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

Fórmulas en raíces para las subresultantes

Tesis presentada para optar al título de Doctor de la Universidad de Buenos Aires en el área Ciencias Matemáticas

Marcelo Alejandro Valdettaro

Director de tesis: Teresa Krick
Consejero de estudios: Pablo Solernó

Buenos Aires, 2017

Agradecimientos

Agradezco principalmente a mi directora Teresa Krick. Porque con gran generosidad me recibió después de mi alejamiento del trabajo de investigación y facilitó mucho que yo retomara los estudios al aceptar dirigir esta tesis. Con su pasión y laboriosidad hizo que este trabajo resultara de la mejor manera posible. Me hizo aprender mucho y fue un placer trabajar con ella.

Gracias a Pablo Solernó por aceptar ser mi consejero de estudios y ayudarme mucho tanto en aspectos académicos como administrativos. Siempre es un gusto trabajar o conversar con él.

Gracias a Leandro Cagliero, Lalo González Vega y Juan Sabia. Por su generosidad al aceptar ser jurados de esta tesis. Por mostrar interés y por sus comentarios y observaciones enriquecedoras.

Gracias a Carlos D'Andrea, Agnes Szanto y Alin Bostan. Por compartir con Teresa y conmigo gran parte del trabajo presentado en esta tesis y porque aprendí mucho de los tres, además del placer que fue conocerlos y trabajar con ellos.

Gracias a Marie-Françoise Roy y Aviva Szpirglas, que se interesaron en nuestros resultados y compartieron con nosotros su enfoque, que nos ayudó a tener otra perspectiva.

Gracias a Ariel Pacetti, que también me recibió muy amablemente cuando quise retomar los estudios y me ayudó con sus consejos.

Gracias a Nicolás Sirolli. Por sus habituales y desinteresadas ayudas técnicas, y su amistad.

Gracias a Santiago Laplagne. Por ayudarme generosamente con el programa Maple.

Gracias a Eugenia Rodríguez. Por ser casi una segunda consejera y darme siempre una mano con las cuestiones administrativas.

Y más allá de aquellos que tuvieron que ver concretamente con esta tesis, agradezco a toda la gente valiosa que conocí en la facultad en todos estos años. Hice muchos amigos y compartí con ellos cosas muy gratas que hicieron muy placentera toda la carrera.

Y por supuesto, gracias a mi familia. Porque sí. Porque siempre me dieron todo, porque siempre están y porque son lo más importante.

Fórmulas en raíces para las subresultantes

Resumen

Los objetos centrales de esta tesis son los polinomios subresultantes de dos polinomios en una variable, que son, *en el caso de polinomios con raíces simples*, múltiplos escalares de lo que hoy se llama sumas de Sylvester de sus conjuntos de raíces, como demostró J.J. Sylvester en 1853. En primer término presentamos aquí una generalización de las sumas de Sylvester para multiconjuntos de manera que sigue valiendo la relación con los polinomios subresultantes. En el caso en que los multiconjuntos tienen suficientes elementos distintos, esta generalización es particularmente elegante ya que tiene el mismo aspecto que las sumas de Sylvester. Cuando no hay suficientes elementos distintos, nuestra generalización es más compleja ya que necesita introducir polinomios de Schur. Sin embargo cabe mencionar que ejemplos previos parecen indicar que no se va a poder encontrar ninguna generalización sencilla de las sumas de Sylvester para multiconjuntos arbitrarios. Nuestro enfoque introduce un *Lema de intercambio* que permite interpolar ciertos polinomios simétricos en distintos conjuntos de nodos. Obtenemos además más aplicaciones naturales de este lema, no sólo a otras propiedades de subresultantes sino también a construcciones relacionadas con matrices de Bézout y bases de Gröbner. Finalmente estudiamos completamente el caso particular de dos polinomios con una sola raíz múltiple cada uno y logramos probar que las subresultantes son, en ese caso, un múltiplo escalar de cierto polinomio de Jacobi, módulo un cambio de variables afín. Esto permite obtener, vía la ecuación diferencial satisfecha por los polinomios de Jacobi, una cota optimal de complejidad para determinar los coeficientes de una subresultante en la base monomial. De este modo logramos mejorar, para esta clase de polinomios, las cotas de complejidad que existen para el cálculo de una subresultante de polinomios arbitrarios.

Palabras clave: Subresultantes, Sumas de Sylvester, Lema de intercambio, Polinomios de Schur, Polinomios de Jacobi, Complejidad.

Formulas in roots for the subresultants

Abstract

The main objects of this thesis are the subresultant polynomials of two univariate polynomials, which are, *for simple-root polynomials*, scalar multiples of what is known today as Sylvester sums, as shown by J.J. Sylvester in 1853. First we present a generalization of Sylvester sums for multisets so that the relationship with subresultants still holds. In the case that the multisets have enough different elements, this generalization is particularly elegant since it has the same shape as Sylvester sums. When there are not enough different elements, our generalization is more complex since it needs to introduce Schur polynomials. However it should be mentioned that previous examples seem to indicate that it will not be possible to obtain any simple generalization of Sylvester sums for arbitrary multisets. Our approach introduces an *Exchange lemma* which allows to interpolate some symmetric polynomials in different sets of nodes. We also obtain other natural applications of this lemma, not only concerning further properties of subresultants but also other constructions related to Bézout matrices and Gröbner bases. Finally we fully study the particular case of two polynomials with only one multiple root each and prove that their subresultants are scalar multiples of a certain Jacobi polynomial, modulo an affine change of variables. This allows to obtain, using the differential equation satisfied by Jacobi polynomials, an optimal complexity bound for determining the coefficients of a subresultant in the monomial basis. In this way we improve, for this family of polynomials, the existing complexity bounds for computing a subresultant of arbitrary polynomials.

Keywords: Subresultants, Sylvester's sums, Exchange lemma, Schur polynomials, Jacobi polynomials, Complexity.

Índice general

Introducción

Los objetos principales de esta tesis son los *polinomios subresultantes*, que llamaremos aquí *subresultantes*, de dos polinomios univariados con coeficientes en un dominio íntegro. Éstos son una generalización de la conocida *resultante* de dos polinomios, y fueron introducidas de manera implícita por C.G. Jacobi [Jac1836] y posteriormente de manera explícita por J.J. Sylvester [Syl1839, Syl1840] bajo el nombre "prime derivative of the d-degree"(la terminología "subresultante"parece haber sido introducida por George Collins a fines de los 60). Ver también [GaLu2003] para una descripción histórica del tema.

Como es bien sabido, la resultante de dos polinomios es una expresión en los coeficientes de éstos que determina cuándo son coprimos. Las subresultantes son polinomios que determinan no solamente quién es exactamente el máximo común divisor de los dos polinomios, sino que además describen toda la sucesión de restos en el algoritmo de Euclides extendido, al dividir un polinomio por el otro. Estas construcciones tienen una gran importancia algorítmica y proporcionan, por ejemplo, un método eficiente para el cálculo del máximo común divisor y de la sucesión de restos.

Precisamente, sea R un dominio íntegro con cuerpo de fracciones K y sean $f = \sum_{i=0}^{m} a_i x^i$, $g = \sum_{i=0}^{n} b_i x^i \in R[x]$ dos polinomios de grados exactamente m y n, es decir, tales que $a_m \neq 0$ y $b_n \neq 0$. Dado $0 \leq d < \text{mín}\{m, n\}$ o $d = \text{mín}\{m, n\}$ si $m \neq n$, la subresultante de orden d entre f y g está definida como

$$\text{Sres}_d(f,g)(x) := \det \begin{array}{|cccccc|l} \multicolumn{6}{c}{\overbrace{\phantom{a_m \cdots a_{d+1}\ x^{n-d-1}f(x)}}^{m+n-2d}} & \\ a_m & \cdots & & \cdots & a_{d+1-(n-d-1)} & x^{n-d-1}f(x) & \\ & \ddots & & & \vdots & \vdots & n-d \\ & & a_m & \cdots & a_{d+1} & f(x) & \\ \hline b_n & \cdots & & \cdots & b_{d+1-(m-d-1)} & x^{m-d-1}g(x) & \\ & \ddots & & & \vdots & \vdots & m-d \\ & & b_n & \cdots & b_{d+1} & g(x) & \end{array} \in R[x].$$

Aunque no resulta inmediato de la definición, $\text{Sres}_d(f,g)(x)$ es un polinomio de grado menor o igual que d, cuando es no nulo. El caso $d = 0$ se corresponde con la resultante $\text{Res}(f,g) \in R$ y satisface $\text{Res}(f,g) = 0$ si, y sólo si, f y g tienen un factor no trivial en común en $K[x]$. Generalizando esto, la sucesión de subresultantes

$$\{\text{Sres}_d(f,g)(x) : 0 \leq d < \text{mín}\{m,n\} \text{ o } d = \text{mín}\{m,n\} \text{ si } m \neq n\},$$

nos da un múltiplo no nulo del máximo común divisor de f y g para el mínimo valor de d para el cual $\text{Sres}_d(f,g)(x) \neq 0$, y todas las subresultantes no nulas en esa sucesión se

corresponden con los restos sucesivos en el esquema de Euclides extendido. Esto se conoce hoy como el "Fundamental Theorem of Polynomial Remainder Sequences", el Teorema 1.1.5, demostrado independientemente en [Col1967, Cor.1.2] y [BrTr1971, Fund.Th.] (ver también [GCL1992, Th.7.4]).

Una descripción de la resultante que muestra bien que ésta se anula si, y sólo si, los polinomios tienen una raíz en común en una clausura algebraica $\overline{K}$ de K, es la fórmula de Poisson ([Poi1802]) que para $f = a_m(x-\alpha_1)\cdots(x-\alpha_m),\ g = b_n(x-\beta_1)\cdots(x-\beta_n) \in \overline{K}[x]$ con $a_m \neq 0 \neq b_n$, dice que

$$\operatorname{Res}(f,g) = a_m^n b_n^m \prod_{\substack{1\le i\le m\\ 1\le j\le n}} (\alpha_i - \beta_j).$$

Esta fórmula representa una expansión en las raíces de f y g de la resultante y resulta muy útil para entenderla mejor. Por ejemplo, con esta fórmula es fácil ver que si $f = q\cdot g + r$, entonces $\operatorname{Res}(f,g) = \lambda \operatorname{Res}(g,r)$ para algún $\lambda \in K\backslash\{0\}$.

Para las subresultantes existen también tales expansiones en raíces, las *sumas de Sylvester* introducidas también por él en [Syl1840b], pero sólo están definidas cuando los polinomios f y/o g no tienen raíces múltiples: Sean $A,\ B \subset K$ dos conjuntos con cardinales $|A| = m$ y $|B| = n$. Para $0 \le p \le m,\ 0 \le q \le n$, la suma doble de Sylvester $\operatorname{Syl}_{p,q}(A,B)(x)$ está definida por

$$\operatorname{Syl}_{p,q}(A,B)(x) := \sum_{\substack{A'\subset A,\, B'\subset B\\ |A'|=p,\,|B'|=q}} \frac{\mathcal{R}(A',B')\,\mathcal{R}(A\backslash A', B\backslash B')\mathcal{R}(x,A')\,\mathcal{R}(x,B')}{\mathcal{R}(A',A\backslash A')\,\mathcal{R}(B',B\backslash B')} \in K[x],$$

donde $\mathcal{R}(Y,Z) := \prod_{y\in Y, z\in Z} (y-z)$ con la convención $\mathcal{R}(Y,Z) = 1$ si $Y = \emptyset$ o $Z = \emptyset$.

Estos son claramente polinomios de grado menor o igual que $p+q =: d$. En los casos $p = 0$ o $q = 0$, las sumas suelen llamarse sumas simples:

$$\operatorname{Syl}_{d,0}(A,B)(x) = \sum_{\substack{A'\subset A\\ |A'|=d}} \frac{\mathcal{R}(A\backslash A', B)\mathcal{R}(x,A')}{\mathcal{R}(A',A\backslash A')} \ \text{ y } \ \operatorname{Syl}_{0,d}(A,B)(x) = \sum_{\substack{B'\subset B\\ |B'|=d}} \frac{\mathcal{R}(A,B\backslash B')\mathcal{R}(x,B')}{\mathcal{R}(B',B\backslash B')}.$$

Sylvester enunció en [Syl1840b], y luego probó en [Syl1853], que dichas sumas pueden interpretarse como una fórmula de Poisson para las subresultantes ya que para

$$f = \prod_{\alpha\in A}(x-\alpha) \ \text{ y } \ g = \prod_{\beta\in B}(x-\beta),$$

y para $d = p+q$ con $0 \le d < \min\{m,n\}$ o $d = \min\{m,n\}$ si $m \neq n$, se tiene

$$\operatorname{Sres}_d(f,g)(x) = \frac{(-1)^{p(m-d)}}{\binom{d}{p}} \operatorname{Syl}_{p,q}(A,B)(x), \ \text{ en } \mathbb{Z}[A,B][x],$$

y en particular

$$\operatorname{Sres}_d(f,g)(x) = (-1)^{d(m-d)} \operatorname{Syl}_{d,0}(A,B)(x) = \operatorname{Syl}_{0,d}(A,B)(x). \tag{1}$$

Sin embargo estas relaciones tienen una limitación: sólo tienen sentido si los polinomios f y g (o al menos uno de los dos en el caso de las sumas simples) tienen raíces simples, ya que si no, no están definidas, pues aparecen ceros en los denominadores, mientras que las subresultantes están definidas también para polinomios con raíces múltiples.

