vectorial sobre* $\mathbb{K}$*.*

3.3. Cálculo de resultantes multivariadas

En este apartado vamos a intentar dar un método para calcular resultantes. Sean $\mathbf{F}_0, \ldots, \mathbf{F}_n \in \mathbb{Z}[u_{i,\alpha}][x_0, \ldots, x_n]$ polinomios universales homogéneos de grados $d_0, \ldots, d_n$, definimos

$$d = \sum_{i=0}^{n}(d_i - 1) + 1 = \sum_{i=0}^{n} d_i - n. \tag{3.4}$$

Si $\alpha \in \mathbb{N}^n$ es un multi-índice, se tiene que en total hay $N = \binom{d+n}{n}$ posibles valores de α que verifiquen que $|\alpha| = d$, por tanto hay N monomios $\underline{x}^\alpha$ de grado d. Vamos a dar un resultado que necesitaremos.

Lema 3.3.1. *Si $\underline{x}^\alpha$ es un monomio de grado d, entonces existe $0 \leq i \leq n$ tal que $x_i^{d_i}$ divide a $\underline{x}^\alpha$.*

Demostración. Razonando por reducción al absurdo, si para todo i se tiene que $x_i^{d_i}$ no divide a $\underline{x}^\alpha$, entonces $\alpha_i \leq d_i - 1$ para todo i, luego

$$\sum_{i=0}^{n} \alpha_i \leq \sum_{i=0}^{n}(d_i - 1) < d,$$

por tanto llegamos a contradicción ya que habíamos supuesto $|\alpha| = d$. □

Ahora definimos los siguientes conjuntos disjuntos:

$$\begin{aligned}
S_0 &= \{\underline{x}^\alpha \ : \ |\alpha| = d,\ x_0^{d_0} \text{ divide a } \underline{x}^\alpha\},\\
S_1 &= \{\underline{x}^\alpha \ : \ |\alpha| = d,\ x_0^{d_0} \text{ no divide a } \underline{x}^\alpha \text{ pero } x_1^{d_1} \text{ sí}\},\\
&\vdots\\
S_n &= \{\underline{x}^\alpha \ : \ |\alpha| = d,\ x_0^{d_0}, \ldots, x_{n-1}^{d_n - 1} \text{ no divide a } \underline{x}^\alpha \text{ pero } x_n^{d_n} \text{ sí}\}.
\end{aligned} \tag{3.5}$$

Proposición 3.3.2. *Hay exactamente $d_0 \cdots d_{n-1}$ monomios en S_n.*

Demostración. Voy a probar que dados $a_0, \ldots, a_{n-1}$ con $0 \leq a_i \leq d_i - 1$, existe un único a_n tal que $x_0^{a_0} \cdots x_n^{a_n} \in S_n$. Si pruebo esto, se tendría que en S_n hay tantos monomios como n-úplas de números con la condición de que cada $0 \leq a_i \leq d_i - 1$, luego habría $d_0 \cdots d_{n-1}$ elementos en S_n. Para que el monomio $x_0^{a_0} \cdots x_n^{a_n}$ pertenezca a S_n tiene que verificarse que $a_0 + \ldots + a_n = d$, luego el único valor que nos podría servir es $a_n = d - a_0 - \ldots - a_{n-1}$. Además, para este valor de a_n, el monomio $x_0^{a_0} \cdots x_n^{a_n}$ pertenece a S_n porque $x_0^{d_0} \cdots x_{n-1}^{d_{n-1}}$ no lo divide al ser cada $a_i < d_i$, y por el lema anterior necesariamente $x_n^{d_n}$ tiene que dividirlo, con esto ya hemos probado lo que queríamos ya que por construcción, a_n es único. □

Por el lema anterior, todo monomio de grado d pertenece a uno de estos conjuntos. Además si $\underline{x}^\alpha \in S_i$ y escribiendo

$$\underline{x}^\alpha = x_i^{d_i} \cdot \underline{x}^\alpha / x_i^{d_i},$$

tenemos que $\underline{x}^\alpha / x_i^{d_i}$ es un monomio de grado $d - d_i$. Consideramos el siguiente sistema:

$$\begin{aligned} \frac{\underline{x}^\alpha}{x_0^{d_0}} \cdot \mathbf{F}_0 = 0, \quad \forall \underline{x}^\alpha \in S_0, \\ \vdots \\ \frac{\underline{x}^\alpha}{x_n^{d_n}} \cdot \mathbf{F}_n = 0, \quad \forall \underline{x}^\alpha \in S_n. \end{aligned} \tag{3.6}$$

Como cada $\mathbf{F}_i$ tiene grado d_i, se tiene que $\underline{x}^\alpha / x_i^{d_i} \cdot \mathbf{F}_i$ es un polinomio homogéneo de grado d, por tanto, cada polinomio del lado izquierdo del sistema (3.6) se puede poner como una suma de monomios de grado d. Por otro lado, ya sabemos que en total hay N monomios distintos de grado d. Además, tenemos que el sistema tiene tantas ecuaciones como elementos en $S_0 \cup \ldots \cup S_n$, que también es N. Si consideramos cada monomio como una incógnita tenemos un sistema lineal de N ecuaciones con N incógnitas.

Notación 3.3.3. Denotaremos por $D_n \in \mathbb{Z}[u_{i,\alpha}]$ al determinante de la matriz de coeficientes del sistema (3.6). Como de costumbre, si especializamos los polinomios $\mathbf{F}_i$ en unos polinomios homogéneos $F_0, \ldots, F_n \in \mathbb{K}[x_0, \ldots, x_n]$, tenemos que $D_n(F_0, \ldots, F_n) \in \mathbb{K}$.

En el siguiente ejemplo vamos a ver que si tenemos dos polinomios universales homogéneos, D_1 coincide con la matriz de Sylvester (2.3).

Ejemplo 3.3.4. Si consideramos dos polinomios universales homogéneos $\mathbf{F}, \mathbf{G} \in \mathbb{Z}[u_{i,\alpha}][x, y]$ de grados 2 y 3,

$$\begin{aligned} \mathbf{F} &= c_0 x^2 + c_1 xy + c_2 y^2, \\ \mathbf{G} &= d_0 x^3 + d_1 x^2 y + d_2 xy^2 + d_3 y^3. \end{aligned}$$

Tenemos que $d = 2 + 3 - 1 = 4$, $N = \binom{4+1}{1} = 5$ y, los posibles valores de α son $(0,4), (4,0), (1,3), (3,1)$ y $(2,2)$. Calculando los conjuntos S_0, S_1 tenemos que

$$\begin{aligned} S_0 &= \{x^4, x^3 y, x^2 y^2\}, \\ S_1 &= \{y^4, xy^3\}. \end{aligned}$$

Por tanto tenemos el sistema:

$$\begin{aligned}
0 &= \frac{x^4}{x^2}\mathbf{F} = c_0x^4 + c_1x^3y + c_2x^2y^2,\\
0 &= \frac{x^3y}{x^2}\mathbf{F} = c_0x^3y + c_1x^2y^2 + c_2xy^3,\\
0 &= \frac{x^2y^2}{x^2}\mathbf{F} = c_0x^2y^2 + c_1xy^3 + c_2y^4,\\
0 &= \frac{xy^3}{y^3}\mathbf{G} = d_0x^4 + d_1x^3y + d_2x^2y^2 + d_3xy^3,\\
0 &= \frac{y^4}{y^3}\mathbf{G} = d_0x^3y + d_1x^2y^2 + d_2xy^3 + d_3y^4,
\end{aligned}$$

cuya matriz de coeficientes es la traspuesta de la matriz de Sylvester (2.3). Con este procedimiento vemos fácilmente que lo mismo ocurre si tenemos dos polinomios unviersales homogéneos de grados d_0 y d_1, se sigue verificando que D_1 es la traspuesta de la matriz de Sylvester.

De hecho, tenemos que D_n divide a la resultante, más concretamente tenemos el siguiente resultado:

Proposición 3.3.5. *Se tiene que:*

$$D_n = \mathrm{Res} \cdot A_n,$$

donde A_n es un polinomio entero en los coeficientes de $\mathbf{F}'_0, \ldots, \mathbf{F}'_{n-1}$, donde $\mathbf{F}'_i = \mathbf{F}_i(x_0, \ldots, x_{n-1}, 0)$.

Demostración. Primero vamos a ver que la resultante divide a D_n, es decir, veremos que $D_n \in \langle \mathrm{Res} \rangle$. Si denotamos por M al número de las variables $u_{i,\alpha}$, veremos que D_n se anula en $\mathrm{V}(\mathrm{Res})$ donde

$$\mathrm{V}(\mathrm{Res}) = \{c_{i,\alpha} : \ \mathrm{Res}(F_0, \ldots, F_n) = 0\} \subseteq \mathbb{K}^M,$$

y F_i es la especialización de $\mathbf{F}_i$ en los valores $c_{i,\alpha}$. Si $F_0, \ldots, F_n$ son polinomios homogéneos y tenemos que $F_0 = \ldots = F_n = 0$ tiene una solución no trivial, $(c_0, \ldots, c_n)$, es claro que también es solución del sistema (3.6) cuando especializamos los polinomios $\mathbf{F}_i$ en F_i, luego $D_n(F_0, \ldots, F_n) = 0$. Entonces, si para cierta especialización $c_{i,\alpha}$ de los polinomios $\mathbf{F}_i$ se tiene que $\mathrm{Res}(F_0, \ldots, F_n) = 0$, es decir, los puntos $c_{i,\alpha} \in \mathrm{V}(\mathrm{Res})$, entonces el sistema $F_0 = \ldots = F_n = 0$ tiene una solución no trivial gracias al teorema 3.1.1 y por tanto $D_n(F_0, \ldots, F_n) = 0$. Entonces ya hemos probado lo que queríamos porque hemos visto que

$$D_n \in \mathrm{I}(\mathrm{V}(\mathrm{Res})) = \sqrt{\langle \mathrm{Res} \rangle} = \langle \mathrm{Res} \rangle,$$

donde la priemera igualdad es gracias el teorema de los ceros de Hilbert y la segunda igualdad es gracias a que Res es un polinomio irreducible. Ahora veamos que A_n no depende de los coeficientes de F_n. Tanto D_n como Res son polinomios en $\mathbb{Z}[u_{i,\alpha}]$ por tanto, $A_n \in \mathbb{Q}[u_{i,\alpha}]$ ya que al dividir D_n por Res generamos coeficientes racionales. Si llamamos $m \in \mathbb{Z}$ al mínimimo común múltiplo de los denominadores de A_n, se tiene que $mA_n \in \mathbb{Z}[u_{i,\alpha}]$ y además, $mD_n = \text{Res} \cdot mA_n$, como $Z[u_{i,\alpha}]$ es un dominio de factorización única, existen $g_1, \ldots, g_s \in \mathbb{Z}[u_{i,\alpha}]$ irreducibles tales que $D_n = g_1 \cdots g_s$. Como Res es irreducible y divide a D_n necesariamente es uno de los g_i, y reordenando podemos suponer que $\text{Res} = g_s$, por tanto se deduce que $mA_n = m(g_1 \cdots g_{s-1})$, luego $A_n \in \mathbb{Z}[u_{i,\alpha}]$. Vamos a ver que D_n es homogéneo de grado $d_0 \cdots d_{n-1}$ visto como un polinomio en los coeficientes de $\mathbf{F}_n$, para ello vamos a ver que $D_n(F_0, \ldots, \lambda F_n) = \lambda^{d_0 \cdots d_{n-1}} D_n(F_0, \ldots, F_n)$. Si en el sistema (3.6), especializando en polinomios $F_0, \ldots, F_n$, si cambiamos F_n por λF_n estaremos modificando $d_0 \cdots d_{n-1}$ filas gracias a la proposición 3.3.2, por tanto se verifica la igualdad anterior. Entonces, tanto D_n como Res son homogéneos de grado $d_0 \cdots d_{n-1}$ en los coeficientes de $\mathbf{F}_n$, luego de la igualdad $D_n = \text{Res} \cdot A_n$ se sigue que A_n tiene grado cero en los coeficientes de $\mathbf{F}_n$, por tanto A_n solo depende de los coeficientes de $\mathbf{F}_0, \ldots, \mathbf{F}_{n-1}$. Para terminar la demostración falta ver que los coeficientes de $\mathbf{F}_0, \ldots, \mathbf{F}_{n-1}$ que acompañan a una potencia positiva de x_n no aparecen en A_n. Para ver esto, definimos el peso de cada variable $u_{i,\alpha}$, y lo denotaremos por $w(u_{i,\alpha})$, como el exponente α_n al que está elevado x_n, es decir, cada $u_{i,\alpha}$ acompaña a un monomio $\underline{x}^{\alpha}$ en el polinomio $\mathbf{F}_i$ y lo que estamos definiendo como el peso de $u_{i,\alpha}$ es el valor al que está elevado x_n en el monomio $\underline{x}^{\alpha}$. Si tenemos un monomio en $\mathbb{Z}[u_{i,\alpha}]$, será de la forma $u_{i_1,\alpha_1}^{m_1} \cdots u_{i_t,\alpha_t}^{m_t}$, definimos el peso del monomio como la suma de los pesos de cada u_{i_j,α_j} multiplicado por su respectivo exponente m_j. Por último, decimos que un polinomio en $\mathbb{Z}[u_{i,\alpha}]$ es *isobárico* si todos los monomios que lo forman tienen el mismo peso. Se puede probar que un polinomio $P(u_{i,\alpha})$ es isobárico de peso m si y solo si se tiene que para todo $\lambda \in \mathbb{K}$ distinto de cero

$$P(\lambda^{w(u_{i,\alpha})} u_{i,\alpha}) = \lambda^m P(u_{i,\alpha}).$$

De aquí se deduce fácilmente que D_n es isobárico de peso $d_0 \cdots d_n$ y que de la igualdad $D_n = \text{Res} \cdot A_n$ se tiene que como D_n es isobárico lo son tanto Res como A_n y el peso de D_n es la suma de los pesos de Res y A_n. Si, por ahorrar notación, llamamos u_i a la variable que acompaña a $x_i^{d_i}$ en $\mathbf{F}_i$, se tiene que uno de los términos de Res es $\pm u_0^{d_1 \cdots d_n} \cdots u_n^{d_1 \cdots d_{n-1}}$, ya que si especializamos los polinomios $\mathbf{F}_i$ en polinomios de la forma $a_i x_i^{d_i}$ con a_i no nulo, gracias a los teoremas 3.1.1 y 3.2.1 se tiene que

$$\text{Res}(a_0 x_0^{d_0}, \ldots, a_n x_n^{d_n}) = a_0^{d_1 \cdots d_n} \cdots a_n^{d_0 \cdots d_{n-1}}.$$

Como dicho término de Res tiene peso $d_0 \cdots d_n$, y es isobárico, se tiene que el peso de Res es igual al de D_n y por tanto el peso de A_n es nulo. □

Esta proposición nos da una forma de calcular la resultante: primero factorizamos D_n en factores irreducibles y el único factor en el que aparezcan todas las variables es la resultante. Sin embargo, este método que es muy simple teóricamente, computacionalmente es terrible debido al mal comportamiento computacional que tiene la factorización. Podemos abordar el problema de una forma un poco mejor, la construcción que hemos hecho de los conjuntos S_i en (3.5) depende del orden de las variables, es decir, hemos empezado comprobando con $x_0^{d_0}$ y hemos terminado con $x_n^{d_n}$, por eso hemos llamado al determinante D_n, haciendo recalcar la variable que hemos comprobado la última. Si cambiamos este orden y fijamos para $0 \leq i \leq n-1$, x_i como la última variable, los conjuntos (3.5) cambiarán y por tanto tendremos otro sistema (3.6) diferente, y si denotamos D_i al determinante de dicho sistema podemos dar otra fórmula para la resultante.

Proposición 3.3.6. *Si consideramos polinomios universales* $\mathbf{F}_0, \ldots, \mathbf{F}_n$*, la resultante es el máximo común divisor de los polinomios* $D_0, \ldots, D_n$ *vistos también como polinomios universales, es decir,*

$$\text{Res} = \pm \text{mcd}(D_0, \ldots, D_n). \tag{3.7}$$

Demostración. Para cada i, hay $n!$ posibles formas de ordenadar las variables $x_0, \ldots, x_n$ siendo x_i la última, luego hay $n!$ formas posibles de elegir D_i. Lo que queremos probar es que la fórmula del enunciado se verifica para cualquier elección de cada D_i. Como vimos en la proposición 3.3.5, $D_n = \text{Res} \cdot A_n$, usando los mismos argumentos se puede probar que $D_i = \text{Res} \cdot A_i$, donde $A_i \in \mathbb{Z}[u_{i,\alpha}]$ no depende de los coeficientes de $\mathbf{F}_i$, para cualquier elección de D_i. Por tanto tenemos que

$$\text{mcd}(D_0, \ldots, D_n) = \text{Res} \cdot \text{mcd}(A_0, \ldots, A_n),$$

y como cada A_i no depende de las variables $u_{i,\alpha}$, $\text{mcd}(A_0, \ldots, A_n) \in \mathbb{Z}$. Además, si especializamos cada $\mathbf{F}_i$ en los polinomios $x_i^{d_i}$ y ordenando correctamente las ecuaciones (3.6) se tiene que $D_n(x_0^{d_0}, \ldots, x_n^{d_n}) = \pm 1$, y entonces

$$\text{mcd}(D_0(x_0^{d_0}, \ldots, x_n^{d_n}), \ldots, D_n(x_0^{d_0}, \ldots, x_n^{d_n})) = \pm 1,$$

y como $\text{Res}(x_0^{d_0}, \ldots, x_n^{d_n}) = 1$, necesariamente $\text{mcd}(A_0, \ldots, A_n) = \pm 1$. □

Lamentablemente esta fórmula tampoco es muy útil en la práctica pero nos lleva hacia la fórmula que nos dice como encontrar exactamente el factor A_n de la proposición 3.3.5, que va a ser un menor del determinante D_n. Vamos a dar una defínción que nos permitirá calcular el menor que nos interesa.

Definición 3.3.7. Sean $d_0, \ldots, d_n$ números positivos y d como en 3.4.

1. Un monomio $\underline{x}^\alpha$ de grado d diremos que es reducido si $x_i^{d_i}$ divide a $\underline{x}^\alpha$ solamente para un i.

2. ${D_n}'$ es el determinante de la submatriz de la matriz de coeficientes del sistema (3.6) que se obtiene eliminando todas las filas y columnas correspondientes a monomios $\underline{x}^\alpha$ reducidos.

Esto nos da una fórmula de la resultante como el cociente de dos determinantes.

Teorema 3.3.8. *Sean $\mathbf{F}_0, \ldots, \mathbf{F}_n$ polinomios universales, la resultante viene dada por:*

$$\text{Res} = \pm \frac{D_n}{{D_n}'}.$$

Además, si K es un cuerpo y $F_0, \ldots, F_n \in K[x_0, \ldots, x_n]$, entonces la fórmula para la resultante se verifica siempre que ${D_n}' \neq 0$.

Este teorema lo he encontrado en [3, Ch.3,Sec.4,Th.4.9] y una demostración se puede encontrar en [8]. En el ejemplo 3.3.4, tenemos que todos los monomios que aparecen son reducidos, y por tanto ${D_1}' = 1$ y se tiene que la resultante de dos polinomios homogéneos es el determinante de la matriz de Sylvester.

Ejemplo 3.3.9. Sean $\mathbf{F}_0, \mathbf{F}_1, \mathbf{F}_2$ polinomios universales de grados $1, 2$ y 2 respectivamente, los escribimos como

$$\begin{aligned}
\mathbf{F}_0 &= a_0x_0 + a_1x_1 + a_2x_2,\\
\mathbf{F}_1 &= b_0x_0^2 + b_1x_1^2 + b_2x_2^2 + b_3x_0x_1 + b_4x_0x_2 + b_5x_1x_2,\\
\mathbf{F}_1 &= c_0x_0^2 + c_1x_1^2 + c_2x_2^2 + c_3x_0x_1 + c_4x_0x_2 + c_5x_1x_2.
\end{aligned}$$

Vamos a calcular $\text{Res}_{1,2,2}$. Para ello vamos a ultilizar la fórmula del teorema anterior con D_0, tenemos que $d = 1{+}2{+}2{-}2 = 3$ y $N = \binom{3+2}{2} = 10$ y todos los posibles valores de α son $(3,0,0), (0,3,0), (0,0,3), (2,1,0), (1,2,0), (1,0,2)$, $(2,0,1), (0,1,2), (0,2,1)$ y $(1,1,1)$. Como queremos considerar D_0 tenemos que comprobar x_0 la última, por tanto vamos a comprobar con el orden x_2, x_1, x_0 y obtenemos los siguientes conjuntos:

$$\begin{aligned}
S_0 &= \{x_0^3, x_0^2x_1, x_0^2x_2, x_0x_1x_2\},\\
S_1 &= \{x_0x_1^2, x_1^3, x_1^2x_2\},\\
S_2 &= \{x_0x_2^2, x_1x_2^2, x_2^3\}.
\end{aligned}$$

Construimos el sistema (3.6),

$$
\begin{aligned}
0 &= \frac{x_0^3}{x_0}\mathbf{F}_0 = a_0x_0^3 + a_1x_0^2x_1 + a_2x_0^2x_2,\\
0 &= \frac{x_0^2x_1}{x_0}\mathbf{F}_0 = a_0x_0^2x_1 + a_1x_0x_1^2 + a_2x_0x_1x_2,\\
0 &= \frac{x_0^2x_2}{x_0}\mathbf{F}_0 = a_0x_0^2x_2 + a_1x_0x_1x_2 + a_2x_0x_2^2,\\
0 &= \frac{x_0x_1x_2}{x_0}\mathbf{F}_0 = a_0x_0x_1x_2 + a_1x_1^2x_2 + a_2x_1x_2^2,\\
0 &= \frac{x_0x_1^2}{x_1^2}\mathbf{F}_1 = b_0x_0^3 + b_3x_0^2x_1 + b_4x_0^2x_2 + b_5x_0x_1x_2 + b_1x_0x_1^2 + b_2x_0x_2^2,\\
0 &= \frac{x_1^3}{x_1^2}\mathbf{F}_1 = b_0x_0^2x_1 + b_4x_0x_1x_2 + b_3x_0x_1^2 + b_1x_1^3 + b_5x_1^2x_2 + b_2x_1x_2^2,\\
0 &= \frac{x_1^2x_2}{x_1^2}\mathbf{F}_1 = b_0x_0^2x_2 + b_3x_0x_1x_2 + b_4x_0x_2^2 + b_1x_1^2x_2 + b_5x_1x_2^2 + b_2x_2^3,\\
0 &= \frac{x_0x_2^2}{x_2^2}\mathbf{F}_2 = c_0x_0^3 + c_3x_0^2x_1 + c_4x_0^2x_2 + c_5x_0x_1x_2 + c_1x_0x_1^2 + c_2x_0x_2^2,\\
0 &= \frac{x_1x_2^2}{x_2^2}\mathbf{F}_2 = c_0x_0^2x_1 + c_4x_0x_1x_2 + c_3x_0x_1^2 + c_1x_1^3 + c_5x_1^2x_2 + c_2x_1x_2^2,\\
0 &= \frac{x_2^3}{x_2^2}\mathbf{F}_2 = c_0x_0^2x_2 + c_3x_0x_1x_2 + c_4x_0x_2^2 + c_1x_1^2x_2 + c_5x_1x_2^2 + c_2x_2^3,
\end{aligned}
$$

donde las columnas están ordenadas de la siguiente manera:

$$x_0^3, x_0^2x_1, x_0^2x_2, x_0x_1x_2, x_0x_1^2, x_0x_2^2, x_1^3, x_1^2x_2, x_1x_2^2, x_2^3.$$

Por tanto, $D_0 = \det(M_0)$ donde M_0 es la matriz

$$
M_0 = \begin{pmatrix}
a_0 & a_1 & a_2 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & a_0 & 0 & a_2 & a_1 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & a_0 & a_1 & 0 & a_2 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & a_0 & 0 & 0 & 0 & a_1 & a_2 & 0\\
b_0 & b_3 & b_4 & b_5 & b_1 & b_2 & 0 & 0 & 0 & 0\\
0 & b_0 & 0 & b_4 & b_3 & 0 & b_1 & b_5 & b_2 & 0\\
0 & 0 & b_0 & b_3 & 0 & b_4 & 0 & b_1 & b_5 & b_2\\
c_0 & c_3 & c_4 & c_5 & c_1 & c_2 & 0 & 0 & 0 & 0\\
0 & c_0 & 0 & c_4 & c_3 & 0 & c_1 & c_5 & c_2 & 0\\
0 & 0 & c_0 & c_3 & 0 & c_4 & 0 & c_1 & c_5 & c_2
\end{pmatrix}.
$$

Ahora tenemos que todos los monomios son reducidos salvo $x_0x_1^2$ y $x_0x_2^2$, por tanto eliminando todas las filas y columnas salvo las correspondientes a

dichos monomios nos queda el sistema

$$0 = b_1 x_0 x_1^2 + b_2 x_0 x_2^2,$$
$$0 = c_1 c_0 x_1^2 + c_2 x_0 x_2^2.$$

Entonces, $D_0' = \det(M_0')$ donde M_0' es la matriz

$$M_0' = \begin{pmatrix} b_1 & b_2 \\ c_1 & c_2 \end{pmatrix}.$$

Ahora solo quedaría calcular dichos determinantes para obtener el polinomio $\mathrm{Res}_{1,2,2}$.

Hay muchas más fórmulas para calcular resultantes, para más información consultar [4], [11] y [12].

Capítulo 4

Teoría de la eliminación

Para intentar motivar este capítulo, supongamos que tenemos un sistema de dos ecuaciones en dos variables:

$$\begin{aligned} f_1(x, y) &= 0, \\ f_2(x, y) &= 0. \end{aligned} \tag{4.1}$$

Para encontrar las soluciones de dicho sistema, vamos a intentar dividir el proceso en dos partes:

1. **Eliminación:** En este paso vamos a intentar transformar nuestro sistema (4.1) en otro equivalente en el cual haya alguna ecuación que solo dependa de y, es decir, que hayamos eliminado la variable x de alguna ecuación. Una vez tengamos hecho esto, podemos resolver la ecuación que solo depende de y para hallar la coordenada y-ésima de una solución.

2. **Extensión:** En este paso, vamos a intentar extender la solución obtenida en el paso de eliminación, es decir, una vez tengamos la coordenada y-ésima de la solución, bajo que condiciones la podemos extender a una solución completa (x, y) de nuestro sistema original.

Otra reformulación de este problema es que si tenemos el ideal I en $K[x, y]$, generado por f_1 y f_2, cuando resolvemos el sistema (4.1) lo que estamos haciendo realmente es calcular $\mathrm{V}(I)$. Por tanto, nuestro objetivo es intentar determinar $\mathrm{V}(I) \subseteq K^2$. Para hacer esto vamos a intentar ir determinando los puntos coordenada a coordenada, es decir, para ver que puntos $(a_1, a_2) \in \mathrm{V}(I)$, primero vamos a intentar determinar las coordenadas a_2 y a partir de ellas calcular las coordenadas a_1 para que $(a_1, a_2) \in \mathrm{V}(I)$. En este capítulo vamos a dar la teoría que nos permitirá realizar este proceso correctamente con un número arbitrario de variables y en el siguiente capítulo se explica como hacerlo en la práctica.

4.1. Teorema de eliminación

En este apartado vamos a presentar la teoría necesaria para poder hacer el paso de eliminación arriba mencionado. Lo que vamos a hacer es intentar desglosar nuestro ideal original en otros más pequeños en los que hayan desaparecido algunas de las variables, es decir, en ideales tales que los polinomios que estén en ellos no dependan de algunas de las variables.

Definición 4.1.1. Sea K un cuerpo, consideramos un ideal $I \subseteq K[x_1, \ldots, x_n]$. Definimos el l-ésimo ideal de eliminación $I_l \subseteq K[x_{l+1}, \ldots, x_n]$ como:

$$I_l = I \cap K[x_{l+1}, \ldots, x_n].$$

Lo que nos dice esta definición es que en I_l están todos los elementos de I que no dependen de las variables $x_1, \ldots, x_l$, es decir, al quedarnos con el ideal I_l hemos eliminado las primeras l variables del ideal I. El teorema de eliminación nos va a decir cómo es este ideal y para ello nos va a proporcionar un sistema de generadores de dicho ideal.

Teorema 4.1.2 (Teorema de eliminación)**.** *Sea K un cuerpo y consideramos un ideal $I \subseteq K[x_1, \ldots, x_n]$. Sea G una base de Gröbner de I respecto de un orden de eliminación fijado donde $x_i > x_j$, para todo $i = 1, \ldots, l$, y todo $j = l+1, \ldots, n$. Entonces:*

$$G_l = G \cap K[x_{l+1}, \ldots, x_n]$$

es una base de Gröbner del ideal de eliminación I_l.

Demostración. Primero observamos que G_l es un subconjunto finito de I_l ya que

$$G_l = G \cap K[x_{l+1}, \ldots, x_n] \subseteq I \cap K[x_{l+1}, \ldots, x_n] = I_l,$$

por ser G base de Gröbner de I. Por la definición de base de Gröbner 1.1.8, G_l será base de Gröbner de I_l si los iniciales de los elementos de G_l generan $\text{in}(I_l)$, es decir, queremos ver que para todo $f \in I_l$ existe $g \in G_l$ tal que $\text{in}(g)$ divide a $\text{in}(f)$. Sea $f \in I_l = I \cap K[x_{l+1}, \ldots, x_n]$, en particular,

$$\text{in}(f) \in \text{in}(I) \cap K[x_{l+1}, \ldots, x_n].$$

Esto implica que existe $g \in G$ tal que $\text{in}(g)$ divide a $\text{in}(f)$. Ahora, como las variables $x_1, \ldots, x_l$ no están en $\text{in}(f)$, tampoco estarán en $\text{in}(g)$ ya que si no entraría en contradicción con que $\text{in}(g)$ divide a $\text{in}(f)$. Por último, gracias a que el orden que hemos fijado es un orden de eliminación con $x_i > x_j$, si $i = 1, \ldots, l$, y $j = l+1, \ldots, n$, tenemos que $g \in K[x_{l+1}, \ldots, x_n]$, porque si no entraríamos en contradicción con la definición de inicial 1.1.3. Entonces hemos probado que $g \in G \cap K[x_{l+1}, \ldots, x_n] = G_l$ como queríamos. □

El teorema de eliminación nos dice que siempre que tengamos un orden de eliminación como el del enunciado, las bases de Gröbner nos permiten tener toda la información del ideal de eliminación I_l ya que vamos a conocer un sistema de generadores de dicho ideal. Además una vez tengamos G, el teorema nos dice que G_l está formada por los elementos $g_j \in G$ que no tengan las variables $x_1, \ldots, x_l$, es decir, por los $g_j \in K[x_{l+1}, \ldots, x_n]$.
Esto nos permite, una vez fijado el orden de eliminación, eliminar las variables mayores. Por ejemplo, podemos fijar desde el principio el orden lexicográfico con $x_1 > \ldots > x_n$ y entonces podríamos eliminar x_1, x_1 y x_2,..., pero hay que tener cuidado, si no queremos usar el orden lexicográfico y queremos fijar otro orden de eliminación, para poder considerar la base de Gröbner G_i, tenemos que haber calculado G con un orden de eliminación en el que $x_j > x_t$ para $1 \leq j \leq i < i+1 \leq t \leq n$, por tanto vamos a tener que hacer varios cálculos de base de Gröbner dependiendo del ideal de eliminación que estemos buscando, ya que si ahora quisieramos calcular G_{i+1} tendríamos que la variable x_{i+1} no es del grupo de las mayores y por tanto no la podemos eliminar.

Ejemplo 4.1.3. Sea $I = \langle x - t^2, y - t^3 \rangle \subseteq K[x, y, t]$, si fijamos el orden lexicográfico con $x > y > t$, tenemos que $G = \{x - t^2, y - t^3\}$ es una base de Gröbner de I. Por tanto, $I_2 = I \cap K[t] = \langle 0 \rangle$ ya que en G_1 no hay ningún elemento que solo dependa de t, esto nos dice que en I no hay ningún polinomio solo en la variable t. También vemos que $I_1 = I \cap K[y, t] = \langle y - t^3 \rangle$. Ahora si quisieramos eliminar la variable t, tendríamos que cambiar el orden por otro orden de eliminación en el que t no fuese la más pequeña, por ejemplo si elegimos el orden lexicográfico con $t > y > x$ tenemos que $G = \{x^3 - y^2, ty - x^2, tx - y, t^2 - x\}$ es una base de Gröbner de I para este orden, y por tanto, $I \cap K[x, y] = \langle x^3 - y^2 \rangle$.

4.2. Teorema de extensión

Volviendo al problema que se planteaba al inicio del capítulo, el teorema de extensión es el que nos va a permitir ir calculando las soluciones coordenada a coordenada. El objetivo de este capítulo es probar el teorema de extensión. Vamos a dar dos pruebas, una usando bases de Gröbner y otra usando resultantes.