Cabe mencionar que la motivación de Sylvester para obtener fórmulas en términos de las raíces para las subresultantes no era probablemente la de presentar una "fórmula de Poisson"para las subresultantes, sino que se trataba de entender cómo funciona formalmente el método de Sturm para calcular la cantidad de raíces reales de un polinomio en un intervalo dado. Posteriormente las sumas de Sylvester abrieron la puerta a una mayor flexibilidad para la evaluación de las subresultantes: por ejemplo aparecen varias fórmulas ingeniosas para ello en [ApJo2006], y aparecerán otras en esta tesis. Más aún tales fórmulas también derivaron en interesantes conexiones entre las subresultantes y otros conceptos conocidos y como consecuencia se encontraron nuevas aplicaciones, como por ejemplo la obtención de expresiones cerradas para problemas de interpolación racional, como la interpolación de Cauchy o el problema de interpolación racional osculatoria ([BeLa2000], [DKS2015]). Las fórmulas en raíces pueden también ser útiles para analizar el comportamiento de los coeficientes de las subresultantes sobre cuerpos finitos, lo que contribuiría a la comprensión del funcionamiento del algoritmo de Euclides sobre dichos cuerpos ([MaGa1990]).

En esta tesis nos dedicamos a buscar fórmulas para las subresultantes en términos de las raíces de los polinomios para el caso general, es decir, cuando se admiten raíces múltiples. Este proyecto fue iniciado hace varios años por Carlos D'Andrea, Teresa Krick y Agnes Szanto, que obtuvieron por ejemplo distintas fórmulas para las subresultantes como determinantes que involucran matrices de Vandermonde y Wronskianas generalizadas en las raíces de los polinomios para el caso general ([DKS2013, Th.2.5]). También mostraron una fórmula expandida en raíces muy intrincada para la subresultante de orden 1 en el caso general que ejemplifica que no se puede esperar nada sencillo como respuesta a nuestra pregunta. Para $f = (x-\alpha_1)^{m_1}\cdots(x-\alpha_r)^{m_r}$ y $g = (x-\beta_1)^{n_1}\cdots(x-\beta_s)^{n_s}$ con $\alpha_i \neq \alpha_j$, $\beta_k \neq \beta_\ell$ y para $d = 1$, obtienen en [DKS2013, Th.2.7]:

$$\begin{aligned}\mathrm{Sres}_1(f,g)(x) = \sum_{i=1}^{r}(-1)^{m-m_i}\Big(\prod_{\substack{1\le j\le r\\ j\neq i}} \frac{g(\alpha_j)^{m_j}}{(\alpha_i-\alpha_j)^{m_j}}\Big) g(\alpha_i)^{m_i-1}\Big((x-\alpha_i)\\ \cdot \sum_{\substack{k_1+\cdots+\widehat{k_i}+\cdots\\ \cdots+k_{r+s}=m_i-1}} \prod_{\substack{1\le j\le r\\ j\neq i}} \frac{\binom{m_j-1+k_j}{k_j}}{(\alpha_i-\alpha_j)^{k_j}} \prod_{1\le\ell\le s} \frac{\binom{n_\ell-1+k_{r+\ell}}{k_{r+\ell}}}{(\alpha_i-\beta_\ell)^{k_{r+\ell}}}\\ + \min\{1, m_i-1\} \sum_{\substack{k_1+\cdots+\widehat{k_i}+\cdots\\ \cdots+k_{r+s}=m_i-2}} \prod_{\substack{1\le j\le r\\ j\neq i}} \frac{\binom{m_j-1+k_j}{k_j}}{(\alpha_i-\alpha_j)^{k_j}} \prod_{1\le\ell\le s} \frac{\binom{n_\ell-1+k_{r+\ell}}{k_{r+\ell}}}{(\alpha_i-\beta_\ell)^{k_{r+\ell}}}\Big). \quad (2)\end{aligned}$$

Aquí avanzamos en este proyecto con resultados en dos direcciones distintas. La primera dirección consistió en tratar directamente el caso general y buscar una extensión de la definición de la suma simple $\mathrm{Syl}_{d,0}(A,B)(x)$ para *multiconjuntos*, esto es, admitiendo repeticiones en los elementos de A y de B, que coincide con la definición de suma simple

de Sylvester en el caso en que A y B son conjuntos, y que además satisface la relación (1) con la subresultante de orden d. En el Capítulo 4 se describen los resultados logrados junto con Carlos D'Andrea, Teresa Krick y Agnes Szanto en [DKSV2017]. Primero obtenemos una elegante expresión para valores de d suficientemente grandes (especificados en la Definición 4.1.3) que llamamos *suma de Sylvester múltiple* de los multiconjuntos A y B:

$$\mathrm{SylM}_{d,0}(A,B)(x) := (-1)^{m'(m-d)} \sum_{\substack{A'\subset\overline{A}\\|A'|=d-m'}} \sum_{\substack{B'\subset\overline{B}\\|B'|=m'}} \frac{\mathcal{R}(A\backslash\overline{A},\overline{B}\backslash B')\mathcal{R}(\overline{A}\backslash A',B\backslash B')\mathcal{R}(x,A')\mathcal{R}(x,B')}{\mathcal{R}(A',\overline{A}\backslash A')\mathcal{R}(B',\overline{B}\backslash B')}.$$

Aquí $\overline{A}$ y $\overline{B}$ son los respectivos conjuntos de elementos distintos de A y B, y $m' := m-|\overline{A}|$. Luego obtenemos una expresión más compleja que involucra polinomios de Schur y generaliza esta definición a todos los posibles valores de d (ver Definición 4.1.9), y en el Teorema 4.1.10 mostramos que de este modo obtenemos una fórmula en raíces para la subresultante de dos polinomios arbitrarios. Con el programa Maple ([Map2016]) desarrollamos un código para computar estas fórmulas y damos en ese capítulo un link de acceso al archivo en donde está escrito dicho código. Cabe señalar que ejemplos previos, como el de la iguadad (2), parecen indicar que no se va a poder encontrar ninguna generalización sencilla de las sumas de Sylvester para multiconjuntos arbitrarios. Al respecto presenciamos una charla en la que Aviva Szpirglas presentó un trabajo realizado junto con Marie-Françoise Roy, en el que abordan este mismo problema pero su enfoque es igual de complicado. El Capítulo 4 concluye con la Sección 4.2, propia de esta tesis, que generaliza la noción de suma doble de Sylvester a multiconjuntos.

Para la construcción de las fórmulas del Capítulo 4 utilizamos la *interpolación simétrica multivariada* introducida por W.Y.Chen y J.D.Louck en [ChLo1996], que dio lugar a una identidad tan sorprendente como poderosa que llamamos *lema de intercambio*. El Capítulo 2 está dedicado a presentar este lema en sus distintas versiones y generalizaciones. La siguiente es una versión débil, pero de ella se derivan todas las generalizaciones:

Sea $d \geq 0$ y sean A, B subconjuntos finitos de un cuerpo K, con $|A| \geq d$ y $|B| \geq d$. Sea X un conjunto de variables con $|X| \leq |A| - d$. Entonces

$$\sum_{A'\subset A,|A'|=d} \mathcal{R}(A\backslash A',B)\frac{\mathcal{R}(X,A')}{\mathcal{R}(A\backslash A',A')} = \sum_{B'\subset B,|B'|=d} \mathcal{R}(A,B\backslash B')\frac{\mathcal{R}(X,B')}{\mathcal{R}(B',B\backslash B')}.$$

Este lema no sólo es la herramienta principal que aplicamos para poder definir la suma de Sylvester mútiple, sino que además nos permite reinterpretar algunos resultados conocidos de un modo sencillo y natural. Por ejemplo reobtenemos el Teorema 1.2.6 que describe las sumas de Sylvester en función de expresiones análogas a las subresultantes en la totalidad de los posibles valores de p y q, es decir aún cuando $d = p + q$ no cae en el rango de la definición de la subresultante. Esto está desarrollado en el Capítulo 3 y es, esencialmente, el contenido del trabajo [KSV2017], realizado en colaboración con Teresa Krick y Agnes Szanto.

En el Capítulo 5, original de esta tesis, desarrollamos más aplicaciones del lema de intercambio a otras propiedades de las subresultantes y, más aún, mostramos que dicho lema no sólo tiene alcances dentro del marco de las subresultantes, sino que además se aplica a

otras construcciones que pueden resultar interesantes. En la Sección 5.1 probamos el Teorema 5.1.2 que generaliza el Fundamental Theorem of Polynomial Remainder Sequence, mediante una construcción que llamamos *subresultante multivariada* (Definición 5.1.1) que nos ofrece más información que la subresultante univariada. En la Sección 5.2 mostramos una aplicación a las llamadas matrices de Bézout (ligadas a las subresultantes) logrando algunas reescrituras de sus coeficientes que permiten entender de manera más natural algunas de sus propiedades. La Sección 5.3 presenta una aplicación a la base de Gröbner del ideal de polinomios simétricos que se anulan en $\mathcal{L}_d(B)$, donde para un conjunto B con n elementos y $1 \leq d \leq n$, $\mathcal{L}_d(B)$ es el conjunto de las $(n-d)$-uplas formadas por elementos distintos de B. El Capítulo 5 concluye con la Sección 5.4 donde se muestra cómo puede interpretarse mediante interpolación simétrica la conocida escritura en fracciones simples de un cociente de polinomios, y se generaliza a varias variables.

La segunda dirección que contempla esta tesis es el estudio del caso extremal en que los dos polinomios tienen una sola raíz múltiple cada uno, o sea $f = (x-\alpha)^m$ y $g = (x-\beta)^n$. Este estudio, que se encuentra en el Capítulo 6, tiene un enfoque totalmente diferente al anterior y utiliza una construcción que por ahora sólo aplica en este caso. La Sección 6.2 refleja el contenido del trabajo [BDKSV2017] realizado conjuntamente con Alin Bostan, Carlos D'Andrea, Teresa Krick y Agnes Szanto. Allí obtenemos una expresión para las subresultantes $\mathrm{Sres}_d((x-\alpha)^m, (x-\beta)^n)(x)$ cuando $\alpha \neq \beta$ (ya que si $\alpha = \beta$ son todas obviamente nulas) en la base de Bernstein

$$\{(x-\alpha)^j (x-\beta)^{d-j} : 0 \leq j \leq d\}. \tag{3}$$

Más precisamente, dados $m, n \in \mathbb{N}$ y $0 \leq d < \min\{m, n\}$, y dados α y β, elementos distintos de un cuerpo K, se muestra en los Teoremas 6.2.1 y 6.2.2 que se tiene

$$\mathrm{Sres}_d((x-\alpha)^m, (x-\beta)^n)(x) = (-1)^{\binom{d}{2}} (\alpha-\beta)^{(m-d)(n-d)} \sum_{j=0}^{d} q_j(m,n,d)(x-\alpha)^j (x-\beta)^{d-j}, \tag{4}$$

donde los coeficientes $q_0(m,n,d), \ldots, q_d(m,n,d)$ satisfacen

$$q_0(m,n,d) = (-1)^{\binom{d}{2}} \prod_{i=1}^{d} \frac{(i-1)!\,(m+n-2d+i-2)!}{(m-i-1)!(n-i)!},$$
$$q_j(m,n,d) = \frac{\binom{d}{j}\binom{n-d+j-1}{j}}{\binom{m-1}{j}}\, q_0(m,n,d) \quad \text{para} \quad 1 \leq j \leq d.$$

Una observación interesante es que dado que todos estos coeficientes son números enteros, ya que se obtienen como determinantes de ciertas matrices de Hankel que involucran coeficientes binomiales, se pueden interpretar en cualquier característica, y luego el resultado vale para cuerpos de característica arbitraria, con lo cual se puede en cada caso determinar si estas subresultantes se anulan y qué grado tienen. En particular calculamos también el coeficiente de grado d de $\mathrm{Sres}_d((x-\alpha)^m, (x-\beta)^n)(x)$ y deducimos que si la característica de K es suficientemente grande, cada una de ellas tiene grado exactamente d.

La Sección 6.3, objeto de un trabajo en elaboración con Alin Bostan, Teresa Krick y Agnes Szanto, continúa el desarrollo de este caso estructurado y muestra el sorprendente aunque aparentemente desconocido hecho que en este caso las subresultantes son de hecho múltiplos escalares de los famosos polinomios de Jacobi, módulo un cambio afín de variables.

Recordamos que la clásica familia de polinomios ortogonales conocida como polinomios de Jacobi $P_d^{(k,l)}(x)$ para $d \in \mathbb{N}$ y $k, l \in \mathbb{Z}$ se puede definir por ejemplo por la fórmula de Rodrigues en un cuerpo de característica distinta de 2:

$$P_d^{(k,l)}(x) := \frac{(-1)^d}{2^d\, d!}(1-x)^{-k}(1+x)^{-l}\frac{\partial^d}{\partial x^d}\left[(1-x)^{k+d}(1+x)^{l+d}\right].$$

En el Teorema 6.3.1 se prueba el resultado siguiente:

$$\mathrm{Sres}_d((x-\alpha)^m,(x-\beta)^n)(x) = \lambda\, P_d^{(-n,-m)}\left(\frac{2x-\alpha-\beta}{\beta-\alpha}\right), \tag{5}$$

donde

$$\lambda = (\alpha-\beta)^{(m-d)(n-d)+d}\prod_{i=1}^{d}\frac{i!(m+n-d-i-1)!}{(m-i)!(n-i)!}.$$

Observamos que de hecho esta descripción es exactamente la descripción en términos de la base de Bernstein definida en (3) (y por lo tanto vale para cualquier característica), aunque la demostración aquí es completamente independiente y autocontenida.

La identidad (5) implica, dada la ecuación diferencial satisfecha por los polinomios de Jacobi, que los coeficientes de $\mathrm{Sres}_d((x-\alpha)^m,(x-\beta)^n)(x)$ satisfacen una recurrencia lineal de segundo orden. Este es un hecho crucial que permite deducir que, para un cuerpo de característica 0 o suficientemente grande, se pueden determinar con complejidad aritmética lineal los coeficientes de una de estas subresultantes en la base monomial. Esto siginifica una complejidad óptima para el cálculo de las subresultantes de esta familia estructurada de polinomios, más eficiente que el cálculo de las subresultantes de polinomios arbitrarios (Teorema 6.3.4).

Para llegar a esta conclusión, primero nos dimos cuenta de que la fórmula (4) implicaba la recurrencia lineal satisfecha por los coeficientes de $\mathrm{Sres}_d((x-\alpha)^m,(x-\beta)^n)(x)$ en la base monomial, utilizando una aproximación computacional de "predicción y prueba", con el programa Maple ([Map2016]). Al estudiar la ecuación diferencial asociada a dicha recurrencia, nos dimos cuenta de que tenía una base de soluciones formada por polinomios de Jacobi. Logramos entonces producir una primera prueba de la relación (5), a través de identidades de funciones hipergeométricas, y finalmente pudimos encontrar la prueba autocontenida y elemental que presentamos aquí. En conclusión, estos últimos resultados le deben mucho a una aproximación matemática experimental.

El Capítulo 1 trata de los preliminares generales de toda la tesis: presentamos las subresultantes, las sumas de Sylvester y las relaciones conocidas entre ambos conceptos. En cada uno de los capítulos siguientes se menciona cuáles son los resultados que están comprendidos en trabajos publicados y cuáles son propios de esta tesis.

Capítulo 1

Preliminares: Subresultantes y Sumas de Sylvester

Este capítulo preliminar presenta los objetos centrales a partir de los cuales se desarrolla esta tesis: la teoría clásica de subresultantes y la menos conocida de sumas de Sylvester, mencionando la conexión entre ambas teorías que ya fue enunciada y luego presentada por J.J. Sylvester en diversos trabajos que especificamos en cada sección.

En la Sección 1.1 nos dedicamos a presentar las subresultantes y en la Sección 1.2 las sumas de Sylvester y la relación con las primeras.

1.1. Subresultantes

Las subresultantes constituyen una generalización de la conocida resultante de dos polinomios univariados f y g con coeficientes en un cuerpo K. Es bien sabido que la resultante nos da una condición sobre los coeficientes de f y g para saber cuándo el grado de su máximo común divisor es exactamente 0, i.e. $\mathrm{mcd}(f,g) = 1$. La subresultante es una construcción que va más allá con la información y nos determina cuál es el grado exacto del máximo común divisor $\mathrm{mcd}(f,g)$ y lo calcula, sin aplicar el algoritmo de Euclides. Las resultantes y subresultantes fueron introducidas implícitamente por Jacobi ([Jac1836]) y explícitamente por Sylvester ([Syl1839], [Syl1840]). La resultante es un concepto muy recurrente en varias ramas de la matemática y tiene una importancia algorítmica muy reconocida actualmente. Las subresultantes, que generalizan la resultante, proporcionan, entre otras cosas, un algoritmo eficiente para el cálculo del máximo común divisor de dos polinomios ([Col1967], [BrTr1971]). En esta sección haremos una exposición teórica detallada inspirada en [Kri2017]. También puede verse [GaLu2003] para un desarrollo histórico.

Definición 1.1.1. Sean $f = a_m x^m + \cdots + a_0$ y $g = b_n x^n + \cdots + b_0$ dos polinomios con coeficientes en un cuerpo K (o eventualmente en un dominio íntegro con cuerpo de fracciones K) de grados exactamente m y n respectivamente, es decir, $a_m \neq 0$ y $b_n \neq 0$. El *polinomio subresultante* de orden d de f y g está definido para $0 \leq d < \mathrm{mín}\{m,n\}$ o

$d = \min\{m, n\}$ si $m \neq n$, como

$$\mathrm{Sres}_d(f,g)(x) := \det \begin{array}{|cccccc|c} \multicolumn{6}{c}{\overbrace{\phantom{a_{d+1-(n-d-1)}\ x^{n-d-1}f(x)}}^{m+n-2d}} & \\ a_m & \cdots & & \cdots & a_{d+1-(n-d-1)} & x^{n-d-1}f(x) & \\ & \ddots & & & \vdots & \vdots & n-d \\ & & a_m & \cdots & a_{d+1} & f(x) & \\ \hline b_n & \cdots & & \cdots & b_{d+1-(m-d-1)} & x^{m-d-1}g(x) & \\ & \ddots & & & \vdots & \vdots & m-d \\ & & b_n & \cdots & b_{d+1} & g(x) & \\ \end{array},$$

donde los coeficientes eventualmente no definidos son 0.

A esta matriz que define la subresultante se la llama *matriz de Sylvester*. Veamos algunos ejemplos sencillos.

Ejemplo 1.1.2.

(1) Si $d = 0$, entonces $\mathrm{Sres}_0(f,g)(x) = \mathrm{Res}(f,g)$, la resultante de f y g.

(2) $\mathrm{Sres}_m(f,g)(x) = a_m^{n-m-1} f$ si $m < n$ y $\mathrm{Sres}_n(f,g)(x) = b_n^{m-n-1} g$ si $n < m$.

(3) Sean $f = a_2x^2+a_1x+a_0 = a_2(x-\alpha_1)(x-\alpha_2)$ y $g = b_2x^2+b_1x+b_0 = b_2(x-\beta_1)(x-\beta_2)$. Entonces

$$\mathrm{Sres}_1(f,g)(x) = \det \begin{pmatrix} a_2 & f \\ b_2 & g \end{pmatrix} = a_2g - b_2f = a_2b_2\big((\alpha_1 - \beta_1 + \alpha_2 - \beta_2)x - (\alpha_1\alpha_2 - \beta_1\beta_2)\big).$$

Observemos que $\mathrm{Sres}_1(f,g)(x) = 0 \Leftrightarrow \alpha_1 + \alpha_2 = \beta_1 + \beta_2$ y $\alpha_1\alpha_2 = \beta_1\beta_2$, es decir $(x-\alpha_1)(x-\alpha_2) = (x-\beta_1)(x-\beta_2)$, o sea, f y g tienen las mismas raíces, que equivale a $\mathrm{gr}(\mathrm{mcd}(f,g)) = 2$. Mientras que si sólo coincide una raíz, digamos $\alpha_2 = \beta_2$ pero $\alpha_1 \neq \beta_1$, tenemos que $\mathrm{mcd}(f,g) = x - \alpha_2$ y $\mathrm{Res}(f,g) = 0$. Y resulta

$$0 \neq \mathrm{Sres}_1(f,g)(x) = a_2b_2\big((\alpha_1 - \beta_1)x - (\alpha_1 - \beta_1)\alpha_2\big) = a_2b_2(\alpha_1 - \beta_1)\mathrm{mcd}(f,g).$$

Vamos ahora a enunciar y demostrar una de las propiedades fundamentales de las subresultantes.

Teorema 1.1.3. *Sea* $k := \min\{d : \mathrm{Sres}_d(f,g)(x) \neq 0\}$. *Entonces*

$$\deg(\mathrm{mcd}(f,g)) = k \quad y \quad \mathrm{Sres}_k(f,g)(x) = \lambda\,\mathrm{mcd}(f,g),$$

para algún $\lambda \in K\backslash\{0\}$.

Para demostrar este resultado presentamos la construcción que permite que aparezca de modo natural la matriz de Sylvester.

Nos gustaría considerar la transformación lineal $\widetilde{\Phi}_d$ definida por

$$\begin{array}{rccc} \widetilde{\Phi}_d: & K[x]_{<n-d} \times K[x]_{<m-d} & \to & K[x]_{<m+n-d} \\ & (s,t) & \mapsto & s\,f + t\,g. \end{array}$$

Cuando $d = 0$, $\widetilde{\Phi}_0$ es la conocida transformación lineal entre dos espacios vectoriales de la misma dimensión que define la matriz de Sylvester para la resultante. El problema es que, cuando $d > 0$, ésta no es una transformación lineal entre espacios vectoriales de la misma dimensión, ya que $\dim_K(K[x]_{<n-d} \times K[x]_{<m-d}) = m + n - 2d$ mientras que $\dim_K(K[x]_{<m+n-d}) = m + n - d$. Para obtener una transformación lineal entre espacios de igual dimensión, descartamos los monomios de grado menor que d: escribamos $h = q_{x^d}(h)\, x^d + r_{x^d}(h)$, donde $q_{x^d}(h)$ y $r_{x^d}(h)$ son respectivamente el cociente y el resto de dividir a h por x^d, y notemos que $\operatorname{gr}(q_{x^d}(h)) < m + n - 2d$ cuando $\operatorname{gr}(h) < m + n - d$. De este modo *corregimos* la transformación lineal $\widetilde{\Phi}_d$ y definimos Φ_d:

$$\begin{array}{rccc} \Phi_d: & K[x]_{<n-d} \times K[x]_{<m-d} & \to & K[x]_{<m+n-2d} \\ & (s,t) & \mapsto & q_{x^d}(s\,f + t\,g). \end{array}$$

Se tiene entonces que Φ_d es un isomorfismo si, y sólo si, su matriz en cualquier par de bases es inversible. Considerando las bases canónicas ordenadas de $K[x]_{<n-d} \times K[x]_{<m-d}$ y $K[x]_{<m+n-2d}$ respectivamente,

$$\mathcal{B} := \Big((x^{n-d-1},0),\dots,(1,0),(0,x^{m-d-1}),\dots,(0,1)\Big) \text{ y } \mathcal{B}' := \Big(x^{m+n-2d-1},\dots,1\Big),$$

la matriz $[\Phi_d]_{\mathcal{B},B'}$ de Φ_d en las bases $\mathcal{B}$ y $\mathcal{B}'$ resulta ser

$$[\Phi_d]_{\mathcal{B},B'} = \left(\begin{array}{c|c|c|c|c} \uparrow & & \uparrow & \uparrow & \\ \big[q_{x^d}(x^{n-d-1}f)\big]_{\mathcal{B}'} & \cdots & [q_{x^d}(f)]_{\mathcal{B}'} & [q_{x^d}(x^{m-d-1}g)]_{\mathcal{B}'} & \cdots \\ \downarrow & & \downarrow & \downarrow & \end{array} \right.$$

$$\left. \begin{array}{c} \uparrow \\ [q_{x^d}(g)]_{\mathcal{B}'} \\ \downarrow \end{array} \right)$$

$$= \overbrace{\left[\begin{array}{ccc|ccccc} a_m & & & b_n & & & \\ \vdots & \ddots & & \vdots & \ddots & & \\ \vdots & & a_m & \vdots & & \ddots & \\ \vdots & & \vdots & b_d & & & b_n \\ a_d & & \vdots & \vdots & \ddots & & \vdots \\ \vdots & \ddots & \vdots & \vdots & & \ddots & \vdots \\ a_{d-(n-d-1)} & \cdots & a_d & b_{d-(m-d-1)} & \cdots & \cdots & b_d \end{array}\right]}^{n-d \qquad\qquad m-d} \Bigg\}\, m+n-2d \quad \in K^{(m+n-2d)\times(m+n-2d)}.$$

Aquí otra vez, los coeficientes eventualmente no definidos son 0.