4.2.1. Teorema de extensión y bases de Gröbner

Primero vamos a introducir una notación y a dar unos resultados previos que vamos a necesitar para demostrar el teorema de extensión. Sea K un

cuerpo y $f \in K[x_1, \ldots, x_n]$ no nulo lo podemos escribir de la siguiente forma:

$$f = c_f(x_2, \ldots, x_n)x_1^{N_f} + \textit{ términos en los que } x_1 \textit{ tiene grado menor que } N_f,$$

donde $N_f \geq 0$ y $c_f \in K[x_2, \ldots, x_n]$ es no nulo. Además, elegimos $c_f = 0$ cuando $f = 0$ y si f no tiene la variable x_1, entonces $N_f = 0$ y $c_f = f$. Definimos el grado de f respecto de x_1 como $\deg(f, x_1) = N_f$. En el siguiente lema vamos a dar dos propiedades sobre $\deg(f, x_1)$ y c_f que vamos a necesitar más adelante.

Lema 4.2.1. *Sea $I \subseteq K[x_1, \ldots, x_n]$ un ideal y fijamos un orden de eliminación con $x_1 > x_i$ para $2 \leq i \leq n$. Sea $G = \{g_1, \ldots, g_t\}$ una base de Gröbner de I respecto de ese orden. Para cada $f \in I$ lo escribimos como el resultado de su división por G, $f = \sum_{j=1}^{t} A_j g_j$ donde $A_j \in K[x_1, \ldots, x_n]$ para $1 \leq j \leq t$. Entonces:*

1. $\deg(f, x_1) \geq \deg(A_j g_j, x_1)$ *siempre que* $A_j \neq 0$.
2. $c_f = \sum_j c_{A_j} c_{g_j}$, *para los* $A_j g_j$ *tales que* $\deg(A_j g_j, x_1) = \deg(f, x_1)$.

Demostración. La primera afirmación es consecuencia del algoritmo de división, es decir, al dividir f por G tenemos la expresión $f = \sum_{j=1}^{t} A_j g_j$ del enuncidado ya que como $f \in I$ el resto es nulo. Una de las propiedades del algoritmo de división nos dice que:

$$\forall j = 1, \ldots, t, \ \text{in}(f) \geq \text{in}(A_j g_j),$$

y como nuestro orden es de eliminación siendo la variable x_1 la mayor, se tiene que:

$$\deg(f, x_1) = \deg(\text{in}(f), x_1) \geq \deg(\text{in}(A_j g_j), x_1) = \deg(A_j g_j, x_1).$$

La hipotésis del enunciado de que $A_j g_j \neq 0$ es simplemente para representar los elementos que aportan algo en la escritura de f, también es cierto si quitamos esa condición pero realmente quitarla o añadirla no afecta al resultado. Para ver la segunda propiedad, podemos escribir para $1 \leq j \leq t$:

$$A_j = c_{A_j}(x_2, \ldots, x_n)x_1^{N_{A_j}} + \textit{ términos } a\underline{x}^{\alpha} \textit{ tales que} N_{\underline{x}^{\alpha}} < N_{A_j},$$
$$g_j = c_{g_j}(x_2, \ldots, x_n)x_1^{N_{g_j}} + \textit{ términos } a\underline{x}^{\alpha} \textit{ tales que} N_{\underline{x}^{\alpha}} < N_{g_j},$$

y entonces el producto $A_j g_j$ se puede escribir como:

$$A_j g_j = c_{A_j} c_{g_j}(x_2, \ldots, x_n)x_1^{N_j} + \textit{ términos } a\underline{x}^{\alpha} \textit{ tales que} N_{\underline{x}^{\alpha}} < N_j,$$

donde $N_j = N_{A_j} + N_{g_j}$. Y de aquí comparando los coeficientes de x_1^N a los dos lados de la igualdad $f = \sum_{j=1}^{t} A_j g_j$ se tiene lo que queremos. □

Teorema 4.2.2. *Sea $I \subseteq K[x_1, \ldots, x_n]$ un ideal y fijamos un orden de eliminación con $x_1 > x_i$ para $2 \leq i \leq n$. Sea $G = \{g_1, \ldots, g_t\}$ una base de Gröbner de I respecto de ese orden. Para cada $1 \leq j \leq t$ escribimos:*

$$g_j = c_j(x_2, \ldots, x_n)x_1^{N_j} + \text{ términos } a\underline{x}^{\alpha} \text{ tales que} N_{\underline{x}^{\alpha}} < N_j,$$

donde $N_j \geq 0$ y $c_j \in K[x_2, \ldots, x_n]$ no nulo. Sea $a = (a_2, \ldots, a_n) \in K^{n-1}$ y suponemos que $a \in \mathrm{V}(I_1)$ con la propiedad de que $a \notin \mathrm{V}(c_1, \ldots, c_t)$. Entonces:

$$\{f(x_1, a) \ : \ f \in I\} = \langle g_0(x_1, a)\rangle \subseteq K[x_1], \tag{4.2}$$

donde $g_0 \in G$ sastisface que $c_0(a) \neq 0$ y g_0 tiene grado mínimo respecto de x_1 entre todos los elementos $g_j \in G$ con $c_j(a) \neq 0$. Además:

1. $\deg(g_0(x_1, a)) > 0$.
2. *Si $g_0(a_1, a) = 0$ para algún $a_1 \in K$, entonces $(a_1, a) \in \mathrm{V}(I)$.*

Demostración. Si suponemos cierto (4.2) vamos a ver que se cumple (1) y (2). Elegimos $g_0 \in G$ con las propiedades del enunciado. Para probar (1), razonando por reducción al absurdo, si $\deg(g_0(x_1, a)) = 0$, entonces $\deg(g_0, x_1) = 0$ porque estamos suponiendo que $c_0(a) \neq 0$. Entonces $g_0 \in I_1$ y con la definición que hemos dado tenemos que $g_0 = c_0$. Pero entonces llegamos a contradicción ya que como $a \in \mathrm{V}(I_1)$ y $g_0 \in I_1$, $c_0(a) = g_0(a) = 0$, pero habíamos supuesto $c_0(a) \neq 0$. Ahora, la propiedad (2) es consecuencia inmediata de (4.2) porque si $g_0(a_1, a) = 0$, por (4.2) tenemos que $f(a_1, a) = 0$ para todo $f \in I$, es decir, que $(a_1, a) \in \mathrm{V}(I)$.
Por tanto, si probamos (4.2), habremos probado el teorema. Definimos la aplicación evaluación en a como:

$$\begin{array}{rccc} \phi_a \colon & K[x_1, \ldots, x_n] & \longrightarrow & K[x_1] \\ & f(x_1, \ldots, x_n) & \longmapsto & f(x_1, a) \end{array} \tag{4.3}$$

Debido a que la evaluación es compatible con la suma y producto de polinomios, tenemos que la aplicación ϕ_a es un homomorfismo de anillos. Aunque en general no es cierto, en este caso tenemos que si $I \subseteq K[x_1, \ldots, x_n]$ es un ideal, $\phi_a(I) = \{f(x_1, a) \ : \ f \in I\}$ es un ideal de $K[x_1]$. Para verlo, primero es claro que el polinomio nulo en $K[x_1]$ pertenece a $\phi_a(I)$ porque el polinomio nulo en $K[x_1, \ldots, x_n]$ pertenece a I por ser un ideal. Ahora, si tenemos dos polinomios $h, g \in \phi_a(I)$, existen $f_h, f_g \in I$ tales que $f_h(x_1, a) = h(x_1)$, $f_g(x_1, a) = g(x_1)$ y como $\phi_a(f_h + f_g) = \phi_a(f_h) + \phi_a(f_g) = h + g$, tenemos que $h + g \in \phi_a(I)$. Ahora, dado $g \in \phi_a(I)$, $r \in K[x_1]$, existe $f \in I$ tal que $f(x_1, a) = g(x_1)$ y r se puede ver como un polinomio de $K[x_1, \ldots, x_n]$

además cumpliendo que $r(x_1, a) = r(x_1)$, entonces $rf \in I$ por ser I ideal y $\phi_a(rf) = \phi_a(r)\phi_a(f) = rg$ lo que implica que $rg \in \phi_a(I)$, por tanto $\phi_a(I)$ es un ideal de $K[x_1]$. Además como I está generado por los $g_j \in G$, se tiene que $\phi_a(I)$ está generado por los $\phi_a(g_j) = g_j(x_1, a)$. Entonces para demostrar (4.2) basta ver que $g_j(x_1, a) \in \langle g_0(x_1, a)\rangle$ para todo $g_j \in G$ ya que la otra implicación es obvia al ser $\phi_a(I)$ generado por los $g_j(x_1, a)$ con $g_j \in G$ y ser g_0 uno de los g_j.
Para ver esto, vamos a separar la prueba en dos pasos:

1. Probar que si $g_j \in G$ y $\deg(g_j, x_1) < \deg(g_0, x_1)$, entonces $g_j(x_1, a) = 0$.

2. Probar por inducción sobre $\deg(g_j, x_1)$ que $g_j(x_1, a) \in \langle g_0(x_1, a)\rangle$, donde el paso 1 va a ser el caso base de la inducción.

Para el paso 1, sea $d_0 = \deg(g_0, x_1)$. Debido a la elección de g_0 tenemos que $c_0(a) \neq 0$, entonces $\deg(g_0(x_1, a)) = d_0$ y además, para cualquier otro $g_j \in G$ con $\deg(g_j, x_1) < d_0$ se tiene que $c_j(a) = 0$, luego al evaluar g_j en a su grado disminuye, es decir $\deg(g_j(x_1, a)) < \deg(g_j, x_1)$. Vamos a ver que de hecho se anula, es decir, $g_j(x_1, a) = 0$ y quedaría probado el paso 1.
Razonando por reducción al absurdo, suponemos que existe $g_j \in G$ con $\deg(g_j, x_1) < d_0$ y $g_j(x_1, a) \neq 0$. Por lo que hemos comentado, todos estos g_j's pierden grado cuando se evalúan en a. Ahora, entre todos los g_j's que cumplan esta propiedad, denotamos por g_b al que minimiza la pérdida de grado cuando se evalúa en a y veamos que la exitencia de este g_b nos lleva a contradicción.
Sea $\delta = \deg(g_b, x_1) - \deg(g_b(x_1, a))$ la cantidad de grado que pierde g_b cuando se evalúa en a. Para cualquier otro $g_j \in G$ con $\deg(g_j, x_1) < d_0$ se tiene que $g_j(x_1, a) = 0$ o entonces tiene una pérdida de grado como poco δ.
Sea $d_b = \deg(g_b, x_1)$, entonces $\deg(g_b(x_1, a)) = d_b - \delta$. Construimos el siguiente polinomio:

$$\begin{aligned} S &= c_0 x_1^{d_0 - d_b} g_b - c_b g_0 \in I \\ &= c_0 x_1^{d_0 - d_b}(c_b x_1^{d_b} + \ldots) - c_b(c_0 x_1^{d_0} + \ldots). \end{aligned}$$

Entonces $\deg(S, x_1) < d_0$ ya que se anula el término de grado d_0. Ahora vamos a calcular $\deg(S(x_1, a))$ de dos formas diferentes y ver que llegamos a contradicción.
La primera forma de calcular el grado es evaluar directamente en a. Entonces tenemos que

$$S(x_1, a) = c_0(a) x_1^{d_0 - d_b} g_b(x_1, a) - c_b(a) g_0(x_1, a) = c_0(a) x_1^{d_0 - d_b} g_b(x_1, a)$$

porque $c_b(a) = 0$ y $c_0(a) \neq 0$, por tanto,

$$\deg(S(x_1, a)) = d_0 - d_b + \deg(g_b(x_1, a)) = d_0 - d_b + d_b - \delta = d_0 - \delta. \quad (4.4)$$

La segunda forma de ver el grado, como tenemos que $S \in I$ lo podemos escribir como $S = \sum_{j=1}^{t} B_j g_j$, donde $B_j \in K[x_1, \ldots, x_n]$ para $1 \leq j \leq t$. Usando el lema previo 4.2.1 y que $\deg(S, x_1) < d_0$) tenemos la desigualdad

$$\deg(B_j, x_1) + \deg(g_j, x_1) = \deg(B_j g_j, x_1) \leq \deg(S, x_1) < d_0$$

siempre que $B_j \neq 0$. Además se tiene que los g_j's que aparecen en la desigualdad cumplen que $\deg(g_j, x_1) < d_0$, luego $g_j(x_1, a) = 0$ o tiene una pérdida de grado respecto a x_1 como poco δ. Entonces se sigue que

$$\deg(B_j(x_1, a)) + \deg(g_j(x_1, a)) \leq \deg(B_j, x_1) + \deg(g_j, x_1) - \delta < d_0 - \delta,$$

ahora evaluando la expresión $S = \sum_{j=1}^{t} B_j g_j$ en a tenemos que

$$\deg(S(x_1, a)) \leq \text{máx}(\deg(B_j(x_1, a)) + \deg(g_j(x_1, a))) < d_0 - \delta.$$

Y hemos entrado en contradicción con (4.4) y queda probado el paso 1.
Para el paso 2, probaremos por inducción sobre $\deg(g_j, x_1)$ que para todo $g_j \in G$ se tiene que $g_j(x_1, a) \in \langle g_0(x_1, a)\rangle$. Si $\deg(g_j, x_1) < d_0$, entonces por el paso 1 se tiene que $g_j(x_1, a) = 0 \in \langle g_0(x_1, a)\rangle$.
Empezando con la inducción, sea $d > d_0$ y suponemos que la afirmación del paso 2 es cierta para todo $g_j \in G$ con $\deg(g_j, x_1) < d$. Sea $g_j \in G$ con $\deg(g_j, x_1) = d$ y consideramos el polinomio:

$$\begin{aligned} S &= c_0 g_j - c_j x_1^{d-d_0} g_0 \in I \\ &= c_0(c_j x_1^d + \ldots) - c_j x_1^{d-d_0}(c_0 x_1^{d_0} + \ldots). \end{aligned}$$

Como se anula el término de grado d se tiene que $\deg(S, x_1) < d$.
Ahora como $S \in I$ lo podemos escribir de la forma $S = \sum_{l=1}^{t} B_l g_l$, donde $B_l \in K[x_1, \ldots, x_n]$ para $1 \leq l \leq t$. Repitiendo el proceso que hicimos en el paso 1, se puede ver que $\deg(g_l, x_1) < d$ cuando $B_l \neq 0$ y por hipótesis de inducción se tiene que $g_l(x_1, a) \in \langle g_0(x_1, a)\rangle$ cuando $B_l \neq 0$. Entonces,

$$c_0 g_j = c_j x_1^{d-d_0} g_0 + S = c_j x_1^{d-d_0} g_0 + \sum_{l=1}^{t} B_l g_l$$

como $c_0(a) \neq 0$ implica que

$$c_0(a) g_j(x_1, a) = c_j(a) x_1^{d-d_0} g_0(x_1, a) + \sum_{l=1}^{t} B_l(x_1, a) g_l(x_1, a) \in \langle g_0(x_1, a)\rangle.$$

Por tanto hemos probado la inducción y completado el paso 2. □

Con estos resultados previos ya podemos enunciar y demostrar de forma sencilla el teorema de extensión.

Teorema 4.2.3 (Teorema de extensión)**.** *Sea $\mathbb{K}$ un cuerpo algebraicamente cerrado y sea $I = \langle f_1, \ldots, f_s \rangle \subseteq \mathbb{K}[x_1, \ldots, x_n]$ un ideal. Sea I_1 el primer ideal de eliminación de I. Para cada $1 \leq i \leq s$ escribimos f_i como:*

$$f_i = c_i(x_2, \ldots, x_n)x_1^{N_i} + \text{ términos } a\underline{x}^{\alpha} \text{ tales que} N_{\underline{x}^{\alpha}} < N_i,$$

donde $N_i \geq 0$ y $c_i \in \mathbb{K}[x_2, \ldots, x_n]$ no nulo. Suponemos que tenemos un punto $(a_2, \ldots, a_n) \in \mathrm{V}(I_1)$. Si $(a_2, \ldots, a_n) \notin \mathrm{V}(c_1, \ldots, c_s)$ entonces existe $a_1 \in \mathbb{K}$ tal que $(a_1, \ldots, a_n) \in \mathrm{V}(I)$.