Definamos

$$c_d(f,g) := \det([\Phi_d]_{\mathcal{B},B'}) \in K,$$

y supongamos por ahora que $c_d(f,g) \neq 0$. En este caso Φ_d es un isomorfismo y, por lo tanto, existen únicos $s, t \in K[x]$ con $\operatorname{gr}(s) < n-d$ y $\operatorname{gr}(t) < m-d$ tales que $q_{x^d}(s\,f+t\,g) = c_d(f,g)$. En particular existen $c_{d-1},\dots,c_0 \in K$ tales que, para dichos s y t,

$$s\,f + t\,g = c_d(f,g)x^d + c_{d-1}x^{d-1} + \cdots + c_0,$$

que tiene grado exactamente d. Trabajemos con ese polinomio $s\,f + t\,g$ de grado d. Denotemos

$$s = s_{n-d-1}x^{n-d-1} + \cdots + s_0 \quad \text{y} \quad t = t_{m-d-1}x^{m-d-1} + \cdots + t_0.$$

Aplicando la regla de Cramer, dado que $c_d(f,g) = \det([\Phi_d]_{\mathcal{B},B'})$, se tiene que la solución $(s_{n-d-1},\ldots,s_0,t_{m-d-1},\ldots,t_0)$ del sistema lineal

$$[\Phi_d]_{\mathcal{B},B'} \begin{pmatrix} s_{n-d-1} \\ \vdots \\ s_0 \\ t_{m-d-1} \\ \vdots \\ t_0 \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ c_d(f,g) \end{pmatrix},$$

satisface que s_{n-d-k} y t_{m-d-k} son los respectivos determinantes de la matriz $[\Phi_d]_{\mathcal{B},B'}$ donde se reemplazó la columna k, respectivamente $n-d+k$, por $(0,\ldots,0,1)^t$. Pero notemos que

$$s_{n-d-1} = \det \overset{\begin{array}{ccc} 1 & \qquad n-d-1 \qquad & \qquad m-d \qquad \end{array}}{\left|\begin{array}{c|ccc|ccc} 0 & & & & b_n & & \\ \vdots & a_m & & & \vdots & \ddots & \\ \vdots & \vdots & \ddots & & \vdots & & b_n \\ \vdots & \vdots & & a_m & \vdots & & \vdots \\ \vdots & \vdots & & \vdots & \vdots & & \vdots \\ 0 & a_{d+1-(n-d-2)} & \cdots & a_{d+1} & b_{d+1-(m-d-1)} & \cdots & b_{d+1} \\ 1 & a_{d+1-(n-d-1)} & \cdots & a_d & b_{d-(m-d-1)} & \cdots & b_d \end{array}\right|} \; {\scriptstyle m+n-2d}$$

$$= \det \overset{\begin{array}{cc} \qquad n-d-1 \qquad & \qquad m-d \qquad \end{array}}{\left|\begin{array}{cccc|ccc} a_m & & & & b_n & & \\ a_{m-1} & a_m & & & \vdots & \ddots & \\ \vdots & \vdots & \ddots & & \vdots & & b_n \\ \vdots & \vdots & & a_m & \vdots & & \vdots \\ \vdots & \vdots & & \vdots & \vdots & & \vdots \\ a_{d+1-(n-d-1)} & a_{d+1-(n-d-2)} & \cdots & a_{d+1} & b_{d+1-(m-d-1)} & \cdots & b_{d+1} \\ \hline 1 & 0 & \cdots & 0 & 0 & \cdots & 0 \end{array}\right|} \; \begin{array}{l} {\scriptstyle m+n-2d-1} \\ {\scriptstyle 1} \end{array},$$

y así para todas las columnas k. Por lo tanto,

$$s = s_{n-d-1}x^{n-d-1} + \cdots + s_0$$

$$= \det \overset{\begin{array}{cc} \qquad n-d \qquad & \qquad m-d \qquad \end{array}}{\left|\begin{array}{ccc|ccc} a_m & & & b_n & & \\ \vdots & \ddots & & \vdots & \ddots & \\ \vdots & & a_m & \vdots & & b_n \\ \vdots & & \vdots & \vdots & & \vdots \\ a_{d+1-(n-d-1)} & \cdots & a_{d+1} & b_{d+1-(m-d-1)} & \cdots & b_{d+1} \\ \hline x^{n-d-1} & \cdots & 1 & 0 & \cdots & 0 \end{array}\right|} \; \begin{array}{l} {\scriptstyle m+n-2d-1} \\ {\scriptstyle 1} \end{array},$$

y

$$t = t_{m-d-1}x^{m-d-1} + \cdots + t_0$$

$$= \det \begin{array}{|ccc|ccc|} \multicolumn{3}{c}{\overbrace{}^{n-d}} & \multicolumn{3}{c}{\overbrace{}^{m-d}} & \\ a_m & & & b_n & & & \\ \vdots & \ddots & & \vdots & \ddots & & \\ \vdots & & a_m & \vdots & & b_n & \} m+n-2d-1 \\ \vdots & & \vdots & \vdots & & \vdots & \\ a_{d+1-(n-d-1)} & \cdots & a_{d+1} & b_{d+1-(m-d-1)} & \cdots & b_{d+1} & \\ \hline 0 & \cdots & 0 & x^{m-d-1} & \cdots & 1 & 1 \end{array} .$$

Finalmente, el polinomio $s\,f + t\,g$ de grado d es

$$s\,f + t\,g = \det \begin{array}{|ccc|ccc|} \multicolumn{3}{c}{\overbrace{}^{n-d}} & \multicolumn{3}{c}{\overbrace{}^{m-d}} & \\ a_m & & & b_n & & & \\ \vdots & \ddots & & \vdots & \ddots & & \\ \vdots & & a_m & \vdots & & b_n & \} m+n-2d-1 \\ \vdots & & \vdots & \vdots & & \vdots & \\ a_{d+1-(n-d-1)} & \cdots & a_{d+1} & b_{d+1-(m-d-1)} & \cdots & b_{d+1} & \\ \hline x^{n-d-1}f & \cdots & f & x^{m-d-1}g & \cdots & g & 1 \end{array} .$$

La subresultante de la Definición 1.1.1 se define por medio de esta matriz, cuya transpuesta es la que llamamos matriz de Sylvester. Tomamos su transpuesta por razones históricas y por comodidad.

Propiedades de la subresultante y comentarios.

(1) El polinomio $\mathrm{Sres}_d(f,g)(x) \in K[x]$ está definido para $0 \leq d < \text{mín}\{m,n\}$ o $d = \text{mín}\{m,n\}$ si $m \neq n$, independientemente de que $c_d(f,g)$ sea 0 o no. Además su grado es menor o igual que d. Lo probamos en la construcción cuando $c_d(f,g) \neq 0$, pero en general es fácil verificar que los coeficientes de los monomios x^{d+1} hasta $x^{m+n-d-1}$ son nulos porque se corresponden con determinantes de matrices con dos filas repetidas. Al coeficiente principal de la subresultante se lo llama la *subresultante principal* y se lo nota $\mathrm{PSres}_d(f,g)$. Esto es,

$$\mathrm{PSres}_d(f,g) := \mathrm{coeff}_{x^d}\left(\mathrm{Sres}_d(f,g)(x)\right).$$

(2) Se tienen las siguientes relaciones:

- $\mathrm{Sres}_d(f,g)(x) = (-1)^{(m-d)(n-d)}\mathrm{Sres}_d(g,f)(x)$.
- $\mathrm{Sres}_d(af,bg)(x) = a^{n-d}b^{m-d}\mathrm{Sres}_d(f,g)(x)$.

Ambas observaciones pueden verse de manera inmediata mediante operaciones fundamentales en la matriz de Sylvester.

(3) *La identidad de Bézout*: La subresultante satisface una identidad

$$\mathrm{Sres}_d(f,g)(x) = s\,f + t\,g \text{ con } \mathrm{gr}(s) < n-d \text{ y } \mathrm{gr}(t) < m-d,$$

ya que descomponiendo la última columna de la matriz de Sylvester como $(x^{n-d-1},\dots 1,0,\dots,0)f+(0,\dots,0,x^{m-d-1},\dots,1)g$ recuperamos fácilmente los polinomios s y t.

Observemos en particular que $\mathrm{Sres}_d(f,g)(x) \in \langle f,g\rangle = \langle \mathrm{mcd}(f,g)\rangle$ implica

$$\mathrm{mcd}(f,g) \mid \mathrm{Sres}_d(f,g)(x) \text{ en } K[x]. \tag{1.1}$$

La identidad de Bézout tiene además una noción de unicidad que se especifica en el siguiente resultado.

Proposición 1.1.4. *Sean $F_d(f,g)$ y $G_d(f,g)$ los polinomios de $K[x]$ definidos por*

$$F_d(f,g) := \det \begin{array}{|cccccc|c} \multicolumn{6}{c}{\overbrace{\phantom{a_m \cdots a_{d+1-(n-d-1)}\ x^{n-d-1}}}^{m+n-2d}} & \\ a_m & \cdots & & \cdots & a_{d+1-(n-d-1)} & x^{n-d-1} & \\ & \ddots & & & \vdots & \vdots & n-d \\ & & a_m & \cdots & a_{d+1} & 1 & \\ \hline b_n & \cdots & & \cdots & b_{d+1-(m-d-1)} & 0 & \\ & \ddots & & & \vdots & \vdots & m-d \\ & & b_n & \cdots & b_{d+1} & 0 & \\ \hline \end{array},$$

$$G_d(f,g) := \det \begin{array}{|cccccc|c} \multicolumn{6}{c}{\overbrace{\phantom{a_m \cdots a_{d+1-(n-d-1)}\ 0}}^{m+n-2d}} & \\ a_m & \cdots & & \cdots & a_{d+1-(n-d-1)} & 0 & \\ & \ddots & & & \vdots & \vdots & n-d \\ & & a_m & \cdots & a_{d+1} & 0 & \\ \hline b_n & \cdots & & \cdots & b_{d+1-(m-d-1)} & x^{m-d-1} & \\ & \ddots & & & \vdots & \vdots & m-d \\ & & b_n & \cdots & b_{d+1} & 1 & \\ \hline \end{array}.$$

Se tiene que $\mathrm{Sres}_d(f,g)(x) = F_d(f,g)\,f + G_d(f,g)\,g$. *Además, si existen polinomios F y G tales que* $\deg(F) < n-d$, $\deg(G) < m-d$ *y* $F\,f + G\,g = \mathrm{Sres}_d(f,g)(x) \neq 0$, *entonces* $F = F_d(f,g)$ *y* $G = G_d(f,g)$.

Demostración. La identidad $\mathrm{Sres}_d(f,g)(x) = F_d(f,g)\,f + G_d(f,g)\,g$ la observamos en **(3)**. Veamos la unicidad. Tenemos

$$F\,f + G\,g = \mathrm{Sres}_d(f,g)(x) = F_d(f,g)\,f + G_d(f,g)\,g,$$

con lo cual

$$(F - F_d(f,g))f + (G - G_d(f,g))g = 0. \tag{1.2}$$

Si $G - G_d(f,g) = 0$, entonces necesariamente $F - F_d(f,g) = 0$ y termina la demostración. Supongamos que $G - G_d(f,g) \neq 0$ y lleguemos a una contradicción. Dividiendo en (1.2) por $\mathrm{mcd}(f,g)$ resulta

$$(F - F_d(f,g))\frac{f}{\mathrm{mcd}(f,g)} = -(G - G_d(f,g))\frac{g}{\mathrm{mcd}(f,g)}.$$

Pero como $\frac{f}{\mathrm{mcd}(f,g)}$ y $\frac{g}{\mathrm{mcd}(f,g)}$ son coprimos, necesariamente $\frac{f}{\mathrm{mcd}(f,g)} \mid G - G_d(f,g)$. Con lo cual, $m - \deg(\mathrm{mcd}(f,g)) \leq \deg(G - G_d(f,g)) < m - d$. Luego: $d < \deg(\mathrm{mcd}(f,g))$.

Por otro lado, por (1.1) tenemos que, si $\mathrm{Sres}_d(f,g)(x) \neq 0$, se tiene

$$\deg(\mathrm{mcd}(f,g)) \leq \deg(\mathrm{Sres}_d(f,g)(x)) \leq d.$$

Esto implica necesariamente que $\mathrm{Sres}_d(f,g)(x) = 0$, lo cual contradice nuestra hipótesis, y así queda probado el enunciado. □

Es fácil observar también que la identidad de (**2**) junto con la Proposición 1.1.4 nos permiten deducir

$$G_d(f,g) = (-1)^{(m-d)(n-d)} F_d(g,f). \tag{1.3}$$

Estamos ahora en condiciones de probar el Teorema 1.1.3, que generaliza la propiedad fundamental de la subresultante y el Ejemplo 1.1.2(3).

Demostración del Teorema 1.1.3. Ya vimos en (1.1) que para todo d se tiene $\gcd(f,g) \mid \mathrm{Sres}_d(f,g)(x)$. También es inmediato verificar que existen únicos $s, t \in K[x]$ con $\mathrm{gr}(s) < n - \mathrm{gr}(\mathrm{mcd}(f,g))$ y $\mathrm{gr}(t) < m - \mathrm{gr}(\mathrm{mcd}(f,g))$ tales que $\mathrm{mcd}(f,g) = s\,f + t\,g$. Luego, $\Phi_{\mathrm{gr}(\mathrm{mcd}(f,g))}(s,t) = 1$ tiene solución única y por lo tanto $\Phi_{\mathrm{gr}(\mathrm{mcd}(f,g))}$ es un isomorfismo. Con lo cual $c_{\mathrm{gr}(\mathrm{mcd}(f,g))}(f,g) \neq 0$, lo que implica $\mathrm{gr}(\mathrm{mcd}(f,g)) \geq k$ por la definición de k. □

Más generalmente, el *Teorema fundamental de la sucesión de restos polinomiales* describe exactamente toda la sucesión de subresultantes $\mathrm{Sres}_0(f,g)(x), \ldots, \mathrm{Sres}_d(f,g)(x)$ en función de los sucesivos restos que se obtienen cuando se realiza el algoritmo de Euclides para calcular $\mathrm{mcd}(f,g)$:

Teorema 1.1.5. *([Col1967, Th.1] [BrTr1971, Fund.Th.], [GCL1992, Th.7.4]) Sea K un cuerpo y sean $f, g \in K[x]$ con $\deg(f) =: m \leq n := \deg(g)$. Sea $0 \leq d < m$ o $d = m$ si $n > m$, y supongamos que $R_0 = g, R_1 = f, \ldots, R_k = c\,\mathrm{mcd}(f,g)$, con $c \in K\backslash\{0\}$, es la sucesión de restos en el algoritmo de Euclides entre f y g, llamando $r_i = \deg(R_i)$. Se tiene:*

1. *Si $d < r_k$, entonces $\mathrm{Sres}_d(f,g)(x) = 0$.*
2. *Si $d \geq r_k$, entonces*

$$\mathrm{Sres}_d(f,g)(x) = \begin{cases} \lambda_i R_i(x) & \text{si } d = r_i \\ \eta_i R_i(x) & \text{si } d = r_{i-1} - 1 \\ 0 & \text{en otro caso}, \end{cases}$$

con $\lambda_i, \eta_i \in K\backslash\{0\}$.

En [GCL1992, Th.7.4] se especifican los escalares λ_i y η_i. En el Capítulo 5 veremos una generalización de este teorema.

También nos será de gran utilidad el siguiente resultado conocido que se deduce, por ejemplo, de los Lemas 7.7.4 y 7.7.6 en [Mis1993].

Proposición 1.1.6. *Sean K un cuerpo y $f, g \in K[x]$ de grados m y n respectivamente y sea $0 \leq d < \text{mín}\{m,n\}$ o $d = \text{mín}\{m,n\}$ si $m \neq n$, con $\text{PSres}_d(f,g)(x) \neq 0$ (o sea, $\deg(\text{Sres}_d(f,g)(x)) = d$). Si existen polinomios $F, G \in K[x]$ con $\deg(F) < n-d$ y $\deg(G) < m-d$ tales que $F\,f + G\,g$ es un polinomio no nulo con $\deg(F\,f + G\,g) \leq d$, entonces existe $\lambda \in K\backslash\{0\}$ tal que*

$$F\,f + G\,g = \lambda\,\text{Sres}_d(f,g)(x).$$

1.2. Sumas de Sylvester

La conocida fórmula de Poisson para la resultante (c.f. [Poi1802])

$$\text{Res}(f,g) = a_m^n \prod_{1 \leq i \leq m} g(\alpha_i),$$

es una expresión para la resultante en términos de las raíces de los polinomios. Dado que la resultante es un caso particular de la subresultante, es natural preguntarse por una fórmula de Poisson más general que corresponda a esta última. De esto se tratan las sumas de Sylvester, introducidas también por él en [Syl1853]. Necesitamos antes de definirlas fijar la siguiente notación.

Notación 1.2.1. Dados dos subconjuntos finitos no vacíos A y B de un cuerpo K, notamos

$$\mathcal{R}(A,B) = \prod_{a \in A,\, b \in B} (a-b),$$

y definimos $\mathcal{R}(A,B) = 1$ si $A = \emptyset$ o $B = \emptyset$.

La siguiente es una observación muy sencilla, pero dado que la usaremos permanentemente, vamos a destacarla.

Observación 1.2.2. Sean A y B subconjuntos de un cuerpo K, con $|A| = m$ y $|B| = n$. Se tiene

1. $\mathcal{R}(A,B) = (-1)^{mn}\mathcal{R}(B,A)$.
2. $\mathcal{R}(A,B) = 0 \iff A \cap B \neq \emptyset$.

Ahora podemos definir las sumas de Sylvester.

Definición 1.2.3. Sean A y B dos subconjuntos de un cuerpo K, con $|A| = m$ y $|B| = n$, y sean $0 \leq p \leq m$, $0 \leq q \leq n$. Se define la *suma doble de Sylvester* como

$$\mathrm{Syl}_{p,q}(A,B)(x) := \sum_{\substack{A' \subset A,\, B' \subset B \\ |A'|=p,\, |B'|=q}} \mathcal{R}(A', B')\, \mathcal{R}(A \backslash A', B \backslash B')\, \frac{\mathcal{R}(x, A')\, \mathcal{R}(x, B')}{\mathcal{R}(A', A \backslash A')\, \mathcal{R}(B', B \backslash B')},$$

que es un polinomio en x de grado acotado por $p + q =: d$. Cuando $p = 0$ o $q = 0$, las expresiones que resultan son llamadas *sumas simples de Sylvester*. Esto es, las sumas simples de Sylvester son

$$\mathrm{Syl}_{d,0}(A,B)(x) = \sum_{A' \subset A,\, |A'|=d} \mathcal{R}(A \backslash A', B) \frac{\mathcal{R}(x, A')}{\mathcal{R}(A', A \backslash A')},$$

y

$$\mathrm{Syl}_{0,d}(A,B)(x) = \sum_{B' \subset B,\, |B'|=d} \mathcal{R}(A, B \backslash B') \frac{\mathcal{R}(x, B')}{\mathcal{R}(B', B \backslash B')}.$$

Para los casos extremos las sumas dobles dan resultados sencillos:

$$\begin{aligned}
&\mathrm{Syl}_{0,0}(A,B)(x) = \mathcal{R}(A,B), \\
&\mathrm{Syl}_{m,0}(A,B)(x) = \mathcal{R}(x,A), \\
&\mathrm{Syl}_{0,n}(A,B)(x) = \mathcal{R}(x,B), \\
&\mathrm{Syl}_{m,n}(A,B)(x) = \mathcal{R}(A,B)\mathcal{R}(x,A)\mathcal{R}(x,B).
\end{aligned}$$

Además es fácil ver que $\mathrm{Syl}_{p,q}(A,B)(x) = (-1)^{pq+(m-p)(n-q)}\mathrm{Syl}_{q,p}(B,A)(x)$, trabajando cuidadosamente con el signo vía la Observación 1.2.2.

En el trabajo de Sylvester se muestra la relación entre ambas sumas simples:

Proposición 1.2.4.

$$\mathrm{Syl}_{d,0}(A,B)(x) = (-1)^{d(m-d)}\mathrm{Syl}_{0,d}(A,B)(x).$$

En el Capítulo 3 veremos que este resultado se puede obtener como consecuencia inmediata del *lema de intercambio* que presentamos en el Capítulo 2.

Vamos a relacionar ahora las sumas de Sylvester con las subresultantes. Dados dos conjuntos A y B, con $|A| = m$ y $|B| = n$, podemos asociarlos a los polinomios $f(x) := \mathcal{R}(x, A)$ y $g(x) := \mathcal{R}(x, B)$. De este modo, por ejemplo:

$$\begin{aligned}
&\mathrm{Syl}_{0,0}(A,B)(x) = \mathcal{R}(A,B) = \mathrm{Res}(f,g), \\
&\mathrm{Syl}_{m,0}(A,B)(x) = \mathcal{R}(x,A) = f, \\
&\mathrm{Syl}_{0,n}(A,B)(x) = \mathcal{R}(x,B) = g, \\
&\mathrm{Syl}_{m,n}(A,B)(x) = \mathcal{R}(A,B)\mathcal{R}(x,A)\mathcal{R}(x,B) = \mathrm{Res}(f,g)\, f\, g.
\end{aligned}$$

Sylvester enunció en [Syl1840b], y luego probó en [Syl1853, Section II], la siguiente relación entre subresultantes y sumas dobles.

Teorema 1.2.5. *Sean A y B subconjuntos de un cuerpo K, con $|A| = m$ y $|B| = n$ y sean $f(x) := \mathcal{R}(x, A)$ y $g(x) := \mathcal{R}(x, B)$. Sean $0 \leq p \leq m$, $0 \leq q \leq n$ y $d := p + q$, con $0 \leq d < \min\{m, n\}$ o $d = \min\{m, n\}$ si $m \neq n$. Entonces*

$$\mathrm{Syl}_{p,q}(A, B)(x) = (-1)^{p(m-d)} \binom{d}{p} \mathrm{Sres}_d(f, g)(x).$$

En particular

$$\mathrm{Syl}_{d,0}(A, B)(x) = (-1)^{d(m-d)} \mathrm{Sres}_d(f, g)(x).$$

Más en general, si f y g no son necesariamente mónicos, se tiene

$$a_m^{n-d} b_n^{m-d} \mathrm{Syl}_{d,0}(A, B)(x) = (-1)^{d(m-d)} \mathrm{Sres}_d(f, g)(x),$$

si $f = a_m \mathcal{R}(x, A)$ y $g = b_n \mathcal{R}(x, B)$. En efecto, asumiendo que vale para polinomios mónicos, y llamando $\widetilde{f} = \mathcal{R}(x, A)$ y $\widetilde{g} = \mathcal{R}(x, B)$, se tiene

$$\begin{aligned} \mathrm{Sres}_d(f, g)(x) = \mathrm{Sres}_d(a_m \widetilde{f}, b_n \widetilde{g})(x) &= a_m^{n-d} b_n^{m-d} \mathrm{Sres}_d(\widetilde{f}, \widetilde{g})(x) \\ &= (-1)^{d(m-d)} a_m^{n-d} b_n^{m-d} \mathrm{Syl}_{d,0}(A, B)(x). \end{aligned}$$

El resultado del Teorema 1.2.5 también puede encontrarse en [LaPr2003], [DHKS2007] y [RoSz2011]. Este teorema es el que nos dice que las sumas de Sylvester pueden verse como una generalización de la fórmula de Poisson para la resultante. Nos brinda justamente una fórmula para la subresultante en términos de las raíces de los polinomios. Hay, sin embargo, una gran limitación. Hemos partido de dos conjuntos A y B y asociamos a ellos los polinomios $\mathcal{R}(x, A)$ y $\mathcal{R}(x, B)$, que en particular tienen raíces simples. Sin embargo, $\mathrm{Sres}_d(f, g)(x)$ está definida independientemente de la multiplicidad de las raíces de los polinomios, pues la definición depende de sus coeficientes, mientras que las sumas de Sylvester (simples o dobles) sólo están definidas para conjuntos (sin elementos repetidos). En el Capítulo 4 extenderemos las sumas de Sylvester para abarcar el caso general.

En trabajos más recientes se logró obtener la descripción completa de $\mathrm{Syl}_{p,q}(A, B)(x)$ para todos los casos posibles de $0 \leq p \leq m$ y $0 \leq q \leq n$:

Teorema 1.2.6. *([DHKS2009, Main Th. 1], [KrSz2012, Th. 1]) Sean A y B subconjuntos de un cuerpo K con $|A| = m$ y $|B| = n$, tales que $1 \leq m \leq n$. Sean $0 \leq p \leq m$ y $0 \leq q \leq n$ y sean $d := p + q$ y $k := m + n - d - 1$. Si $f = \mathcal{R}(x, A)$ y $g = \mathcal{R}(x, B)$ se tiene*

$$\mathrm{Syl}_{p,q}(A, B)(x) = \begin{cases} (-1)^{p(m-d)} \binom{d}{p} \mathrm{Sres}_d(f, g)(x) & \text{si } 0 \leq d < m \text{ o } m = d < n \\ 0 & \text{si } m < d < n - 1 \\ (-1)^{(p+1)(m+n-1)} \binom{m}{p} f & \text{si } m < d = n - 1 \\ (-1)^{\sigma} \Big(\binom{k}{m-p} F_k(f, g)\ f - \binom{k}{n-q} G_k(f, g)\ g \Big) & \\ = (-1)^{\sigma+1} \Big(\binom{k}{n-q} \mathrm{Sres}_k(f, g) - \binom{k+1}{m-p} F_k(f, g)\ f \Big) & \text{si } n \leq d \leq m + n - 1 \\ \mathrm{Res}(f, g)\ f\, g & \text{si } d = m + n, \end{cases}$$

donde $\sigma := (d - m)(n - q) + d - n - 1$ y donde $F_k(f, g)$ y $G_k(f, g)$ son los coeficientes polinomiales de f y g en la identidad de the Bézout descriptos en la Proposición 1.1.4.