Demostración. Fijamos un orden de eliminación con $x_1 > x_i$ para $2 \leq i \leq t$ y sea $G = \{g_1, \ldots, g_t\}$ una base de Gröbner de I. Sea $a = (a_2, \ldots, a_n)$ como en el enunciado y veamos que al menos existe un $g_j \in G$ tal que $c_{g_j} \neq 0$. Por hipótesis, como $a \notin \mathrm{V}(c_1, \ldots, c_s)$ existe $i \in \{1, \ldots, s\}$ tal que $c_i(a) \neq 0$. Escribiendo f_i como el resultado de la división por G, $f_i = \sum_{j=1}^{t} A_j g_j$, con $A_j \in \mathbb{K}[x_1, \ldots, x_n]$ para $1 \leq j \leq t$, por el lema 4.2.1 tenemos que:

$$c_i = \sum_{\deg(A_j g_j, x_1) = N_i} c_{A_j} c_{g_j}.$$

Entonces como $c_i(a) \neq 0$ significa que existe al menos un $j \in \{1, \ldots, t\}$ tal que $c_{g_j} \neq 0$. Ahora estamos en condiciones de aplicar el teorema 4.2.2.
El teorema nos dice que existe $g_0 \in G$ con $\deg(g_0(x_1, a)) > 0$. Además como $\mathbb{K}$ es un cuerpo algebraicamente cerrado, existe $a_1 \in \mathbb{K}$ tal que $g_0(a_1, a) = 0$. Entonces, el teorema también nos dice que $(a_1, a) \in \mathrm{V}(I)$ como queríamos probar. □

4.2.2. Teorema de extensión y resultantes

En esta sección vamos a volver a demostrar el teorema de extensión pero esta vez usando resultantes vistos en el capítulo 2. Vamos a empezar dando unos resultados previos que serán necesarios para la demostración del teorema. Sea K un cuerpo y $f, g \in K[x_1, \ldots, x_n]$ polinomios no nulos de grados l y m en x_1 respectivamente. Los podemos ver como polinomios en $K[x_2, \ldots, x_n][x_1]$ y escribirlos como:

$$\begin{aligned} f(x) &= \sum_{i=0}^{l} c_i x_1^i, \\ g(x) &= \sum_{i=0}^{m} d_i x_1^i. \end{aligned} \tag{4.5}$$

donde $c_i, d_i \in K[x_2, \ldots, x_n]$ con c_l, d_m no nulos. Como en la sección anterior, el grado de f respecto de la variable x_1 lo vamos a denotar por $\deg(f, x_1) = l$ y de la misma forma para g. Por la proposición 2.2.2 se tiene que $\mathrm{Res}(f, g, x_1)$ es un polinomio en $K[x_2, \ldots, x_n]$ y además, por la proposición 2.2.7 podemos escribir:

$$\mathrm{Res}(f, g, x_1) = Af + Bg,$$

con $A, B \in K[x_1, \ldots, x_n]$, es decir, tenemos que

$$\mathrm{Res}(f, g, x_1) \in \langle f, g \rangle \cap K[x_2, \ldots, x_n].$$

Entonces tenemos que $\mathrm{Res}(f, g, x_1)$ pertenece al primer ideal de eliminación de $\langle f, g \rangle$. Si tenemos un punto $a = (a_2, \ldots, a_n) \in K^{n-1}$ podemos evaluar $\mathrm{Res}(f, g, x_1)(a)$ que es lo que llamaremos una especialización de la resultante, sin embargo, puede ocurrir que

$$\mathrm{Res}(f, g, x_1)(a) \neq \mathrm{Res}(f(x_1, a), g(x_1, a)).$$

Vamos a ilustrar esto con el siguiente ejemplo:

Ejemplo 4.2.4. Sean $f, g \in \mathbb{C}[x, y]$ los siguientes polinomios:

$$f = x^2y + 3x - 1,$$
$$g = 6x^2 + y^2 - 4.$$

Entonces tenemos que la matriz de Sylvester respecto de la variable x es la siguiente matriz de tamaño 4×4:

$$\mathrm{Syl}(f, g, x) = \begin{pmatrix} -1 & 0 & y^2 - 4 & 0 \\ 3 & -1 & 0 & y^2 - 4 \\ y & 3 & 6 & 0 \\ 0 & y & 0 & 6 \end{pmatrix},$$

y $\mathrm{Res}(f, g, x) = \det(\mathrm{Syl}(f, g, x)) = (y^2 - 4)(12y + 54 + y^2(y^2 - 4)) + 36$. Se tiene que $\mathrm{Res}(f, g, x)(0) = -180$, pero si evaluamos f, g en $y = 0$ tenemos que $f(x, 0) = 3x - 1$, $g(x, 0) = 6x^2 - 4$ y si calculamos $\mathrm{Syl}(3x - 1, 6x^2 - 4)$ tenemos la matriz 3×3:

$$\mathrm{Syl}(3x - 1, 6x^2 - 4) = \begin{pmatrix} -1 & 0 & -4 \\ 3 & -1 & 0 \\ 0 & 3 & 6 \end{pmatrix},$$

y $\mathrm{Res}(3x - 1, 6x^2 - 4) = \det(\mathrm{Syl}(3x - 1, 6x^2 - 4)) = -30$.

Pero afortunadamente tenemos una situación en la que sabemos la relación que tienen estas dos expresiones.

Proposición 4.2.5. *Sean $f, g \in K[x_1, \ldots, x_n]$ no nulos con $\deg(f, x_1) = l$ y $\deg(g, x_1) = m$. Sea $a = (a_2, \ldots, a_n) \in K^{n-1}$ tal que:*

1. *$f(x_1, a) \in K[x_1]$ y $\deg(f(x_1, a)) = l$ (esto implica que $c_0(a) \neq 0$).*
2. *$g(x_1, a) \in K[x_1]$ no nulo y $\deg((g(x_1, a)) = p \leq m$.*

Si c_0 es como en (4.5), entonces:

$$\mathrm{Res}(f, g, x_1)(a) = c_0(a)^{m-p}\mathrm{Res}(f(x_1, a), g(x_1, a)).$$

Demostración. Si $l = m = 0$, las hipótesis de f y g no nulos implican que $c_0(a), d_0(a) \neq 0$ y por la expresión (2.4) la ecuación de la proposición se simplifica a la igualdad $1 = 1$.
Si $l = 0$ y $m > 0$ entonces $f(x_1, a) = c_0(a) \neq 0$ por ser f no nulo. Entonces por (2.4) se tiene que:

$$\mathrm{Res}(f(x_1, a), g(x_1, a)) = \begin{cases} c_0(a)^p & si\ p > 0 \\ 1 & si\ p = 0 \end{cases}.$$

Además, también por (2.4) se tiene que $\mathrm{Res}(c_o, g, x_1)(a) = c_0(a)^m$, por lo tanto es cierto. El caso $m = 0$ y $l > 0$ se hace de manera similar.
Ahora suponemos $l, m > 0$. Si evaluamos $\mathrm{Syl}(f, g, x_1)$ en el punto a y calculamos su determinante,

$$\mathrm{Res}(f, g, x_1)(a) = \begin{vmatrix} c_0(a) & & & d_0(a) & & \\ c_1(a) & \ddots & & d_1(a) & \ddots & \\ c_2(a) & \ddots & c_0(a) & \vdots & \ddots & d_0(a) \\ \vdots & & c_1(a) & d_m(a) & & d_1(a) \\ c_l(a) & & \vdots & & \ddots & \vdots \\ & & c_l(a) & & & d_m(a) \end{vmatrix}. \tag{4.6}$$

Si $\deg(g(x_1, a)) = p = m$ entonces $d_0(a) \neq 0$ y escribiendo:

$$f(x_1, a) = c_0(a)x_1^l + \ldots + c_l(a),$$
$$g(x_1, a) = d_0(a)x_1^m + \ldots + d_m(a),$$

se tiene que $\mathrm{Res}(f, g, x_1)(a) = \mathrm{Res}(f(x_1, a), g(x_1, a))$ simplemente por la definición de resultante de dos polinomios en una variable 2.1.4.
Si $p < m$, entonces $d_0(a) = \ldots = d_{m-p-1}(a) = 0$ y $d_{m-p} \neq 0$, desarollando por la primera fila en 4.6 se llega a la expresión de la proposición. □

Ahora si consideramos $\mathbb{K}$ un cuerpo algebraicamente cerrado tenemos el siguiente corolario.

Corolario 4.2.6. *Sean $f, g \in \mathbb{K}[x_1, \ldots, x_n]$ polinomios no nulos tales que $\deg(f, x_1) = l$ y $\deg(g, x_1) = m$. Sea $a = (a_2, \ldots, a_n) \in \mathbb{K}^{n-1}$ tal que:*

1. *$f(x_1, a) \in \mathbb{K}[x_1]$ tiene grado l o $g(x_1, a) \in \mathbb{K}[x_1]$ tiene grado m.*
2. *$\mathrm{Res}(f, g, x_1)(a) = 0$.*

Entonces existe $a_1 \in \mathbb{K}$ tal que $f(a_1, a) = g(a_1, a) = 0$.

Demostración. De la propiedad (1) podemos suponer que $\deg(f(x_1, a)) = l$, si ocurriese que $g(x_1, a)$ fuese el que tuviese grado m se hace igual. Como $\deg(f(x_1, a)) = l$ implica que $c_0(a) \neq 0$. Si suponemos que $g(x_1, a) \neq 0$ y sea $p = \deg(g(x_1, a))$ por la proposición anterior tenemos que:

$$0 = \mathrm{Res}(f, g, x_1)(a) = c_0(a)^{m-p}\mathrm{Res}(f(x_1, a), g(x_1, a)).$$

Por el corolario 2.2.3 y como $\mathrm{Res}(f(x_1, a), g(x_1, a)) = 0$, existe $a_1 \in \mathbb{K}$ tal que $f(a_1, a) = g(a_1, a) = 0$ como queríamos probar.
Ahora si $g(x_1, a) = 0$ y $\deg(f(x_1, a)) = l > 0$ entonces $f(x_1, a)$ tiene al menos una raíz $a_1 \in \mathbb{K}$, luego $f(a_1, a) = g(a_1, a) = 0$ como queremos probar.
Vamos a ver que no puede ocurrir que $l = 0$ con las hipótesis del enunciado. Si suponemos $l = 0$ por la definición 2.4 tenemos que $\mathrm{Res}(f, g, x_1) = c_0^m$, y como tenemos que $c_0(a) \neq 0$ por ser f no nulo entramos en contradicción con (2). □

Ahora ya estamos en condiciones de poder enunciar y probar el teorema de extensión.

Teorema 4.2.7 (Teorema de extensión)**.** *Sea $\mathbb{K}$ un cuerpo algebraicamente cerrado y sea $I = \langle f_1, \ldots, f_s \rangle \subseteq \mathbb{K}[x_1, \ldots, x_n]$ un ideal. Sea I_1 el primer ideal de eliminación de I. Para cada $1 \leq i \leq s$ escribimos f_i como:*

$$f_i = c_i(x_2, \ldots, x_n)x_1^{N_i} + \text{ términos } a\underline{x}^{\alpha} \text{ tales que} N_{\underline{x}^{\alpha}} < N_i,$$

donde $N_i \geq 0$ y $c_i \in \mathbb{K}[x_2, \ldots, x_n]$ no nulo. Suponemos que tenemos un punto $(a_2, \ldots, a_n) \in \mathrm{V}(I_1)$. Si $(a_2, \ldots, a_n) \notin \mathrm{V}(c_1, \ldots, c_s)$ entonces existe $a_1 \in \mathbb{K}$ tal que $(a_1, \ldots, a_n) \in \mathrm{V}(I)$.

Demostración. La primera parte se repite de la de demostración del teorema 4.2.2. Resumiendo, tenemos que la aplicación evaluación en a

$$\begin{array}{rccc} \phi_a \colon & \mathbb{K}[x_1, \ldots, x_n] & \longrightarrow & \mathbb{K}[x_1] \\ & f(x_1, \ldots, x_n) & \longmapsto & f(x_1, a) \end{array}$$

es un homomorfismo de anillos tal que la imagen de un ideal I es un ideal en $\mathbb{K}[x_1]$. Gracias al algoritmo de división, ver [2, Ch.1,Sec.5,Coro.4], se tiene que existe $g \in \mathbb{K}[x_1]$ tal que $\phi_a(I) = \langle g(x_1)\rangle$, entonces

$$\phi_a(I) = \{f(x_1, a) \ : \ f \in I\} = \langle g(x_1)\rangle,$$

y en particular existe $f_0 \in I$ tal que $g(x_1) = f_0(x_1, a)$. Entonces

$$\phi_a(I) = \{f(x_1, a) \ : \ f \in I\} = \langle f_0(x_1, a)\rangle.$$

Ahora como $a \notin \mathrm{V}(c_1, \ldots, c_s)$, existe $1 \leq i \leq s$ tal que $c_i(a) \neq 0$, entonces $\deg(f_i(x_1, a)) = \deg(f_i, x_1)$, es decir, f_i no pierde grado al evaluar en i. Además, como f_i no es nulo gracias a que $c_i(a) \neq 0$ se tiene que $\deg(f_i, x_i) > 0$ ya que si no, f_i pertenecería a I_1 y como a pertenece a $\mathrm{V}(I_1)$ se tendría que $f_i(x_1, a) = f_i(a) = 0$ lo que no ocurre. Entonces $\phi_a(I)$ no es el ideal nulo y por tanto $f_0(x_1, a)$ es no nulo. Aplicando los resultados previos a los polinomios f_i, f_0 tenemos que

$$\mathrm{Res}(f_i, f_0, x_1) \in \langle f_i, f_0\rangle \cap \mathbb{K}[x_2, \ldots, x_n] \subseteq I \cap \mathbb{K}[x_2, \ldots, x_n] = I_1.$$

Además, como $a \in \mathrm{V}(I_1)$ se tiene que $\mathrm{Res}(f_i, f_0, x_1)(a) = 0$ y como se verifican todas las hipótesis podemos aplicar el corolario 4.2.6, entonces existe $a_1 \in \mathbb{K}$ tal que $f_i(a_1, a) = f_0(a_1, a) = 0$. Como $f_0(a_1, a) = 0$ se tiene que $f(a_1, a) = 0$ para todo $f \in I$ luego $(a_1, a) = (a_1, a_2, \ldots, a_n) \in \mathrm{V}(I)$ como queríamos demostrar. □

Estas dos demostraciones alternativas del Teorema de extensión son una muestra de como las resultantes permiten, a veces, prescindir de las bases de Gröbner.
Como comentario final de esta sección, recalcar que el teorema de extensión da una condición suficiente pero no necesaria para que un punto se pueda extender. Veamos esto con un ejemplo, consideramos los polinomios

$$f(x, y) = x^2y + x - 1,$$
$$g(x, y) = x^2y + x + y^3 - y - 1.$$

Si consideramos el orden lexicográfico con $x > y$ y con el siguiente código de Singular [5] calculamos una base de Gröbner de $I = \langle f, g\rangle$,

```
> ring A=0,(x,y),lp;
> poly f=x2y+x-1;
> poly g=x2y+x+y3-y-1;
> ideal I=f,g;
```

```
> ideal bg=groebner(I);bg;
bg[1]=y3-y
bg[2]=xy2-x+y5-2y3-y2+y+1
bg[3]=x2-xy5+2xy3+xy2-x+y4-y2-y
```

se tiene que $I_1 = \langle y^3 - y \rangle$, y por tanto $0 \in \mathrm{V}(I_1)$. Si intentamos aplicar el teorema de extensión vemos que $c_1(0) = c_2(0) = 0$, luego $0 \in \mathrm{V}(c_1, c_2)$ y el teorema no se puede aplicar. Sin embargo podemos extender 0 al punto $(1, 0) \in \mathrm{V}(I)$.

Capítulo 5

Aplicaciones

En este capítulo vamos a dar un par de aplicaciones de la teoría vista en el capítulo 4 y cuando se pueda lo vamos a intentar relacionar con las resultantes. Como comentario, añadir que aunque vamos a presentar las aplicaciones con ejemplos más o menos sencillos, para aplicar esto a problemas reales posiblemente hagan falta técnicas de cálculo numérico para aproximar soluciones de ecuaciones en una variable.

5.1. Resolución de sistemas

Vamos a ver como se podría abordar el problema usando bases de Gröbner y los teoremas de eliminación y extensión, luego vamos a ver dos métodos usando resultantes. En esta sección solo vamos a tratar el caso en el que los sistemas tengan un número finito de soluciones. Estos sistemas los hemos caracterizado, cuando el cuerpo es algebraicamente cerrado, en la asignatura *Álgebra conmutativa y computacional*, para más información se recomienda consultar [2, Ch.5,Sec.3].