Observemos que el Teorema 1.2.6, si bien está enunciado para $m \leq n$, en efecto da la descripción completa de $\mathrm{Syl}_{p,q}(A,B)(x)$ en términos de $\mathrm{Sres}_d(f,g)(x)$ y de $F_k(f,g)$ y $G_k(f,g)$ para todo valor de m y n, debido a las simetrías

$$\mathrm{Syl}_{p,q}(A,B)(x) = (-1)^{pq+(m-p)(n-q)}\mathrm{Syl}_{q,p}(B,A)(x),$$
$$\mathrm{Sres}_d(f,g)(x) = (-1)^{(m-d)(n-d)}\mathrm{Sres}_d(g,f)(x),$$

que ya hemos observado.

En el Capítulo 3 demostraremos el Teorema 1.2.6 usando técnicas de interpolación y el lema de intercambio del Capítulo 2.

Capítulo 2

Lema de intercambio

En este capítulo presentamos la identidad llamada *lema de intercambio* que será el ingrediente principal en las construcciones que veremos en los Capítulos 3, 4 y 5.

En la Sección 2.1 presentamos los lineamientos generales de la *interpolación simétrica multivariada*, desarrollada por W. Chen y J. Louck, que es el marco teórico en donde se desarrolla el lema de intercambio. En la Sección 2.2 presentamos el lema de intercambio en sus diferentes versiones y generalizaciones. Este lema y algunas de sus variantes se encuentran en el trabajo [DKSV2017], aceptado para su presentación en el congreso MEGA2017, realizado junto con Carlos D'Andrea, Teresa Krick y Agnes Szanto. Una versión anterior del lema, más débil, se encuentra en el trabajo publicado [KSV2017], realizado junto con Teresa Krick y Agnes Szanto. Otras generalizaciones y observaciones son resultados originales de esta tesis. En la Sección 2.2 lo especificamos para cada resultado.

2.1. Preliminar: interpolación simétrica multivariada

El problema de interpolación de Lagrange consiste en explicitar el único polinomio de grado menor o igual que $n-1$ que toma determinados valores en n puntos dados. Concretamente se tiene:

Proposición 2.1.1. *Sean K un cuerpo y $n \in \mathbb{N}$. Sea $A = \{\alpha_1, \ldots, \alpha_n\}$ un subconjunto de K y sean $\beta_1, \ldots, \beta_n \in K$, no necesariamente distintos. Existe un único polinomio $f \in K[x]$, nulo o de grado menor o igual que $n-1$, tal que $f(\alpha_i) = \beta_i$, para $1 \leq i \leq n$, siendo*

$$f(x) = \sum_{1 \leq i \leq n} \beta_i \frac{\prod_{j \neq i}(x - \alpha_j)}{\prod_{j \neq i}(\alpha_i - \alpha_j)}.$$

Más aún, al conjunto

$$\left\{ \frac{\prod_{j \neq i}(x - \alpha_j)}{\prod_{j \neq i}(\alpha_i - \alpha_j)} \, ; \, 1 \leq i \leq n \right\},$$

se lo llama una base de Lagrange, pues cualquier polinomio $f \in K[x]$ nulo o de grado

menor o igual que $n-1$ se escribe de forma única como

$$f(x) = \sum_{1 \le i \le n} f(\alpha_i) \frac{\prod_{j \neq i}(x - \alpha_j)}{\prod_{j \neq i}(\alpha_i - \alpha_j)}.$$

Vamos a trabajar con la generalización de este resultado a polinomios de más de una variable. Consideraremos un espacio vectorial adecuado de polinomios y una base conveniente de dicho espacio. Esta construcción es la llamada interpolación simétrica de Lagrange que fue introducida por W. Chen y J. Louck en [ChLo1996, Th.2.1]. En dicho artículo se describe una base de interpolación de Lagrange para polinomios simétricos en varias variables que especificamos más abajo en la Proposición 2.1.4. Para precisar la interpolación simétrica introducimos la siguiente notación.

Notación 2.1.2. Notamos por $S_{(\ell,d)}$ al K-espacio vectorial formado por todos los polinomios *simétricos* h en ℓ variables $x_1, \ldots, x_\ell$ de multigrado acotado por $(d, \ldots, d)$, i.e. tal que $\deg_{x_i}(h) \le d$ para $1 \le i \le \ell$ (sin una cota específica para el grado total de h). En caso que haya ambigüedad y sea necesario explicitar el cuerpo, escribiremos $S_{(\ell,d)}(K)$.

El siguiente lema nos ayuda a entender la estructura del espacio $S_{(\ell,d)}$.

Lema 2.1.3. $\dim_K(S_{(\ell,d)}) = \binom{\ell+d}{d}$.

Demostración. Por el teorema fundamental de los polinomios simétricos elementales sabemos que el espacio de polinomios simétricos en ℓ-variables está generado, como álgebra, por los polinomios simétricos elementales

$$e_1(x_1, \ldots, x_\ell) = x_1 + \cdots + x_\ell, \ \ldots, \ e_\ell(x_1, \ldots, x_\ell) = x_1 \cdots x_\ell,$$

que son, en particular, polinomios homogéneos de grado 1 en cada variable x_i. Por lo tanto, cada polinomio simétrico h de multigrado acotado por $(d, \ldots, d)$ puede escribirse de forma única como

$$h = \sum_{\mathbf{a}} c_{\mathbf{a}} e_1^{a_1} \cdots e_\ell^{a_\ell},$$

con $|\mathbf{a}| := a_1 + \cdots + a_\ell \le d$. Así, h es un polinomio en $e_1, \ldots, e_\ell$ de grado total acotado por d; y es conocido que el espacio de tales polinomios tiene dimensión $\binom{\ell+d}{d}$. □

Ahora podemos explicitar la base adecuada con la que vamos a trabajar y enunciar el resultado de escritura única en $S_{(\ell,d)}$ que generaliza el caso de una variable. A los efectos de simplificar la escritura, llamaremos $m := \ell + d$, de modo que escribiremos $S_{(m-d,d)}$, que tiene dimensión $\binom{m}{d}$. Recordemos además la definición de $\mathcal{R}(A, B)$ introducida en la Notación 1.2.1.

Proposición 2.1.4. *([ChLo1996, Th.2.1]) Sean $0 \le d \le m-1$ y $X := (x_1, \ldots, x_{m-d})$. Dado $A = \{\alpha_1, \ldots, \alpha_m\}$, el conjunto*

$$\mathcal{A} := \left\{ \mathcal{R}(X, A') \,;\, A' \subset A, |A'| = d \right\} \subset S_{(m-d,d)},$$

es una base de $S_{(m-d,d)}$. *Más aún, cualquier polinomio* $h(X) \in S_{(m-d,d)}$ *se escribe de forma única como*

$$h(X) = \sum_{A' \subset A, |A'|=d} h(A \backslash A') \frac{\mathcal{R}(X, A')}{\mathcal{R}(A \backslash A', A')},$$

donde $h(A \backslash A') := h(\alpha_{i_1}, \ldots, \alpha_{i_{m-d}})$, *con* $A \backslash A' = \{\alpha_{i_1}, \ldots, \alpha_{i_{m-d}}\}$.

Demostración. Como hay exactamente $\binom{m}{d} = \dim_K(S_{(m-d,d)})$ elementos en $\mathcal{A}$, basta probar que son linealmente independientes. Supongamos

$$\sum_{A' \subset A, |A'|=d} c_{A'} \mathcal{R}(X, A') = 0.$$

Para cada subconjunto $\{\alpha_{i_1}, \ldots, \alpha_{i_{m-d}}\} \subset A$, si evaluamos la suma en $x_1 = \alpha_{i_1}, \ldots, x_{m-d} = \alpha_{i_{m-d}}$, cada término de ella se anula, excepto para $A' := A \backslash \{\alpha_{i_1}, \ldots, \alpha_{i_{m-d}}\}$, en el que se obtiene $c_{A'} \mathcal{R}(A \backslash A', A')$. Dado que $\mathcal{R}(A \backslash A', A') \neq 0$, resulta necesariamente que $c_{A'} = 0$, y esto prueba la independencia lineal.

La segunda afirmación se deduce del hecho que $h(X) \in S_{(m-d,d)}$ se escribe unívocamente en la base $\mathcal{A}$, y sus coordenadas están unívocamente definidas por las evaluaciones en cada $\{\alpha_{i_1}, \ldots, \alpha_{i_{m-d}}\} \subset A$. □

W. Chen y J. Louck usan este resultado en su artículo para obtener identidades que involucran polinomios simétricos generalizando, por ejemplo, la siguiente identidad polinomial para un conjunto finito $A = \{\alpha_1, \ldots, \alpha_m\}$ contenido en un cuerpo K, y un conjunto finito de variables $X = \{x_1 \ldots, x_{m-d}\}$:

$$x_1 \cdots x_{m-d} = \sum_{A' \subset A, |A'|=d} \Big(\prod_{\alpha_j \notin A'} \alpha_j \Big) \frac{\prod_{x_j \in X, \alpha_i \in A'} (x_j - \alpha_i)}{\prod_{\alpha_j \notin A', \alpha_i \in A'} (\alpha_j - \alpha_i)}.$$

En el marco de la interpolación simétrica, A. Lascoux probó en [Las, Lem.Rt1] la siguiente identidad: Dados A y B subconjuntos finitos de un cuerpo K, con $|A| = m$ y $|B| = d$, tales que $m \geq d$. Si $X = (x_1, \ldots, x_{m-d})$, se tiene

$$\sum_{A' \subset A, |A'|=d} \mathcal{R}(A \backslash A', B) \frac{\mathcal{R}(X, A')}{\mathcal{R}(A \backslash A', A')} = \mathcal{R}(X, B). \tag{2.1}$$

En la siguiente sección veremos que el lema de intercambio que allí presentamos generaliza esta identidad.

2.2. Lema de intercambio

El lema de intercambio (*exchange lemma*), es una de las fórmulas principales obtenidas en esta tesis y de la que derivamos numerosas aplicaciones. Es una identidad tan sencilla como sorprendente y que generaliza en particular la identidad (2.1) de Lascoux. Al hablar del lema de intercambio vamos a referirnos al Teorema 2.2.2 más abajo, pero daremos

también otras fórmulas, algunas más generales, que pueden verse como diferentes versiones del mismo resultado. El siguiente lema brinda la identidad a partir de la cual se derivan todas las otras y puede ser considerado como una versión débil del lema de intercambio.

Lema 2.2.1. *([KSV2017, Lemma 3.1]) Sea A un subconjunto de un cuerpo K, con $|A| = m$, y sean $0 \leq d \leq m$ y X un conjunto de variables tal que $|X| \leq m - d$. Sea B otro subconjunto finito de K tal que $|B| \geq d$. Entonces*

$$\sum_{A' \subset A, |A'|=d} \mathcal{R}(A \backslash A', B) \frac{\mathcal{R}(X, A')}{\mathcal{R}(A \backslash A', A')} = \sum_{B' \subset B, |B'|=d} \mathcal{R}(A, B \backslash B') \frac{\mathcal{R}(X, B')}{\mathcal{R}(B', B \backslash B')}.$$

Demostración. Supongamos primero que $|X| = m - d$. Notemos que, por la Proposición 2.1.4, el polinomio $h(X) \in S_{(m-d,d)}$ del miembro izquierdo de la igualdad es el único polinomio simétrico de ese espacio que satisface las $\binom{m}{d}$ condiciones $h(A \backslash A') = \mathcal{R}(A \backslash A', B)$. Dado que el polinomio del miembro derecho de la igualdad también pertenece al espacio $S_{(m-d,d)}$, basta probar que especializa lo mismo. Esto es

$$\sum_{B' \subset B, |B'|=d} \mathcal{R}(A, B \backslash B') \frac{\mathcal{R}(A \backslash A', B')}{\mathcal{R}(B', B \backslash B')} = \mathcal{R}(A \backslash A', B), \ \forall A' \subset A, |A'| = d.$$

Pero

$$\begin{aligned} \sum_{B' \subset B, |B'|=d} \mathcal{R}(A, B \backslash B') \frac{\mathcal{R}(A \backslash A', B')}{\mathcal{R}(B', B \backslash B')} &= \sum_{B' \subset B, |B'|=d} \mathcal{R}(A', B \backslash B') \mathcal{R}(A \backslash A', B \backslash B') \frac{\mathcal{R}(A \backslash A', B')}{\mathcal{R}(B', B \backslash B')} \\ &= \mathcal{R}(A \backslash A', B) \sum_{B' \subset B, |B'|=d} \frac{\mathcal{R}(A', B \backslash B')}{\mathcal{R}(B', B \backslash B')}. \end{aligned}$$

Consideremos para Y, un conjunto de variables con $|Y| = d$, el polinomio

$$\Psi(Y) = \sum_{B' \subset B, |B'|=d} \frac{\mathcal{R}(Y, B \backslash B')}{\mathcal{R}(B', B \backslash B')} \in S_{(d,|B|-d)}.$$

De nuevo, por la Proposición 2.1.4, éste es el único polinomio de $S_{(d,|B|-d)}$ que satisface las $\binom{|B|}{d}$ condiciones $\Psi(B') = 1$, $\forall B' \subset B$, $|B'| = d$, por lo que $\Psi = 1$. En particular $\Psi(A') = 1$, lo cual prueba lo que queremos.