5.1.1. Bases de Gröbner

Vamos a empezar viendo un ejemplo sencillo de como se aplican los teoremas de eliminación y extensión para resolver sistemas de ecuaciones.
Dados $f, g \in \mathbb{C}[x, y]$ consideramos el sistema:

$$\begin{aligned} f(x, y) = xy - 1 = 0, \\ g(x, y) = x^3 + xy - x - 1 = 0. \end{aligned}$$

Definimos el ideal $I = \langle xy - 1, x^3 + xy - x - 1 \rangle$ entonces las soluciones de nuestro sistema coinciden con $\mathrm{V}(I) = \{(x, y) \in \mathbb{C}^2 \ : \ f(x, y) = g(x, y) = 0\}$.

Si fijamos el orden lexicográfico con $x > y$, una base de Gröbner de I es $G = \{g_1, g_2\}$, donde

$$g_1 = x - y,$$
$$g_2 = y^2 - 1.$$

Además, gracias a que las bases de Gröbner son sistemas de generadores tenemos que $\mathrm{V}(I) = \mathrm{V}(x - y, y^2 - 1)$. Por tanto, nuestro sistema original se ha convertido en otro equivalente en el que hay una ecuación que solo depende de la variable y,

$$g_1(x, y) = x - y = 0,$$
$$g_2(x, y) = y^2 - 1 = 0.$$

Entonces podemos resolver la segunda ecuación y nos daría que los posibles valores de y en la solución son $y = \pm 1$. Lo que hemos hecho realmente es calcular $I_1 = I \cap \mathbb{C}[y]$, que gracias al teorema de eliminación:

$$I_1 = G \cap \mathbb{C}[y] = \langle y^2 - 1 \rangle.$$

Por tanto $\mathrm{V}(I_1) = \{\pm 1\}$. A las soluciones $y = \pm 1$ las vamos a llamar soluciones parciales del sistema, y lo que buscamos ahora es extenderlas a soluciones completas, es decir, intentamos buscar $x \in \mathbb{C}$ tales que $f(x, y) = g(x, y) = 0$ cuando $y \in \mathrm{V}(I_1)$. Aquí es cuando entra en juego el teorema de extensión, tenemos $y \in \mathrm{V}(I_1)$ y queremos encontrar $x \in \mathbb{C}$ tal que $(x, y) \in \mathrm{V}(I)$. Con la notación del teorema de extensión, tenemos que $c_1 = y$, $c_2 = 1$. Además como $\pm 1 \notin \mathrm{V}(c_1, c_2) = \mathrm{V}(y, 1)$, el teorema nos asegura que son soluciones parciales que podemos extender a una completa. Por tanto, despejando en $g_1(x, y) = 0$ tenemos que las soluciones del sistema son $(1, 1)$ y $(-1, -1)$.
Generalizando este ejemplo, si tenemos $\mathbb{K}$ un cuerpo algebraicamente cerrado, $f_1, \ldots, f_n \in \mathbb{K}[x_1, \ldots, x_n]$ polinomios no nulos y consideramos el sistema

$$f_1 = \cdots = f_n = 0.$$

Contruimos el ideal $I = \langle f_1, \ldots, f_n \rangle$ y la idea es determinar que puntos $(a_1, \ldots, a_n) \in \mathbb{K}^n$ pertenecen a $\mathrm{V}(I)$. Los vamos a intentar construir coordenada a coordenada, es decir, ir construyendo soluciones parciales del sistema cada vez con una coordenada más.
Para determinar las posibles coordenadas a_n, consideramos el ideal de eliminación $I_{n-1} = I \cap \mathbb{K}[x_n]$, su base de Gröbner G_{n-1} y determinamos las soluciones parciales a_n que pertenezcan a $\mathrm{V}(I_{n-1}) = \mathrm{V}(G_{n-1})$. Ahora, aplicamos el teorema de extensión sobre el ideal I_{n-2}, del cual I_{n-1} es su primer ideal de eliminación, para ver que puntos $a_n \in \mathrm{V}(I_{n-1})$ podemos extender a

una solución parcial con una coordenada más $(a_{n-1}, a_n) \in \mathrm{V}(I_{n-2})$. El teorema de extensión solo nos dice la existencia o no de a_{n-1}, pero una vez que hayamos visto que existe, podemos calcularla de la siguiente manera: los generadores de I_{n-2} son polinomios en las variables x_n y x_{n-1}, por tanto igualamos $x_n = a_n$ y resolvemos las ecuaciones, que solo dependen de x_{n-1} y las soluciones comunes a todos los generadores de I_{n-2} son las coordenadas a_{n-1}. Y haciendo este proceso reiteradamente llegaremos a tener los puntos $(a_1, \ldots, a_n) \in \mathrm{V}(I)$ que serán las soluciones completas de nuestro sistema original. De esta forma en cada paso simplemente vamos a tener que resolver un cierto número de ecuaciones en una variable.
También puede ocurrir que por ejemplo $I_{n-1} = \langle 0 \rangle$, esto quiere decir que la variable x_n se convierte en un parámetro y las soluciones del sistema dependerán de él. Este es el caso en el que el sistema tiene infinitas soluciones.
También podríamos haberlo hecho por otro camino, empezando otra vez en el sistema original podríamos haber considerado $f, g \in \mathbb{C}[y][x]$ y escribir:

$$\begin{aligned} f(x) &= xy - 1 = 0, \\ g(x) &= x^3 + (y-1)x - 1 = 0. \end{aligned}$$

Si calculamos $\mathrm{Syl}(f, g, x)$ tenemos la siguiente matriz 4×4,

$$\mathrm{Syl}(xy - 1, x^3 + xy - x - 1, x) = \begin{pmatrix} -1 & 0 & 0 & -1 \\ y & -1 & 0 & y-1 \\ 0 & y & -1 & 0 \\ 0 & 0 & y & 1 \end{pmatrix},$$

entonces $\mathrm{Res}(f, g, x) = y^2 - 1$. Ahora, por la proposición 2.2.3 tenemos que $f(x) = g(x) = 0$ si y solo si $\mathrm{Res}(f, g, x) = 0$, despejando tenemos las soluciones parciales $y = \pm 1$ y podríamos aplicar el teorema de extensión igual que antes para llegar a las soluciones $(1, 1)$ y $(-1, -1)$.
La ventaja de usar resultantes es que nos permiten ahorrarnos el cálculo de base de Gröbner, que en muchos casos es una tarea muy pesada computacionalmente hablando. Vamos a dar dos métodos diferentes usando resultantes, los cuales los he encontrado en [3, Ch.3,Sec.5].

5.1.2. La u-resultante

Suponemos que tenemos n polinomios (no necesariamente homogéneos) $f_1, \ldots, f_n \in \mathbb{K}[x_1, \ldots, x_n]$ y queremos encontrar las soluciones no triviales del sistema

$$f_1 = \cdots = f_n = 0.$$

Como solo hemos definido la resultante para polinomios homogéneos, vamos a homogeneizar los polinomios f_i. Con la misma notación que en el capítulo 3 definimos los polinomios

$$F_i(1, x_1, \ldots, x_n) = f_i(x_1, \ldots, x_n),$$
$$\overline{F}_i(x_1, \ldots, x_n) = F_i(0, x_1, \ldots, x_n),$$

donde los polinomios F_i son polinomios homogéneos en $\mathbb{K}[x_0, \ldots, x_n]$. Vamos a añadir un polinomio más para poder tener $n+1$ polinomios en $n+1$ variables y así poder calcular su resultante. Añadiremos el polinomio

$$F_0 = u_0 x_0 + \ldots + u_n x_n,$$

donde $u_0, \ldots, u_n$ son variables independientes. Como ahora tenemos el mismo número de ecuaciones y de variables tiene sentido considerar su resultante

$$\mathrm{Res}_{1,d_1,\ldots,d_n}(F_0, \ldots, F_n),$$

que como depende de los coeficientes de $F_0, \ldots, F_n$ es un polinomio en las variables $u_0, \ldots, u_n$ al que llamaremos la u-resultante.
Vamos a ver una proposición que nos permitirá, en ciertos casos, resolver el sistema $f_1 = \cdots = f_n = 0$ usando la u-resultante.

Proposición 5.1.1. *Suponemos que el sistema $\overline{F}_1 = \ldots = \overline{F}_n = 0$ solo tiene la solución trivial. Con la notación de arriba, existe una constante $C \neq 0$ tal que*

$$\mathrm{Res}_{1,d_1,\ldots,d_n}(F_0, \ldots, F_n) = C \prod_{p \in \mathrm{V}(f_1,\ldots,f_n)} f_0(p)^{m(p)},$$

donde $m(p)$ es la multiplicidad de p.

Demostración. Sea $C = \mathrm{Res}_{d_1,\ldots,d_n}(\overline{F}_1, \ldots, \overline{F}_n)$, que es distinto de 0 por hipótesis. Gracias al teorema 3.2.4 tenemos que

$$\mathrm{Res}_{1,d_1,\ldots,d_n}(F_0, \ldots, F_n) = C\det(m_{f_0}),$$

donde m_{f_0} es la aplicación multiplicación por f_0 definida en el anillo cociente $\mathbb{K}[x_1, \ldots, x_n]/\langle f_1, \ldots, f_n\rangle$, por el teorema de Bézout es un $\mathbb{K}$-espacio vectorial de dimensión $d_1 \cdots d_n$ y gracias al teorema [3, Ch.2,Sec.4,Th.4.5] se tiene que los autovalores de la matriz m_{f_0} son los valores $f_0(p)$ para $p \in \mathrm{V}(f_1, \ldots, f_n)$. Como $u_0, \ldots, u_n$ son variables independientes y de la expresión de f_0 como

$$f_0 = u_0 + u_1 x_1 + \ldots + u_n x_n,$$

se tiene que si $p_1, p_2 \in \mathrm{V}(f_1, \ldots, f_n)$ son diferentes, entonces $f_0(p_1) \neq f_0(p_2)$. Entonces tenemos que

$$\det(m_{f_0}) = \prod_{p \in \mathrm{V}(f_1,\ldots,f_n)} f_0(p)^{m(p)},$$

lo que prueba la proposición. □

Veamos con un ejemplo como se aplica esta proposición.

Ejemplo 5.1.2. Consideramos el sistema

$$\begin{aligned} f_1 &= x^2 + y^2 - 10 = 0, \\ f_2 &= x^2 + xy + 2y^2 - 16 = 0. \end{aligned}$$

Primero tenemos que homogeneizar los polinomios f_i en otros F_i con la condición de que al especializar una de las variables de F_i en 1, obtengamos f_i, por tanto definimos

$$\begin{aligned} F_1(t, x, y) &= x^2 + y^2 - 10t^2, \\ F_2(t, x, y) &= x^2 + xy + 2y^2 - 16t^2. \end{aligned}$$

Ahora si hacemos $t = 0$ nos damos cuenta que $\overline{F}_1 = \overline{F}_2 = 0$ solo tiene la solución trivial ya que restando ambas ecuaciones tenemos la condición $y(x+y) = 0$, y de aquí se deduce que solo tiene la solución $(0, 0)$. Ahora añadimos el polinomio $F_0 = u_0t + u_1x + u_2y$ y tenemos que calcular $\mathrm{Res}(F_0, F_1, F_2)$. En el ejemplo 3.3.9 ya vimos como se podía calcular $\mathrm{Res}_{1,2,2}$, por tanto especializando los valores de los coeficientes y calculando los determinantes en ese ejemplo se tiene que

$$\begin{aligned} \mathrm{Res}(F_0, F_1, F_2) = \pm(&2u_0^4 + 16u_1^4 + 36u_2^4 - 80u_1^3u_2 + 120u_1u_2^3 \\ &- 18u_0^2u_2^2 + 52u_1^2u_2^2 - 4u_0^2u_1u_2), \end{aligned}$$

y factorizando tenemos

$$\begin{aligned} \mathrm{Res}(F_0, F_1, F_2) = &(u_0 + u_1 - 3u_2)(u_0 - u_1 + 3u_2)(u_0 + 2\sqrt{2}u_1 + \sqrt{2}u_2) \\ &(u_0 - 2\sqrt{2}u_1 - \sqrt{2}u_2). \end{aligned}$$

Ahora si tenemos que un punto $p = (a_1, \ldots, a_n) \in \mathrm{V}(f_1, \ldots, f_n)$ y nos damos cuenta que

$$f_0(p) = u_0 + a_1u_1 + \ldots + a_nu_n,$$

la proposición nos dice que al factorizar $\mathrm{Res}(F_0, \ldots, F_n)$, las soluciones del sistema son justo los coeficientes que acompañan a $u_1, \ldots, u_n$ en dicha factorización, luego las soluciones de nuestro sistema son:

$$(1, -3), (-1, 3), (2\sqrt{2}, \sqrt{2}), (-2\sqrt{2}, -\sqrt{2}).$$

Además vemos que son todas las soluciones ya que por el Teorema de Bézout el sistema tiene 4 soluciones.

El problema de este método es que factorizar un polinomio no es una tarea sencilla computacionalmente hablando, para poder mejorar en este sentido se puede hacer lo siguiente: podemos especializar alguno de los coeficientes de $f_0 = u_0 + u_1x_1 + \ldots + u_nx_n$, por ejemplo haciendo $u_0 = \ldots = u_{n-1} = 0$, $u_n = -1$, la fórmula de la proposición se transforma en

$$\mathrm{Res}_{1,d_1,\ldots,d_n}(u_0x_0 - x_n, F_1, \ldots, F_n) = C \prod_{i=1}^{d_1 \ldots d_n} (u_0 - a_{in}) \tag{5.1}$$

donde a_{in} son las coordenadas n-ésimas de $p_i = (a_{i1}, \ldots, a_{in}) \in \mathrm{V}(f_1, \ldots, f_n)$. Esta resultante es un polinomio en u_0 la cuál es mucho mas fácil de factorizar, y haciendo esto para diferentes especializaciones de las variables u_i iremos obtiendo las coordenadas de las soluciones del sistema, el problema es que este método nos da las coordenadas pero no como se relacionan entre ellas, entonces un estudio a posteriori es necesario.

5.1.3. Esconder variables

Supongamos que tenemos un sistema

$$f_1 = \cdots = f_n = 0,$$

donde los polinomios $f_i \in \mathbb{K}[x_1, \ldots, x_n]$ tienen grado d_i. Si consideramos la variable x_n como coeficiente, es decir, consideramos los polinomios $f_i \in \mathbb{K}[x_n][x_1, \ldots, x_{n-1}]$, a los que denotaremos por f_i', tenemos n polinomios en $n-1$ variables, definimos unos nuevos polinomios $F_i \in \mathbb{K}[x_n][x_0, x_1, \ldots, x_{n-1}]$, homogéneos de grado d_i y que cumplan que

$$F_i(1, x_1, \ldots, x_{n-1}) = f_i'(x_1, \ldots, x_{n-1}).$$

Por tanto tenemos n polinomios homogéneos en n variables y tiene sentido calcular su resultante que denotaremos por

$$\mathrm{Res}^{x_n}_{d_1,\ldots,d_n}(F_1, \ldots, F_n),$$

para recalcar cuál es la variable que hemos escondido en los coeficientes.

Proposición 5.1.3. $\mathrm{Res}^{x_n}_{d_1,\ldots,d_n}(F_1,\ldots,F_n)$ *es un polinomio en* x_n *cuyas raíces son las coordenadas n-ésimas de las soluciones del sistema* $f_1 = \cdots = f_n = 0$.