El caso $|X| < m - d$ se obtiene simplemente tomando coeficientes. Escribamos $X = (x_1, \ldots, x_r)$, con $r < m - d$ y completemos a $m - d$ variables con $X' = (x_{r+1}, \ldots, x_{m-d})$. Entonces vimos que

$$\sum_{A' \subset A, |A'|=d} \mathcal{R}(A \backslash A', B) \frac{\mathcal{R}(X \cup X', A')}{\mathcal{R}(A \backslash A', A')} = \sum_{B' \subset B, |B'|=d} \mathcal{R}(A, B \backslash B') \frac{\mathcal{R}(X \cup X', B')}{\mathcal{R}(B', B \backslash B')}.$$

La igualdad que buscamos se obtiene igualando el coeficiente de $x_{r+1}^d \ldots x_{m-d}^d$ de ambos miembros de esta igualdad. □

Notemos que en el caso particular $|B| = d$ y $|X| = m - d$, el Lema 2.2.1 dice

$$\sum_{A' \subset A, |A'|=d} \mathcal{R}(A \backslash A', B) \frac{\mathcal{R}(X, A')}{\mathcal{R}(A \backslash A', A')} = \mathcal{R}(X, B),$$

que es exactamente la identidad (2.1). En el trabajo [Las, Lem.Rt1], A. Lascoux prueba dicha identidad usando funciones de Schur y no parece posible derivar nuestro lema a partir de tal resultado.

Antes de presentar identidades más generales de este lema tratemos de comprender su significado. Si bien se trata de una identidad de polinomios cuya demostración es bastante elemental, es una igualdad que resulta sorprendente y sus implicancias no son triviales aún en el caso de una variable. Miremos algunos casos particulares.

Para expresiones del tipo $A \backslash \{\alpha\}$, $A \cup \{\beta\}$ y $\mathcal{R}(\{\alpha\}, B)$, vamos a escribir respectivamente $A \backslash \alpha$, $A \cup \beta$ y $\mathcal{R}(\alpha, B)$, para no recargar la notación. Consideremos el caso de una variable, es decir, tomemos $|X| = 1$ en el Lema 2.2.1. Supongamos además $d = m - 1 = |B|$. Aquí la igualdad es inmediata, pues consiste en

$$\sum_{\alpha \in A} \mathcal{R}(\alpha, B) \frac{\mathcal{R}(x, A \backslash \alpha)}{\mathcal{R}(\alpha, A \backslash \alpha)} = \mathcal{R}(x, B),$$

que es exactamente la escritura única del polinomio $\mathcal{R}(x, B)$ mediante la interpolación de Lagrange, es decir, la Proposición 2.1.1. Ésta es, además, la identidad (2.1) de Lascoux para el caso $d = m - 1$. Siguiendo en el caso de una variable y $d = m - 1$, también es sencillo entender la identidad cuando $|B| = m$. Aquí el Lema 2.2.1 dice

$$\sum_{\alpha \in A} \mathcal{R}(\alpha, B) \frac{\mathcal{R}(x, A \backslash \alpha)}{\mathcal{R}(\alpha, A \backslash \alpha)} = \sum_{\beta \in B} \mathcal{R}(A, \beta) \frac{\mathcal{R}(x, B \backslash \beta)}{\mathcal{R}(B \backslash \beta, \beta)}.$$

Llamemos $f(x) := \mathcal{R}(x, A)$, $g(x) := \mathcal{R}(x, B)$ y $h(x)$ al polinomio de la igualdad. Mirando la escritura de h en el miembro izquierdo, tenemos que h es el único polinomio de grado menor o igual que $m - 1$ tal que $h(\alpha) = g(\alpha)$, para todo $\alpha \in A$. Equivalentemente, h es el único polinomio de grado menor o igual que $m - 1$ que es *congruente a g módulo f*. Análogamente, mirando la escritura del lado derecho, resulta que h es el único polinomio de grado menor o igual que $m - 1$ tal que $h(\beta) = (-1)^{m+(m-1)} f(\beta) = -f(\beta)$, para todo $\beta \in B$. Esto es, h es el único polinomio de grado menor o igual que $m - 1$ que es *congruente a $-f$ módulo g*. De modo que el lema dice que, para $\deg(h) \leq m - 1$, se tiene: $h \equiv g (\text{mód } f) \iff h \equiv -f (\text{mód } g)$. Esta equivalencia de hecho es inmediata por las condiciones en las que estamos: f y g son mónicos y de igual grado. Más aún, resulta que $h = g - f$. También es fácil ver que podemos deducir la identidad del caso $|B| = m - 1$ a partir del caso $|B| = m$. En efecto, si consideramos $B = B' \cup \beta_0$, con $|B'| = m - 1$, tenemos

$$\sum_{\alpha \in A} \mathcal{R}(\alpha, B' \cup \beta_0) \frac{\mathcal{R}(x, A \backslash \alpha)}{\mathcal{R}(\alpha, A \backslash \alpha)} = \sum_{\beta \in B' \cup \beta_0} \mathcal{R}(A, \beta) \frac{\mathcal{R}(x, (B' \cup \beta_0) \backslash \beta)}{\mathcal{R}((B' \cup \beta_0) \backslash \beta, \beta)},$$

y si tomamos a ambos lados el coeficiente de β_0 (o bien derivamos respecto a β_0), se recupera fácilmente la identidad del caso $|B| = m - 1$, con B' en lugar de B.

Cuando $|B| > m$, aún siguiendo en el caso de una variable, la igualdad del lema ya no puede leerse en términos de interpolación de Lagrange y su significado no es inmediato.

Podemos dar una escritura del Lema 2.2.1 con una notación más simétrica y quizás más natural, independizándonos de la perspectiva de la interpolación. En las condiciones de dicho lema se tiene

$$\sum_{\substack{A_1 \cup A_2 = A \\ |A_1|=d, |A_2|=m-d}} \frac{\mathcal{R}(A_2, B)\mathcal{R}(X, A_1)}{\mathcal{R}(A_2, A_1)} = \sum_{\substack{B_1 \cup B_2 = B \\ |B_1|=d, |B_2|=|B|-d}} \frac{\mathcal{R}(A, B_2)\mathcal{R}(X, B_1)}{\mathcal{R}(B_1, B_2)}. \tag{2.2}$$

Esta notación es la que usaremos en el lema de intercambio, que es el teorema siguiente, el central de este capítulo. Extiende el Lema 2.2.1 relajando la hipótesis sobre $|X|$ y no impone condiciones sobre $|B|$.

Teorema 2.2.2. *[Lema de intercambio]([DKSV2017, Lemma 2.4]) Sea $d \geq 0$. Sean A y B subconjuntos finitos de un cuerpo K con $|A| \geq d$ y sea X un conjunto de variables con $|X| \leq |A| + |B| - 2d$. Entonces*

1. *Si $|B| \geq d$, se tiene*

$$\sum_{\substack{A_1 \cup A_2 = A \\ |A_1|=d, |A_2|=|A|-d}} \frac{\mathcal{R}(A_2, B)\mathcal{R}(X, A_1)}{\mathcal{R}(A_2, A_1)} = \sum_{\substack{B_1 \cup B_2 = B \\ |B_1|=d, |B_2|=|B|-d}} \frac{\mathcal{R}(A, B_2)\mathcal{R}(X, B_1)}{\mathcal{R}(B_1, B_2)}.$$

2. *Si $|B| < d$, se tiene*

$$\sum_{\substack{A_1 \cup A_2 = A \\ |A_1|=d, |A_2|=|A|-d}} \frac{\mathcal{R}(A_2, B)\mathcal{R}(X, A_1)}{\mathcal{R}(A_2, A_1)} = 0.$$

Demostración. (1) Cuando $|B| \geq d$, si $|X| \leq |A| - d$, estamos en las condiciones del Lema 2.2.1, o más explícitamente, la igualdad (2.2), usando la escritura simétrica; con lo cual, la igualdad es cierta.
Supongamos ahora que $|B| \geq d$ y $|X| > |A| - d$. Llamemos $r := |X| - (|A| - d)$ y escribamos $X = Y \cup Z$, con $Y = (x_1, \cdots, x_{|A|-d})$ y $Z = (x_{|A|-d+1}, \cdots, x_r)$. Definimos

$$h(Y, Z) = \sum_{\substack{A_1 \cup A_2 = A \\ |A_1|=d, |A_2|=|A|-d}} \frac{\mathcal{R}(A_2, B)\mathcal{R}(Y, A_1)\mathcal{R}(Z, A_1)}{\mathcal{R}(A_2, A_1)},$$

y

$$g(Y, Z) = \sum_{\substack{B_1 \cup B_2 = B \\ |B_1|=d, |B_2|=|B|-d}} \frac{\mathcal{R}(A, B_2)\mathcal{R}(Y, B_1)\mathcal{R}(Z, B_1)}{\mathcal{R}(B_1, B_2)}.$$

Queremos ver entonces que $h = g$ y para esto consideramos $g, h \in K(Z)[Y]$, i.e. miramos a dichos polinomios con coeficientes en el cuerpo $K(Z)$ y en las variables Y. Ambos polinomios son simétricos en Y y tienen multigrado en Y acotado por d. Esto es, $h, g \in S_{n-d,d}(K(Z))$. Por la Proposición 2.1.4, basta probar que $h(A_2, Z) = g(A_2, Z)$, para todo $A_2 \subset A$ con $|A_2| = |A| - d$. Claramente, dado un tal A_2, $h(A_2, Z) = \mathcal{R}(A_2, B)\mathcal{R}(Z, A_1)$, donde $A_1 := A \backslash A_2$. Calculemos $g(A_2, Z)$:

$$\begin{aligned} g(A_2, Z) &= \sum_{\substack{B_1 \cup B_2 = B \\ |B_1| = d,\, |B_2| = |B| - d}} \frac{\mathcal{R}(A, B_2)\mathcal{R}(A_2, B_1)\mathcal{R}(Z, B_1)}{\mathcal{R}(B_1, B_2)} \\ &= \mathcal{R}(A_2, B) \sum_{\substack{B_1 \cup B_2 = B \\ |B_1| = d,\, |B_2| = |B| - d}} \frac{\mathcal{R}(A_1, B_2)\mathcal{R}(Z, B_1)}{\mathcal{R}(B_1, B_2)}. \end{aligned}$$

Luego, basta ver que

$$\sum_{\substack{B_1 \cup B_2 = B \\ |B_1| = d,\, |B_2| = |B| - d}} \frac{\mathcal{R}(A_1, B_2)\mathcal{R}(Z, B_1)}{\mathcal{R}(B_1, B_2)} = \mathcal{R}(Z, A_1).$$

Pero esto es cierto de nuevo por (2.2), tomando B en lugar de A, A_1 en lugar de B y Z en lugar de X. En efecto, la hipótesis que necesitamos se cumple, pues $|Z| = |X| - (|A| - d) \leq |B| - d$; y además, en este caso, el único subconjunto de A_1 de cardinal d es el mismo A_1.