Demostración. Como la resultante depende de los coeficientes de los F_i, es claro que es un polinomio en x_n. Para probar la segunda parte, definimos los polinomios $G_i \in \mathbb{K}[x_0,\ldots,x_n]$ homogéneos de grado d_i tal que

$$G_i(1,x_1,\ldots,x_n) = f_i(x_1,\ldots,x_n),$$

y ya sabemos que las raíces del polinomio

$$\mathrm{Res}_{1,d_1,\ldots,d_n}(u_0x_0 - x_n, G_1,\ldots,G_n) \in \mathbb{K}[u_0],$$

nos dan las coordenadas n-ésimas de la solución. Por tanto vamos a escribir

$$\mathrm{Res}^{x_n=u_0}_{d_1,\ldots,d_n}(F_1,\ldots,F_n),$$

esto significa que como hemos considerado x_n como coeficiente, es decir, como una constante, la cambiamos de nombre y la llamamos u_0 y hacemos esto porque vamos a probar que

$$\mathrm{Res}^{x_n=u_0}_{d_1,\ldots,d_n}(F_1,\ldots,F_n) = \pm\mathrm{Res}_{1,d_1,\ldots,d_n}(u_0x_0 - x_n, G_1,\ldots,G_n),$$

y con ese cambio tenemos que son ambos polinomios en u_0. Vamos a probar la igualdad aplicando el teorema 3.2.4 por separado a las dos resultantes. Empezando con $\mathrm{Res}(u_0x_0 - x_n, G_1,\ldots,G_n)$ tenemos que

$$\mathrm{Res}(u_0x_0 - x_n, G_1,\ldots,G_n) = \mathrm{Res}(-x_n, \overline{G}_1,\ldots,\overline{G}_{n-1})^{d_n}\det(m_{f_n}),$$

donde $-x_n, \overline{G}_1,\ldots,\overline{G}_{n-1}$ se ha obtenido a partir de $u_0x_0 - x_n, G_1,\ldots,G_{n-1}$ haciendo $x_0 = 0$, y m_{f_n} es la aplicación multiplicación por f_n en el anillo

$$A = \mathbb{K}[u_0][x_1,\ldots,x_n]/\langle u_0 - x_n, f_1,\ldots,f_{n-1}\rangle.$$

Ahora aplicando el teorema 3.2.4 a $\mathrm{Res}^{x_n=u_0}_{d_1,\ldots,d_n}(F_1,\ldots,F_n)$ tenemos que

$$\mathrm{Res}^{x_n=u_0}_{d_1,\ldots,d_n}(F_1,\ldots,F_n) = \mathrm{Res}(\overline{F}_1,\ldots,\overline{F}_{n-1})^{d_n}\det(m_{f'_n}),$$

donde $\overline{F}_i$ se ha obtenido de F_i haciendo $x_0 = 0$, y $m_{f'_n}$ es la aplicación multiplicación por f'_n en el anillo

$$A' = \mathbb{K}[u_0][x_1,\ldots,x_{n-1}]/\langle f'_1,\ldots,f'_{n-1}\rangle.$$

Ahora vamos a probar que $\overline{\overline{G}_i} = \overline{F_i}$, es decir vamos a probar que

$$G_i(0,x_1,\ldots,x_{n-1},0) = F_i(0,x_1,\ldots,x_{n-1}),$$

y entonces por el corolario 3.2.6 tendríamos que

$$\mathrm{Res}(-x_n, \overline{G}_1, \ldots, \overline{G}_{n-1}) = \pm \mathrm{Res}(\overline{F}_1, \ldots, \overline{F}_{n-1}).$$

Para probar dicha igualdad, tomamos un término de G_i, será de la forma

$$cx_0^{a_0} \cdots x_n^{a_n}, \text{ con } a_0 + \ldots + a_n = d_i.$$

Ahora como $G_i(1, x_1, \ldots, x_n) = f_i(x_1, \ldots, x_n)$, tenemos que el correspondiente término de f_i es

$$c1^{a_0} \cdot x_1^{a_1} \cdots x_n^{a_n},$$

y como el polinomio $f_i'(x_1, \ldots, x_{n-1})$ se obtiene de f_i haciendo x_n una constante, como dijimos al inicio de la demostración la cambiamos el nombre a u_0 y por tanto el correspondiente termino en f_i' es

$$cu_0^{a_n} \cdot x_1^{a_1} \cdots x_{n-1}^{a_{n-1}}.$$

Como $F_i(x_0, x_1, \ldots, x_{n-1})$ es la homogeneización de f_i', es decir, teníamos que $F_i(1, x_1, \ldots, x_{n-1}) = f_i'(x_1, \ldots, x_{n-1})$, el correspondiente término de F_i es

$$cu_0^{a_n} \cdot x_0^{a_0+a_n} x_1^{a_1} \cdots x_{n-1}^{a_{n-1}} = c \cdot x_0^{a_0} \cdots x_{n-1}^{a_{n-1}} (u_0 x_0)^{a_n},$$

ya que $cu_0^{a_n}$ es una constante y F_i tiene que ser homogéneo de grado d_i. De esta expresión se deduce que la homogeneización de f_i' es $G_i(x_0, \ldots, x_{n-1}, u_0 x_0)$ y haciendo $x_0 = 0$ se tiene la igualdad que queríamos probar. Ahora la aplicación

$$\mathbb{K}[u_0][x_1, \ldots, x_n] \to \mathbb{K}[u_0][x_1, \ldots, x_{n-1}]$$

definida por $x_n \to u_0$, lleva f_i en f_i' e induce un isomorfismo entre los anillos A y A'. Además, las aplicaciones m_{f_n} y $m_{f_n'}$ dan un diagrama conmutativo

$$\begin{array}{ccc} A & \cong & A' \\ {\scriptstyle m_{f_n}}\downarrow & & \downarrow{\scriptstyle m_{f_n'}} \\ A & \cong & A' \end{array}$$

De aquí se deduce que $\det(m_{f_n}) = \det(m_{f_n'})$ y termina de probar la proposición. □

Este proceso se puede hacer para cualquier variable, no tiene que ser necesariamente x_n y entonces iremos consiguiendo las coordenadas n-ésimas de las soluciones. Al igual que ocurría con la última parte de la u-resultante, este método nos permite conocer cuáles son las coordenadas de las soluciones pero no como se relacionan entre ellas, entonces un estudio posterior es

necesario. En cambio, este método es más efectivo que el de la u-resultante, en el ejemplo 5.1.2 para calcular $\mathrm{Res}_{1,2,2}(F_0, F_1, F_2)$ tenemos que calcular un determinante 10×10 y luego factorizarlo, en cambio usando este método solo necesitamos calcular $\mathrm{Res}^y_{2,2}(F_1, F_2)$, que es un determinante de tamaño 4×4 y resolver ecuaciones en una variable. Más concretamente, si escondemos la variable y en los coeficientes y consideramos los polinomios

$$\begin{aligned} F_1(t, x) &= x^2 + t^2(y^2 - 10), \\ F_2(t, x) &= x^2 + yxt + t^2(2y^2 - 16), \end{aligned}$$

vimos en el capítulo 3 que su resultante coincide con el determinante de la matriz de Sylvester y por tanto,

$$\mathrm{Res}^y_{2,2}(F_1, F_2) = \begin{vmatrix} y^2 - 10 & 0 & 2y^2 - 16 & 0 \\ 0 & y^2 - 10 & y & 2y^2 - 16 \\ 1 & 0 & 1 & y \\ 0 & 1 & 0 & 1 \end{vmatrix}.$$

Si ahora escondemos la variable x en los coeficientes y considermos los polinomios

$$\begin{aligned} G_1(t, y) &= y^2 + t^2(x^2 - 10), \\ G_2(t, y) &= 2y^2 + xty + t^2(x^2 - 16), \end{aligned}$$

su resultante también coincide con el determinante de la matriz de Sylvester y por tanto,

$$\mathrm{Res}^x_{2,2}(G_1, G_2) = \begin{vmatrix} x^2 - 10 & 0 & x^2 - 16 & 0 \\ 0 & x^2 - 10 & x & x^2 - 16 \\ 1 & 0 & 2 & x \\ 0 & 1 & 0 & 2 \end{vmatrix}.$$

Con el siguiente programa de Singular,

```
> ring A=0,(x,y),lp;
> poly f1=x2+y2-10;
> poly f2=x2+xy+2y2-16;
> poly ry=resultant(f1,f2,x); ry;
2y4-22y2+36
> laguerre(ry,10,2);
[1]:
   -3
[2]:
   -1.414213562
```

```
[3]:
   1.414213562
[4]:
   3
> poly rx=resultant(f1,f2,y); rx;
2x4-18x2+16
> laguerre(rx,10,2);
[1]:
   -2.828427125
[2]:
   -1
[3]:
   1
[4]:
   2.828427125
```

Se llega a que

$$\mathrm{Res}^{y}_{2,2}(F_1, F_2) = 2y^4 - 22y^2 + 36,$$
$$\mathrm{Res}^{x}_{2,2}(G_1, G_2) = 2x^4 - 18x^2 + 16.$$

Resolviendo esas dos ecuaciones por separado, para ello se puede utilizar el comando `laguerre` en Singular, se llega a que los posibles valores de las soluciones para la segunda coordenada son $-3, 3, \sqrt{2}$ y $-\sqrt{2}$. Haciendo lo mismo se tiene que los posibles valores para la primera coordenada son $1, -1, 2\sqrt{2}$ y $-2\sqrt{2}$. Observamos que obtenemos las mismas soluciones que usando el método de la u-resultante, el único problema es que aquí no sabemos como se relacionan las coordenadas entre ellas.

5.2. Implicitación

Una variedad V se puede describir usando ecuaciones paramétricas, esto es, dada la variedad $V \subseteq K^n$ existen funciones $f_1, \ldots, f_n$ definidas en K^m tales que:

$$V = \{(x_1, \ldots, x_n) \in K^n \ : \ x_i = f_i(t_1, \ldots, t_m) \text{ para algún } (t_1, \ldots, t_m) \in K^m\},$$

normalmente se dice que V viene parametizada por las ecuaciones $f_1, \ldots, f_n$ o que V viene dada por las ecuaciones

$$\begin{aligned} x_1 &= f_1(t_1, \ldots, t_m), \\ &\vdots \\ x_n &= f_n(t_1, \ldots, t_m). \end{aligned} \tag{5.2}$$

Las ecuaciones paramétricas nos permiten viajar a través de la variedad. Pero tiene varios problemas, el primero de ellos es que si nos dan un punto $(x_1, \ldots, x_n) \in K^n$ no sabemos de forma sencilla como determinar si dicho punto pertenece o no a la variedad, además en algunas ocasiones la parametrización no abarca toda la variedad, es decir, hay algún punto de V para el cual no existe $(t_1, \ldots, t_m) \in K^m$ verificando (5.2). Por ejemplo, si parametrizamos la circunferencia unidad en $\mathbb{R}^2$ como

$$\begin{aligned} x &= \frac{1-t^2}{1+t^2}, \\ y &= \frac{2t}{1+t^2}, \end{aligned}$$

entonces el punto $(-1, 0)$ pertenece a la circunferencia unidad pero $\frac{1-t^2}{1+t^2} \neq -1$ para cualquier valor de t.
La implicitación intenta resolver estos problemas, nuestro objetivo es encontrar funciones $g_1, \ldots, g_s$ definidas sobre K^n que nos permitan transformar las ecuaciones (5.2) en otras que verifiquen que un punto $(x_1, \ldots, x_n)$ pertenece a la variedad si

$$\begin{aligned} g_1(x_1, \ldots, x_n) &= 0, \\ &\vdots \\ g_s(x_1, \ldots, x_n) &= 0. \end{aligned}$$

Con esto ya estaría resuelto el problema de determinar cuando un punto pertenece a la variedad. Pero como hemos comentado, hay puntos de la variedad que no están representados por las ecuaciones (5.2), entonces el problema que realmente estamos interesados en resolver es encontrar ecuaciones que definan la mínima variedad V que contenga a los puntos dados por la parametrización (5.2). Vamos a abordar dos casos, el primero es cuando las funciones f_i son polinomios, y el segundo es cuando son funciones racionales.

5.2.1. Implicitación polinómica

Empezamos con una parametrización polinómica de una variedad V dada por

$$\begin{aligned} x_1 &= f_1(t_1, \ldots, t_m), \\ &\vdots \\ x_n &= f_n(t_1, \ldots, t_m), \end{aligned} \tag{5.3}$$

es decir, cada $f_i \in K[t_1, \ldots, t_m]$. Podemos pensar geométricamente y definir la aplicación

$$F \colon K^m \longrightarrow K^n \tag{5.4}$$

dada por

$$F(t_1, \ldots, t_m) = (f_1(t_1, \ldots, t_m), \ldots, f_n(t_1, \ldots, t_m)).$$

Entonces $F(K^m)$ es el subconjunto de K^n parametrizado por las ecuaciones (5.3), que no tiene por qué ser una variedad afín como comentamos antes, pero vamos a intentar encontrar las ecuaciones que definan la mínima variedad afín que contenga a $F(K^m)$, y para ello vamos a usar la teoría de eliminación vista en el capítulo 4.
Las ecuaciones (5.3) definen la siguiente variedad en K^{m+n}

$$V = \mathrm{V}(x_1 - f_1, \ldots, x_n - f_n), \tag{5.5}$$

cuyos puntos son de la forma

$$(t_1, \ldots, t_m, f_1(t_1, \ldots, t_m), \ldots, f_n(t_1, \ldots, t_m)),$$

es decir, V es el grafo de la aplicación F.
Vamos a dar dos lemas que necesitaremos más adelante.

Lema 5.2.1. *Sea $I = \langle h_1, \ldots, h_s \rangle$ un ideal en $K[x_1, \ldots, x_n]$ y sea I_l su l-ésimo ideal de eliminación. Si denotamos por π_l a la proyección sobre las $l+1$ últimas coordenadas y $V = \mathrm{V}(I)$, tenemos que:*

$$\pi_l(V) \subseteq \mathrm{V}(I_l).$$

Demostración. Dado $f \in I_l$ y $(a_1, \ldots, a_n) \in V$ queremos ver que f se anula en dicho punto. Como en particular $f \in I$ se tiene que $f(a_1, \ldots, a_n) = 0$ y como f solo tiene las variables $x_{l+1}, \ldots, x_n$ podemos escribir

$$0 = f(a_1, \ldots, a_n) = f(0, \ldots, 0, a_{l+1}, \ldots, a_n) = f(\pi_l(a_1, \ldots, a_n)).$$

Esto implica que f se anula sobre $\pi_l(V)$. Hemos visto que todo punto de $\pi_l(V)$, anula a todas las $f \in I_l$, luego el punto pertenece a $\mathrm{V}(I_l)$ como queremos demostrar. □

Lema 5.2.2. *Sea K un cuerpo con infinitos elementos y sea $f \in K[x_1, \ldots, x_n]$. Entonces f es el polinomio nulo si y solo si la aplicación*

$$\begin{array}{rcc} f\colon K^n & \longrightarrow & K \\ (x_1, \ldots, x_n) & \longmapsto & f(x_1, \ldots, x_n) \end{array}$$

es la aplicación idénticamente nula.

Demostración. En una dirección el resultado es obvio ya que es claro que el polinomio nulo da la aplicación nula. Para probar el recíproco, necesitamos ver que si $f(a_1, \ldots, a_n) = 0$ para todo $(a_1, \ldots, a_n) \in K^n$, entonces f es el polinomio nulo. Para ver esto razonamos por inducción sobre n, el número de variables. Si $n = 1$, un polinomio en $K[x]$ de grado m tiene exactamente m raíces (quizás estén en un cuerpo algebraicamente cerrado que contenga a K). Pero como estamos suponiendo que $f(a) = 0$ para todo $a \in K$ esto significa que f tiene infinitas raíces, luego necesariamente f es el polinomio nulo. Suponemos el resultado cierto para $n-1$ y sea $f \in K[x_1, \ldots, x_n]$ un polinomio que se anule en todos los puntos de K^n, podemos escribir f de la siguiente manera

$$f = \sum_{i=0}^{N} g_i(x_1, \ldots, x_{n-1}) x_n^i,$$

donde $g_i \in \mathbb{K}[x_1, \ldots, x_{n-1}]$. Si probamos que cada g_i es el polinomio nulo en $K[x_1, \ldots, x_{n-1}]$ habremos terminado. Fijado un punto $(a_1, \ldots, a_{n-1}) \in K^{n-1}$ por hipótesis se tiene que para cualquier $a_n \in K$, $f(a_1, \ldots, a_{n-1}, a_n) = 0$. Esto implica que el polinomio $f(a_1, \ldots, a_{n-1}, x_n)$ es el polinomio nulo gracias al paso $n = 1$ de la inducción, y usando la expresión de arriba se tiene que $g_i(a_1, \ldots, a_{n-1}) = 0$ para todo i. Como el punto $(a_1, \ldots, a_{n-1})$ es arbitrario se tiene que para cada i, g_i es la función nula y usando nuestra hipótesis de inducción, g_i es el polinomio nulo para todo i. □

Ahora vamos a enunciar y demostrar un teorema que nos permitirá encontrar la mínima variedad afín que contenga a $F(K^m)$.

Teorema 5.2.3 (Implicitación polinómica)**.** *Sea $I = \langle x_1 - f_1, \ldots, x_n - f_n \rangle$ un ideal de $K[t_1, \ldots, t_m, x_1, \ldots, x_n]$ y sea I_m su m-ésimo ideal de eliminación. Si K es un cuerpo infinito y F la función definida en (5.4), entonces $\mathrm{V}(I_m)$ es la mínima variedad afín en K^n que contiene a $F(K^m)$.*

Demostración. Si consideramos π_m la aplicación proyección tal que a cada punto $(t_1, \ldots, t_m, x_1, \ldots, x_n) \in K^{m+n}$ lo envía al punto $(x_1, \ldots, x_n) \in K^n$ y si V es como en (5.5) se tiene que

$$F(K^m) = \pi_m(V) \subseteq \mathrm{V}(I_m),$$

donde la contención viene dada gracias al lema 5.2.1. Por tanto $\mathrm{V}(I_m)$ es una variedad que contiene a $F(K^m)$, veamos que de hecho es la mínima.
Sea $Z = \mathrm{V}(h_1, \ldots, h_s) \subseteq K^n$ otra variedad afín tal que $F(K^m) \subseteq Z$, queremos probar que $\mathrm{V}(I_m) \subseteq Z$. Si vemos que cada $h_i \in I_m$ tendríamos lo que queremos ya que para cada punto $a \in \mathrm{V}(I_m)$ como $h_i \in I_m$ se tiene que

$h_i(a) = 0$ para todo $i = 1, \ldots, s$, luego se tiene que $a \in Z$ lo que implica que $\mathrm{V}(I_m) \subseteq Z$. Por tanto solo queda probar que dado $i = 1, \ldots, s$, $h_i \in I_m$. Denotamos $h = h_i$ por comodidad, tenemos que $h \in K[x_1, \ldots, x_n]$, pero si queremos lo podemos ver como un polinomio en $K[t_1, \ldots, t_m, x_1 \ldots, x_n]$. Fijamos el orden lexicográfico con $x_1 > \ldots > x_n > t_1 > \ldots > t_m$ y dividiendo h entre $\{x_1 - f_1, \ldots, x_n - f_n\}$ llegamos a una expresión de la forma:

$$h(x_1, \ldots, x_n) = q_1(x_1 - f_1) + \ldots + q_n(x_n - f_n) + r(t_1, \ldots, t_m), \qquad (5.6)$$

gracias a que $\mathrm{in}(x_j - f_j) = x_j$ con el orden que hemos elegido. Dado un punto $a = (a_1, \ldots, a_m) \in K^m$, si sustituimos en la ecuación cada t_i por a_i y cada x_i por $f_i(a)$ tenemos que

$$0 = h(f_1(a), \ldots, f_n(a)) = 0 + \ldots + 0 + r(a).$$

Entonces como $r(a) = 0$ para todo $a \in K^m$, gracias al lema 5.2.2 se tiene que $r(t_1, \ldots, t_m)$ es el polinomio nulo. Entonces sustituyendo en 5.6 llegamos a que

$$h(x_1, \ldots, x_n) = q_1(x_1 - f_1) + \ldots + q_n(x_n - f_n) \in I \cap K[x_1, \ldots, x_n] = I_m,$$

como queríamos probar. □

Por tanto ya sabemos como encontrar la mínima variedad afín que contiene al conjunto definido de manera paramétrica, pero ahora nos podemos preguntar si la variedad que hemos encontrado realmente es la que se estaba dando con las ecuaciones (5.3) o hemos añadido algún punto. Aquí es donde entra en juego el teorema de extensión, con la notación del teorema tenemos que comprobar si podemos extender todos los puntos $(x_1, \ldots, x_n) \in \mathrm{V}(I_m)$ a puntos $(t_1, \ldots, t_m, x_1, \ldots, x_n) \in \mathrm{V}(I)$, ya que si hubiese algún punto de $\mathrm{V}(I_m)$ que no pudiesemos extender significaría que no existen $(t_1, \ldots, t_m)$ verificando (5.3). Veamos con un ejemplo cómo se aplica esto.

Ejemplo 5.2.4. Consideramos la cúspide en $\mathbb{R}^2$,que viene parametrizada por las ecuaciones

$$x = t^2,$$
$$y = t^3,$$

con $t \in \mathbb{R}$. Definimos el ideal $I = \langle x - t^2, y - t^3 \rangle$ y si consideramos el orden lexicográfico con $t > y > x$ ya vimos en el ejemplo 4.1.3 que $I_1 = \langle x^3 - y^2 \rangle$. Por tanto,

$$C = \{(x, y) \in \mathbb{R}^2 : x^3 - y^2 = 0\}$$

es la mínima variedad afín que contiene al conjunto definido con esa parametrización. Si aplicamos el teorema de extensión vemos que $c_1 = c_2 = -1$

y por tanto vamos a poder extender todos los puntos $(x, y) \in C$ a puntos (t, x, y) que verifican las ecuaciones paramétricas. El teorema de extensión nos dice la existencia de ese t en algún cuerpo algebraicamente cerrado que cointenga a $\mathbb{R}$, pero en este caso es obvio que si un punto (x, y) está en C verifica las ecuaciones paramétricas para cualquier valor de t real. Entonces se tiene que C es exactamente la cúspide que parametrizaban las ecuaciones originales.

5.2.2. Implicitación racional

En este caso empezamos con una parametrización racional de una variedad V dada por

$$\begin{aligned} x_1 &= \frac{f_1(t_1, \ldots, t_m)}{g_1(t_1, \ldots, t_m)}, \\ &\vdots \\ x_n &= \frac{f_n(t_1, \ldots, t_m)}{g_n(t_1, \ldots, t_m)}, \end{aligned} \tag{5.7}$$

donde $f_i, g_j \in K[t_1, \ldots, t_m]$ para todos $1 \leq i, j \leq n$. De la misma forma que hicimos para la implicitación queremos construir una aplicación como en 5.4, pero ahora tenemos que tener más cudiado ya que se pueden anular los denominadores. Sea $W = \mathrm{V}(g_1 g_2 \cdots g_n)$ el subconjunto de K^m donde se anulan los denominadores, entonces ya podemos definir la aplicación

$$F \colon K^m \setminus W \longrightarrow K^n \tag{5.8}$$

dada por

$$F(t_1, \ldots, t_m) = \left(\frac{f_1(t_1, \ldots, t_m)}{g_1(t_1, \ldots, t_m)}, \ldots, \frac{f_n(t_1, \ldots, t_m)}{g_n(t_1, \ldots, t_m)} \right).$$

Como en el apartado anterior, necesitamos encontrar la mínima variedad afín que contenga a $F(K^m \setminus W)$. Para ello vamos a considerar una nueva variable y, denotamos $g = g_1 g_2 \cdots g_n$ y construimos el ideal

$$J = \langle g_1 x_1 - f_1, \ldots, g_n x_n - f_n, 1 - gy \rangle \subseteq K[y, t_1, \ldots, t_m, x_1, \ldots, x_n]. \tag{5.9}$$

Hemos introducido la ecuación $1 - gy$ para que los denominadores $g_1, \ldots, g_n$ no se anulen en $\mathrm{V}(J)$. Además tenemos que los puntos de $\mathrm{V}(J)$ son de la forma:

$$\left(\frac{1}{g(t_1, \ldots, t_m)}, t_1, \ldots, t_m, \frac{f_1(t_1, \ldots, t_m)}{g_1(t_1, \ldots, t_m)}, \ldots, \frac{f_n(t_1, \ldots, t_m)}{g_n(t_1, \ldots, t_m)} \right).$$

De la misma manera que hicimos para la implicitación polinomica tenemos que:

$$F(K^m \setminus W) = \pi_{1+m}(\mathrm{V}(J)) \subseteq \mathrm{V}(J_{1+m}),$$

donde J_{1+m} es el $1+m$-ésimo ideal de eliminación de J y la contención es gracias al lema 5.2.1. El siguiente teorema es el que nos permitirá resolver el problema de implicitación.

Teorema 5.2.5 (Implicitación racional)**.** *Sea K un cuerpo infinito y F como en (5.8). Si J es el ideal definido en (5.9), tenemos que $\mathrm{V}(J_{1+m})$ es la mínima variedad en K^n que contiene a $F(K^m \setminus W)$, donde J_{1+m} es el $(1+m)$-ésimo ideal de eliminación de J.*

La demostración es idénticamente a la del teorema 5.2.3 salvo que en este caso se divide $g^N h$ entre $\{g_1 x_1 - f_1, \ldots, g_n x_n - f_n\}$ donde N es un número lo suficiente grande para que $g^N h = P$, donde $P \in K[t_1, \ldots, t_m, x_1, \ldots, x_n]$. La demostración completa se puede encontrar en [2, Ch.3,Sec.3,Th.2].
Como en el apartado anterior, una vez hayamos determinado la mínima variedad que contiene a la parametrización hay que comprobar mediante el teorema de extensión si es realmente la variedad que estábamos buscando o es otra mayor.

Ejemplo 5.2.6. Si consideramos la circunferencia unidad en $\mathbb{R}^2$ parametrizada por

$$x = \frac{1-t^2}{1+t^2},$$
$$y = \frac{2t}{1+t^2}.$$

Construimos $g = (1+t^2)^2$ y el ideal

$$J = \langle (1+t^2)x + t^2 - 1, (1+t^2)y - 2t, 1 - (1+t^2)^2 z \rangle \subseteq \mathbb{R}[z,t,x,y].$$

Si elegimos el orden lexicográfico con $z > t > x > y$, y con Singular calculamos una base de Gröbner, tenemos que $G = \{g_1, g_2, g_3, g_4\}$ es una base de Gröbner de J, donde

$$g_1 = x^2 + y^2 - 1,$$
$$g_2 = ty + x - 1,$$
$$g_3 = tx + t - y,$$
$$g_4 = 4z - x^2 - 2x - 1,$$

y por tanto $J_2 = \langle x^2 + y^2 - 1 \rangle$. Entonces la mínima variedad que contiene al conjunto definido con esa parametrización es

$$S = \{(x,y) \in \mathbb{R}^2 : x^2 + y^2 = 1\}.$$

Además, si aplicamos el teorema de extensión sobre el ideal $J_1 = \langle g_1, g_2, g_3 \rangle$, del cual J_2 es su primer ideal de eliminación, vemos que $c_1 = 0$, $c_2 = y$ y $c_3 = x+1$, luego el teorema de extensión nos dice que la única solución que no podemos extender es $(-1, 0)$, como ya habíamos visto al inicio del capítulo. Por tanto S no es exactamente el conjunto parametrizado por dichas ecuaciones, le hemos añadido el punto $(-1, 0)$, pero esto es justo el problema que queríamos resolver con la implicitación, ya que S sí que es la circunferencia unidad.

5.2.3. Implicitación y resultantes

En esta sección vamos a dar un caso en el que se puede resolver el problema de implicitación usando resultantes. La ventaja de aplicar este método, cuando se pueda, es que no hace falta hacer cálculos de base de Gröbner. Supongamos que tenemos una variedad V parametrizada por:

$$\begin{aligned} x_0 &= f_0(t_1, \ldots, t_n), \\ &\vdots \\ x_n &= f_n(t_1, \ldots, t_n), \end{aligned} \tag{5.10}$$

donde los f_i son polinomios en $\mathbb{K}[t_1, \ldots, t_n]$ (no tienen por qué ser homogéneos) de grados $d_0, \ldots, d_n$ respectivamente.
Para usar los métodos vistos en el capítulo 3 necesitamos tener polinomios homogéneos, vamos a usar una variable auxiliar u con la que vamos a homogeneizar los polinomios, podemos escribir f_i de la siguiente manera:

$$f_i(t_1, \ldots, t_n) = \tilde{f}_{d_i}(t_1, \ldots, t_n) + \tilde{f}_{d_i-1}(t_1, \ldots, t_n) + \ldots + \tilde{f}_0(t_1, \ldots, t_n),$$

donde cada término $\tilde{f}_{d_i-j}$ es homogéneo de grado $d_i - j$ en las variables $(t_1, \ldots, t_n)$. Homogeneizando f_i obtenemos el siguiente polinomio:

$$F_i(t_1, \ldots, t_n, u) = \tilde{f}_{d_i}(t_1, \ldots, t_n) + \tilde{f}_{d_i-1}(t_1, \ldots, t_n)u + \ldots + \tilde{f}_0(t_1, \ldots, t_n)u^{d_i},$$

el cual es homogéneo de grado d_i en las variables $(t_1, \ldots, t_n, u)$. Luego las ecuaciones (5.10) se transforman en:

$$\begin{aligned} x_0 u^{d_0} &= F_0(t_1, \ldots, t_n, u), \\ &\vdots \\ x_n u^{d_n} &= F_n(t_1, \ldots, t_n, u), \end{aligned} \tag{5.11}$$

donde también se ha homogeneizado el lado izquierdo. Notar que si especializamos $u = 1$ tenemos el sistema de ecuaciones (5.10). Ahora podemos enunciar el siguiente resultado que nos permitirá resolver el problema de implicitación.

Proposición 5.2.7. *Con la notación de arriba, suponemos que el sistema*

$$\begin{aligned} \tilde{f}_{d_0}(t_1,\ldots,t_n) &= 0, \\ &\vdots \\ \tilde{f}_{d_n}(t_1,\ldots,t_n) &= 0, \end{aligned} \tag{5.12}$$

solo tiene la solución trivial. Entonces, dado $(x_0,\ldots,x_n) \in \mathbb{K}^n$*, el sistema (5.10) tiene una solución* $(t_1,\ldots,t_n) \in \mathbb{K}^n$ *si y solo si*

$$\mathrm{Res}_{d_0,\ldots,d_n}(F_0 - x_0u^{d_0},\ldots,F_n - x_nu^{d_n}) = 0.$$

Demostración. Por el teorema 3.1.1 se tiene que la resultante se anula si y solo si el sistema (5.11) tiene una solución no trivial $(t_1,\ldots,t_n,u)$. Si $u \neq 0$, entonces $(t_1/u,\ldots,t_n/u)$ es una solución del sistema 5.10. Si $u = 0$, entonces cualquier $(t_1,\ldots,t_n)$ distinto de 0 es una solución no trivial del sistema (5.12), lo que entra en contradicción con nuestra hipótesis. Recíprocamente, si tenemos una solución $(t_1,\ldots,t_n)$ del sistema (5.11), entonces $(t_1,\ldots,t_n,1)$ es una solución no trivial de (5.11). □

Por tanto, lo que nos dice esta proposición es que el polinomio

$$R(x_0,\ldots,x_n) = \mathrm{Res}_{d_0,\ldots,d_n}(F_0 - x_0u^{d_0},\ldots,F_n - x_nu^{d_n}),$$

se anula precisamente en la imagen de la parametrización.

Ejemplo 5.2.8. Volvemos a considerar la cúspide del ejemplo 5.2.4, que venía parametrizada por

$$\begin{aligned} x &= t^2, \\ y &= t^3. \end{aligned}$$

Es claro que $t^2 = t^3 = 0$ solo tiene la solución trivial, y por tanto, el problema se reduce a calcular $\mathrm{Res}(t^2 - xu^2, t^3 - yu^3)$ respecto de las variables t y u, que como ya vimos en el capítulo 3 es el determinante de la matriz de Sylvester,

$$\mathrm{Res}(t^2 - xu^2, t^3 - yu^3) = \begin{vmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ -x & 0 & 1 & 0 & 0 \\ 0 & -x & 0 & -y & 0 \\ 0 & 0 & -x & 0 & -y \end{vmatrix}.$$

Se tiene que $\mathrm{Res}(t^2 - xu^2, t^3 - yu^3) = y^2 - x^3$, que es el mismo resultado que obtuvimos mediante el cálculo de bases de Gröbner. Este es otro ejemplo donde se ve la potencia de las resultantes en algunas ocasiones, ya que no hemos tenido que hacer ningún cálculo de base de Gröbner para llegar al mismo resultado.

5.3. Puntos singulares

En este apartado vamos a intentar determinar cuando una curva en el plano K^2 tiene puntos singulares, esto es, puntos de la curva en los que no vamos a saber determinar su tangente ya sea porque la curva tenga un pico (véase la curva definida por $y^2 = x^3$) o porque la curva se corte a si misma (por ejemplo la curva $y^2 = x^2(1+x)$). Este problema lo podemos resolver con técnicas de cálculo, pero en este apartado vamos a intentar dar una versión algebráica. Suponemos que la curva viene dada por la ecuación $f(x, y) = 0$, donde $f \in K[x, y]$, es decir, un punto (a, b) está en la curva si y solo si $(a, b) \in \mathrm{V}(f)$. Dado un punto (a, b) en el plano, si L es una recta que pasa por dicho punto L viene dada por las ecuaciones:

$$\begin{aligned} x &= a + ct, \\ y &= b + dt, \end{aligned} \tag{5.13}$$

donde $t \in K$ es un parámetro y $c, d \in K$ constantes que no se anulan ambas a la vez (cada par (c, d) da una recta L diferente que pasa por (a, b)). Ahora nos podemos preguntar cómo interactúa esta recta con nuestra curva, es decir, ¿corta o no a la curva?¿es una recta tangente?. Dado un punto $(x, y) \in K^2$, se tiene que pertenece a la curva si $f(x, y) = 0$, por tanto para resolver la pregunta de si nuestra recta corta o no a la curva podemos construir la función

$$g(t) = f(a + ct, b + dt),$$

entonces tendremos que si existe $t_1 \in K$ con $g(t_1) = 0$, el punto

$$\begin{aligned} x &= a + ct_1, \\ y &= b + dt_1, \end{aligned}$$

verifica que $(x, y) \in L$ y además está en la curva. Si ahora suponemos que si que existe este punto t_1, nos podemos preguntar si la recta corta a la curva o es tangente a ella en este punto. Vamos a dar la siguiente definición que necesitaremos para resolver esta pregunta.

Definición 5.3.1. Sea m un entero positivo, $(a, b) \in \mathrm{V}(f)$ un punto de la curva y L una recta que pasa por (a, b). Diremos que L toca a la curva $\mathrm{V}(f)$ con multiplicidad m en (a, b) si L se parametriza como en (5.13) y $t = 0$ es una raíz de multiplicidad m del polinomio $g(t) = f(a + ct, b + dt)$.

Esta definición no depende de la parametrización de L, ya que si suponemos que

$$\begin{aligned} x &= a + \tilde{c}t, \\ y &= b + \tilde{d}t, \end{aligned}$$

es otra parametrización de L, los vectores (c,d) y $(\tilde{c},\tilde{d})$ son paralelos luego existe $\alpha \in K$ con $(c,d) = \alpha(\tilde{c},\tilde{d})$, entonces como estamos mirando la multiplicidad en $t=0$, es la misma. Ahora vamos a dar una proposición que nos va a permitir resolver el problema.

Proposición 5.3.2. *Sea $f \in K[x,y]$ y $(a,b) \in \mathrm{V}(f)$ un punto de la curva que define f. Entonces,*

1. *Si $\nabla f(a,b) \neq (0,0)$, existe una única recta L que pasa por (a,b) la cual toca a la curva con multiplicidad al menos 2.*

2. *Si $\nabla f(a,b) = (0,0)$, todas las rectas que pasen por (a,b) tocan a la curva con multiplicidad al menos 2.*

Donde $\nabla f(a,b) = (\frac{\partial f}{\partial x}, \frac{\partial f}{\partial y})(a,b)$.

Demostración. Sea L una recta que pasa por el punto $(a,b) \in \mathrm{V}(f)$, la parametrizamos como en (5.13). Como (a,b) pertenece a la curva se tiene que $t=0$ es una raíz del polinomio $g(t)$ introducido en la definición anterior. Usando la regla de la cadena tenemos que

$$g'(t) = \frac{\partial f}{\partial x}(a+ct, b+dt)\cdot c + \frac{\partial f}{\partial y}(a+ct,b+dt)\cdot d,$$

y entonces

$$g'(0) = \frac{\partial f}{\partial x}(a,b)\cdot c + \frac{\partial f}{\partial y}(a,b)\cdot d.$$

Si $\nabla f(a,b) = (0,0)$, entonces $g'(0) = 0$ para cualquier valor de (c,d), es decir, para cualquier recta L que pase por (a,b). Como $g'(0)=0$, se tiene que $t=0$ es una raíz de multiplicidad al menos 2 de g, por tanto hemos probado el apartado (2). Si ahora suponemos que $\nabla f(a,b) \neq (0,0)$, para ver si la raíz $t=0$ tiene mutiplicidad al menos 2 necesitamos saber si $g'(0)=0$, es decir, resolver la ecuación

$$\frac{\partial f}{\partial x}(a,b)\cdot c + \frac{\partial f}{\partial y}(a,b)\cdot d = 0.$$

Es una ecuación lineal en las variables c,d cuyos coeficientes son no nulos, por tanto la solución es un espacio de dimensión 1, es decir, existe $(c_0,d_0) \neq (0,0)$ tal que (c,d) es solución si existe $\alpha \in K$ con $\alpha(c_0,d_0) = (c,d)$. Pero como vimos antes, todos los (c,d)'s que verifiquen eso parametrizan la misma recta L. Por tanto hemos probado que existe una única recta L que pasa por (a,b) que tiene multiplicidad al menos 2, lo que prueba (1). □

Usando esta proposición ya podemos definir la recta tangente y los puntos singulares de forma algebráica.

Definición 5.3.3. Sea $f \in K[x,y]$ y $(a,b) \in \mathrm{V}(f)$ un punto de la curva que define f. Entonces decimos que,

1. Si $\nabla f(a,b) \neq (0,0)$, entonces la recta tangente de $\mathrm{V}(f)$ en (a,b) es la única recta que pasa por (a,b) que toca a $\mathrm{V}(f)$ con multiplicidad al menos 2. Diremos que (a,b) es un punto no singular de $\mathrm{V}(f)$.

2. Si $\nabla f(a,b) = (0,0)$ diremos que (a,b) es un punto singular de $\mathrm{V}(f)$.

Entonces dada una curva $\mathrm{V}(f)$, para calcular sus puntos singulares simplemente tenemos que calcular los puntos (a,b) que verifican que $f(a,b) = 0$ para que estén en la curva, y además cumplan que

$$\frac{\partial f}{\partial x}(a,b) = \frac{\partial f}{\partial y}(a,b) = 0.$$

Por tanto nuestro problema se reduce a resolver un sistema, el cual podemos abordar con la teoría vista en el capítulo 4 y los métodos introducidos en la sección 5.1.

Ejemplo 5.3.4. Supongamos que tenemos una curva dada por la ecuación

$$\begin{aligned} 0 = f(x,y) = &-1156 + 688x^2 - 191x^4 + 16x^6 + 544y + 30x^2y - 40x^4y \\ &+ 225y^2 - 96x^2y^2 + 16x^4y^2 - 136y^3 - 32x^2y^3 + 16y^4, \end{aligned}$$

las derivadas parciales de f son

$$\begin{aligned} \frac{\partial f}{\partial x} &= 1376x - 764x^3 + 80x^5 + 60xy - 160x^3y - 192xy^2 + 64x^3y^2 - 64xy^3, \\ \frac{\partial f}{\partial y} &= 544 + 30x^2 - 40x^4 + 450y - 192x^2y + 32x^4y - 408y^2 - 96x^2y^2 + 64y^3. \end{aligned}$$

Tenemos que resolver el sistema

$$\begin{aligned} \frac{\partial f}{\partial x} &= 0, \\ \frac{\partial f}{\partial y} &= 0, \end{aligned}$$

y ver que soluciones (x,y) cumplen que $f(x,y) = 0$. Viendo $\frac{\partial f}{\partial x}$ y $\frac{\partial f}{\partial y}$ como polinomios en $\mathbb{C}[y][x]$, tenemos que $\mathrm{Syl}(\frac{\partial f}{\partial x}, \frac{\partial f}{\partial y}, x)$ es una matriz de tamaño 9×9. Si calculamos la resultante y la igualamas a 0, para ello se puede usar el siguiente código en Singular:

```
> ring A=0,(x,y),lp;
> poly f=1376x-764x3+80x5+60xy-160x3y-192xy2+64x3y2-64xy3;
> poly g=544+30x2-40x4+450y-192x2y+32x4y-408y2-96x2y2+64y3;
> poly r=resultant(f,g,x);
> laguerre(r,10,2);
[1]:
   -0.7063714621
[2]:
   -0.488331088
[3]:
   -0.4883191936
[4]:
   2.831371462
[5]:
   4.25
[6]:
   (-2.10776375+I*0.896174296)
[7]:
   (-2.10776375-I*0.896174296)
[8]:
   (-2.107753366+I*0.8961756896)
[9]:
   (-2.107753366-I*0.8961756896)
[10]:
   (0.4020757406+I*2.052241118)
[11]:
   (0.4020757406-I*2.052241118)
[12]:
   (0.4020816438+I*2.052257039)
[13]:
   (0.4020816438-I*2.052257039)
[14]:
   (1.65988983+I*0.1048785636)
[15]:
   (1.65988983-I*0.1048785636)
[16]:
   (1.659895221-I*0.1049116334)
[17]:
   (1.659895221+I*0.1049116334)
```

Tenemos 17 posibles valores de y. Como c_1, c_2 son constantes usando el teo-

rema de extensión las 17 soluciones parciales se pueden extender a soluciones completas. Luego habría que verificar que soluciones reales (x, y) verifican que están en la curva, es decir, que cumplan $f(x, y) = 0$, y esos serían los puntos singulares. Debido a que el comando `laguerre` aproxima las soluciones tenemos unos pequeños errores, realmente las últimas cuatro soluciones son la misma solución real con multiciplidad 4 y se tiene que los puntos singulares de la curva son

$$(0, 4.25) \text{ y } (\pm 0.9185, 1.6598),$$

donde el primero es solución exacta y el segundo es una aproximación. Aunque parezca muy laborioso, computacionalmente hablando es inmediato obtener las soluciones. En sistemas de este tipo es donde se ve la potencia de la teoría que hemos visto en las secciones previas.

Esto se puede generalizar y estudiar puntos singulares de variedades afines arbitrarias, consultar [2, Ch.9] para más información.

5.4. Envolventes

En esta sección vamos a hacer una pequeña introducción de cómo calcular la envolvente a una familia de curvas en $\mathbb{R}^2$. Antes de dar la definición de envolvente necesitamos definir lo que es una familia de curvas.

Definición 5.4.1. Sea $F \in \mathbb{R}[x, y, t]$ un polinomio donde x e y son las variables y t es un parámetro. Fijado $t \in \mathbb{R}$ consideramos la variedad $\mathrm{V}(F_t) \subseteq \mathbb{R}^2$, que no es más que la variedad definida por $F(x, y, t) = 0$ con t fijo. Definimos la familia de curvas determinada por F como la familia de variedades $\mathrm{V}(F_t)$ cuando t varía en $\mathbb{R}$.

Por ejemlo si consideramos $F(x, y, t) = x^2 + (y - t)^2 - 1$ y fijamos t, tenemos que $\mathrm{V}(F_t)$ es una circunfenrencia de radio 1 y con centro en el punto $(0, t)$. Por tanto la familia de curvas determinada por F es una especie de cilindro centrado en el eje de ordenadas y de radio 1.
Vamos a definir la envolvente a una familia de curvas como una curva que para todo punto de ella, exista una curva de la familia a la que sea tangente en ese punto. Es decir, dada la familia de curvas $\mathrm{V}(F_t)$, buscamos una curva C que cumpla que dado $(x, y) \in C$, existe $t \in \mathbb{R}$ tal que C sea tangente a $\mathrm{V}(F_t)$ en dicho punto. Supongamos por un momento que ya sabemos cual es la curva C y la tenemos parametrizada por

$$\begin{aligned} x &= f(t), \\ y &= g(t). \end{aligned}$$

Además como suponemos que todo punto de C es tangente a la familia, en particular significa que para cada t fijo, existe $t_1 \in \mathbb{R}$ tal que el punto $(f(t_1), g(t_1)) \in \mathrm{V}(F_t)$. No se pierde generalidad si suponemos que la parametrización de C cumple que para cada $t \in \mathbb{R}$, $(f(t), g(t)) \in \mathrm{V}(F_t)$, es decir, se cumple que

$$F(f(t), g(t), t) = 0, \ \forall t \in \mathbb{R}. \tag{5.14}$$

Además, sabemos que dado $t \in \mathbb{R}$, el vector tangente a C es $(f'(t), g'(t))$ y en la sección anterior, en particular en la demostración de la proposición 5.3.2, vimos que la recta tangente a $\mathrm{V}(F_t)$ tiene dirección perpendicular a $(\frac{\partial F}{\partial x}, \frac{\partial F}{\partial y})$. Juntando estas dos cosas, como C es tangente a $\mathrm{V}(F_t)$, se tiene que $(f'(t), g'(t))$ tiene que ser perpendicular a $(\frac{\partial F}{\partial x}, \frac{\partial F}{\partial y})$, es decir que

$$\frac{\partial F}{\partial x}(f(t), g(t), t) \cdot f'(t) + \frac{\partial F}{\partial y}(f(t), g(t), t) \cdot g'(t) = 0.$$

Usando esta relación y derivando en (5.14) tenemos que

$$\frac{\partial F}{\partial t}(f(t), g(t), t) = 0. \tag{5.15}$$

Ahora sabiendo esto, es natural definir la envolvente de la siguiente manera.

Definición 5.4.2. Dada una familia de curvas $\mathrm{V}(F_t)$ en $\mathbb{R}^2$, la envolvente consiste en todos los puntos $(x, y) \in \mathbb{R}^2$ tal que

$$\begin{aligned} F(x, y, t) &= 0, \\ \frac{\partial F}{\partial t}(x, y, t) &= 0, \end{aligned} \tag{5.16}$$

para algún $t \in \mathbb{R}$.

Como pasaba para los puntos singulares hemos reducido nuestro problema de calcular envolventes a resolver sistemas de ecuaciones, y nuestro objetivo es eliminar t de dichas ecuaciones. Entonces podemos usar las técnicas vistas en el capítulo 4 y la sección 5.1. Pero hay que tener cuidado ya que para aplicar el teorema de extensión necesitamos trabajar en $\mathbb{C}$, por tanto nuestras soluciones puede que sean complejas y entonces hay que hacer un cribado para quedarnos con las soluciones reales, en el caso de que existan. Veamos un ejemplo.

Ejemplo 5.4.3. Consideramos $F(x, y, t) = (x - t)^2 - y + t$, entonces la envolvente viene dada por las ecuaciones

$$\begin{aligned} F &= (x - t)^2 - y + t = 0, \\ \frac{\partial F}{\partial t} &= -2(x - t) + 1 = 0. \end{aligned}$$

Si se elige el orden lexicográfico con $t > x > y$ y se calcula una base de Gröbner de $I = \langle F, \frac{\partial F}{\partial t} \rangle$, se tiene que viene dada por los polinomios

$$g_1 = 4x - 4y - 1,$$
$$g_2 = 2t - 2x + 1.$$

Por tanto el primer ideal de eliminación es el generado por g_1 y se tiene que los puntos $(x, y) \in \mathrm{V}(g_1)$ son de la forma $x = y + \frac{1}{4}$. Debido a que el término que acompaña a t en g_2 es una constante, el teorema de extensión nos dice que podemos extender todas las soluciones y despejando en g_2 se tiene que

$$t = \frac{2x - 1}{2},$$

que es real siempre que x sea real. Además, de esta expresión también se deduce que dado (x, y) solamente existe un t que cumpla las ecuaciones, por tanto la extensión es única y nos dice que cada punto de la envolvente $x = y + \frac{1}{4}$ es tangente solamente a una curva de la familia.

Bibliografía

[1] E. Cattani and A. Dickenstein. Introduction to residues and resultants. In: A. Dickenstein, I. Z. Emiris (Eds.): *Solving Polynomial Equations: Foundations, Algorithms, and Applications*. Algorithms and Computation in Mathematics **14**, Springer-Verlag, pp. 1–61, 2005.

[2] D. Cox, J. Little and D. O'Shea. *Ideals, varieties, and algorithms*. Undergraduate Texts in Mathematics. Springer-Verlag, 4th edition, 2005.

[3] D. Cox, J. Little and D. O'Shea. *Using algebraic geometry*, volume 185 of Graduate Texts in Mathematics. Springer-Verlag, 2th edition, 2005.

[4] D'Andrea and A. Dickenstein. *Explicit formulas for the multivariate resultant*, In: Effective Methods in Algebraic Geometry (Bath, 2000), J. Pure Appl. Algebra **164** (2001), 59–86.

[5] W. Decker, G.-M. Greuel, G. Pfister and H. Schönemann, SINGULAR 4-2-0 — A computer algebra system for polynomial computations. http://www.singular.uni-kl.de (2020).

[6] I. Gelfand, M. Kapranov and A. Zelevinsky. *Discriminants, Resultants and Multidimensional Determinants*, Birkhäuser, Boston, 1994.

[7] J.-P. Jouanolou. *Le formalisme du résultant*, Adv. Math. **90** (1991), 117–263.

[8] J.-P. Jouanolou. *Formes d'inertie et résultant: un formulaire*, Adv. Math. **126** (1997), 119–250.

[9] F. Macaulay. *The Algebraic Theory of Modular Systems*, Cambridge U. Press, Cambridge, 1916. Reprint with new introduction, Cambridge U. Press, Cambridge, 1994.

[10] B. Sturmfels. *Solving systems of polynomial equations*, CBMS Regional Conference Series in Mathematics **97**, Amer. Math. Soc. and CBMS, 2002.

[11] B. Sturmfels and A. Zelevinsky. *Multigraded resultants of Sylvester type*, J. Algebra **163** (1994), 115–127.

[12] J. Weyman and A. Zelevinski. *Determinantal formulas for multigraded resultants*, J. Algebraic Geom. **3** (1994), 569–597.