(2) Cuando $|B| < d$, el truco consiste en *agrandar* B agregando variables Y, de modo que $|B \cup Y| = d$. Digamos $Y = (y_1, \cdots, y_s)$, con $s = d - |B|$. Aplicando el item previo, tenemos

$$\begin{aligned} \sum_{\substack{A_1 \cup A_2 = A \\ |A_1| = d, |A_2| = |A| - d}} \frac{\mathcal{R}(A_2, B)\mathcal{R}(X, A_1)}{\mathcal{R}(A_2, A_1)} &= \\ &= (-1)^{(|A|-d)s}\ \mathrm{coeff}_{y_1^{|A|-d} \cdots y_s^{|A|-d}} \left(\sum_{\substack{A_1 \cup A_2 = A \\ |A_1| = d, |A_2| = |A| - d}} \frac{\mathcal{R}(A_2, B \cup Y)\mathcal{R}(X, A_1)}{\mathcal{R}(A_2, A_1)} \right) \\ &= (-1)^{(|A|-d)s}\ \mathrm{coeff}_{y_1^{|A|-d} \cdots y_s^{|A|-d}}\ \mathcal{R}(X, B \cup Y) = 0, \end{aligned}$$

dado que, en este caso, la hipótesis $|X| \leq |A| + |B| - 2d$ junto con $|B| < d$, implica que $|X| < |A| - d$, y por lo tanto no hay coeficiente en los y_i de grado $|A| - d$. □

La siguiente es una observación original de esta tesis.

Observación 2.2.3. La cota $|X| \leq |A| + |B| - 2d$ en el Teorema 2.2.2, cuando $|A|, |B| \geq d$, es óptima. En efecto, si $|X| > |A| + |B| - 2d$, escribamos $X = Y_1 \cup Y_2 \cup Z$ con $|Y_1| = |A| - d$, $|Y_2| = |B| - d$ y $Z \neq \emptyset$. Así, definiendo

$$h(Y_1, Y_2, Z) = \sum_{\substack{A_1 \cup A_2 = A \\ |A_1| = d, |A_2| = |A| - d}} \frac{\mathcal{R}(A_2, B)\mathcal{R}(Y_1, A_1)\mathcal{R}(Y_2, A_1)\mathcal{R}(Z, A_1)}{\mathcal{R}(A_2, A_1)},$$

y

$$g(Y_1, Y_2, Z) = \sum_{\substack{B_1 \cup B_2 = B \\ |B_1|=d,\, |B_2|=|B|-d}} \frac{\mathcal{R}(A, B_2)\mathcal{R}(Y_1, B_1)\mathcal{R}(Y_2, B_1)\mathcal{R}(Z, B_1)}{\mathcal{R}(B_1, B_2)},$$

la igualdad del enunciado se satisface si, y sólo si, lo hace en todas las especializaciones $Y_1 = A_2 \subset A$, con $|A_2| = |A| - d$ y $Y_2 = B_2 \subset B$, con $|B_2| = |B| - d$. Luego de una sencilla operatoria, la condición que resulta es

$$\mathcal{R}(Z, A_1) = \pm\mathcal{R}(Z, B_1)$$

para todos $A_1 \subset A$, $|B_1| \subset B$, con $|A_1| = |B_1| = d$, que claramente no se cumple en general.

El Teorema 2.2.2 puede tener una interpretación incluso más simétrica y de sencilla formulación si pensamos a X como un conjunto de elementos y no de variables, y le damos un rol simétrico al de B. Enunciaremos esta observación olvidándonos del signo, lo cual facilita la comprensión. Esta observación también es original de esta tesis.

Observación 2.2.4. Sean A, B y C subconjuntos finitos de un cuerpo K, y sean $p, q \geq 0$ con $|A| = p + q$. Entonces

$$\sum_{\substack{A_1 \cup A_2 = A \\ |A_1|=p, |A_2|=q}} \frac{\mathcal{R}(A_1, B)\mathcal{R}(A_2, C)}{\mathcal{R}(A_1, A_2)} = \begin{cases} \pm \displaystyle\sum_{\substack{B_1 \cup B_2 = B \\ |B_1|=|B|-q, |B_2|=q}} \frac{\mathcal{R}(B_1, A)\mathcal{R}(B_2, C)}{\mathcal{R}(B_1, B_2)} & \text{si } |B| + p \geq |C| + q \\ \pm \displaystyle\sum_{\substack{C_1 \cup C_2 = C \\ |C_1|=|C|-p, |C_2|=p}} \frac{\mathcal{R}(C_1, A)\mathcal{R}(C_2, B)}{\mathcal{R}(C_1, C_2)} & \text{si } |B| + p \leq |C| + q, \end{cases}$$

donde, por convención, la suma es 0 si alguno de los subconjuntos que la indexa tiene cardinal negativo.

Demostración. Es inmediato aplicando el Teorema 2.2.2 tomando $X = C$ en el primer caso y $X = B$ y $B = C$ en el segundo. □

Esta observación nos dice que la suma del miembro izquierdo siempre puede reescribirse indexada en subconjuntos de otro conjunto. No se pide ninguna hipótesis al respecto. Y de hecho, en el caso $|B| + p = |C| + q$, se puede indexar en subconjuntos de cualquiera de los tres conjuntos. La posibilidad de cambiar los subconjuntos a través de los cuales tenemos escrita la suma nos será de gran utilidad por el hecho que mientras el conjunto involucrado aparezca sólo en el numerador, podrá ser reemplazado por un *multiconjunto*, esto es, podrá tener elementos repetidos y la expresión seguirá teniendo sentido. Así, por ejemplo, si bien la expresión de la izquierda de la Observación 2.2.4 no tiene sentido si A es un multiconjunto, pues se anularían algunos denominadores, sí lo tiene cualquiera de las otras dos. Es un método para, por ejemplo, cambiar los roles de los conjuntos para permitir elementos repetidos en algunos de ellos. En los Capítulos 4 y 5 explotaremos este hecho.

Ahora presentaremos una extensión, original de esta tesis, del Teorema 2.2.2 a mayor cantidad de conjuntos de variables.

Teorema 2.2.5. *Sean $p, q \geq 0$ y $d := p + q$. Sean $A, B \subset K$ finitos con $|A| \geq d$, y sean X y Y dos conjuntos de variables tales que*

$$|X| \leq |A| + |B| - d - p, \ |Y| \leq |A| + |B| - d - q.$$

Entonces

1. *Si $|B| \geq d$, se tiene*

$$\sum_{\substack{A_1 \cup A_2 \cup A_3 = A \\ |A_1|=p, |A_2|=q, |A_3|=|A|-d}} \frac{\mathcal{R}(A_3, B)\mathcal{R}(Y, A_2)\mathcal{R}(X, A_1)}{\mathcal{R}(A_3, A_1)\mathcal{R}(A_3, A_2)\mathcal{R}(A_1, A_2)}$$
$$= \sum_{\substack{B_1 \cup B_2 \cup B_3 = B \\ |B_1|=p, |B_2|=q, |B_3|=|B|-d}} \frac{\mathcal{R}(A, B_3)\mathcal{R}(Y, B_2)\mathcal{R}(X, B_1)}{\mathcal{R}(B_1, B_2)\mathcal{R}(B_1, B_3)\mathcal{R}(B_2, B_3)}.$$

2. *Si $|B| < d$, se tiene*

$$\sum_{\substack{A_1 \cup A_2 \cup A_3 = A \\ |A_1|=p, |A_2|=q, |A_3|=|A|-d}} \frac{\mathcal{R}(A_3, B)\mathcal{R}(Y, A_2)\mathcal{R}(X, A_1)}{\mathcal{R}(A_3, A_1)\mathcal{R}(A_3, A_2)\mathcal{R}(A_1, A_2)} = 0.$$

Demostración. La suma del miembro izquierdo de la igualdad puede reescribirse como

$$\sum_{\substack{A_2 \cup A' = A \\ |A_2|=q, |A'|=|A|-q}} \ \sum_{\substack{A_1 \cup A_3 = A' \\ |A_1|=p, |A_3|=|A|-d}} \frac{\mathcal{R}(A_3, B)\mathcal{R}(Y, A_2)\mathcal{R}(X, A_1)}{\mathcal{R}(A_3, A_1)\mathcal{R}(A', A_2)}$$

$$= \sum_{\substack{A_2 \cup A' = A \\ |A_2|=q, |A'|=|A|-q}} \frac{\mathcal{R}(Y, A_2)}{\mathcal{R}(A', A_2)} \sum_{\substack{A_1 \cup A_3 = A' \\ |A_1|=p, |A_3|=|A|-d}} \frac{\mathcal{R}(A_3, B)\mathcal{R}(X, A_1)}{\mathcal{R}(A_3, A_1)}$$

$$= \sum_{\substack{A_2 \cup A' = A \\ |A_2|=q, |A'|=|A|-q}} \frac{\mathcal{R}(Y, A_2)}{\mathcal{R}(A', A_2)} \sum_{\substack{B_1 \cup B' = B \\ |B_1|=p, |B'|=|B|-p}} \frac{\mathcal{R}(A', B')\mathcal{R}(X, B_1)}{\mathcal{R}(B_1, B')} \tag{2.3}$$

$$= \sum_{\substack{B_1 \cup B' = B \\ |B_1|=p, |B'|=|B|-p}} \frac{\mathcal{R}(X, B_1)}{\mathcal{R}(B_1, B')} \sum_{\substack{A_2 \cup A' = A \\ |A_2|=q, |A'|=|A|-q}} \frac{\mathcal{R}(A', B')\mathcal{R}(Y, A_2)}{\mathcal{R}(A', A_2)}$$

$$= \sum_{\substack{B_1 \cup B' = B \\ |B_1|=p, |B'|=|B|-p}} \frac{\mathcal{R}(X, B_1)}{\mathcal{R}(B_1, B')} \sum_{\substack{B_2 \cup B_3 = B' \\ |B_2|=q, |B_3|=|B|-d}} \frac{\mathcal{R}(A, B_3)\mathcal{R}(Y, B_2)}{\mathcal{R}(B_2, B_3)} \tag{2.4}$$

$$= \sum_{\substack{B_1 \cup B_2 \cup B_3 = B \\ |B_1|=p, |B_2|=q, |B_3|=|B|-d}} \frac{\mathcal{R}(A, B_3)\mathcal{R}(Y, B_2)\mathcal{R}(X, B_1)}{\mathcal{R}(B_1, B_2)\mathcal{R}(B_1, B_3)\mathcal{R}(B_2, B_3)},$$

donde la igualdad (2.3) es el Teorema 2.2.2 aplicado a A', B y X, dado que $|X| \leq |A| + |B| - d - p = |A'| + |B| - 2p$; y la igualdad (2.4) es el mismo teorema aplicado a A, B' y Y, dado que $|Y| \leq |A| + |B| - d - q = |A| + |B'| - 2q$. Esto prueba (1) para $|B| \geq d$. Cuando $|B| < d$, se obtiene 0, también por el mismo teorema. □

Observemos que el Teorema 2.2.5 extiende el Teorema 2.2.2, pues este último es el caso $q = 0$ del primero.

Así como lo hicimos en la Observación 2.2.4, el Teorema 2.2.5 también puede tener una interpretación simétrica y sencilla en términos de conjuntos como lo vemos en la siguiente observación.

Observación 2.2.6. Sean A, B, C y D subconjuntos finitos de un cuerpo K, y sean $p, q, r \geq 0$ con $|A| = p + q + r$. Sea $m = \max\{|B| + p, |C| + q, |D| + r\}$. Entonces

$$\sum_{\substack{A_1 \cup A_2 \cup A_3 = A \\ |A_1|=p, |A_2|=q, |A_3|=r}} \frac{\mathcal{R}(A_1, B)\mathcal{R}(A_2, C)\mathcal{R}(A_3, D)}{\mathcal{R}(A_1, A_2)\mathcal{R}(A_1, A_3)\mathcal{R}(A_2, A_3)}$$

$$= \begin{cases} \pm \displaystyle\sum_{\substack{B_1 \cup B_2 \cup B_3 = A \\ |B_1|=|B|-q-r, |B_2|=q, |B_3|=r}} \frac{\mathcal{R}(B_1, A)\mathcal{R}(B_2, C)\mathcal{R}(B_3, D)}{\mathcal{R}(B_1, B_2)\mathcal{R}(B_1, B_3)\mathcal{R}(B_2, B_3)} & \text{si } m = |B| + p \\ \pm \displaystyle\sum_{\substack{C_1 \cup C_2 \cup C_3 = C \\ |C_1|=|C|-p-r, |C_2|=p, |C_3|=r}} \frac{\mathcal{R}(C_1, A)\mathcal{R}(C_2, B)\mathcal{R}(C_3, D)}{\mathcal{R}(C_1, C_2)\mathcal{R}(C_1, C_3)\mathcal{R}(C_2, C_3)} & \text{si } m = |C| + q \\ \pm \displaystyle\sum_{\substack{D_1 \cup D_2 \cup D_3 = D \\ |D_1|=|D|-p-q, |C_2|=p, |C_3|=q}} \frac{\mathcal{R}(D_1, A)\mathcal{R}(D_2, B)\mathcal{R}(B_3, C)}{\mathcal{R}(D_1, D_2)\mathcal{R}(D_1, D_3)\mathcal{R}(D_2, D_3)} & \text{si } m = |D| + r, \end{cases}$$

donde la suma es 0 si alguno de los subconjuntos que la indexa tiene cardinal negativo.

Demostración. Es inmediato aplicando el Teorema 2.2.5 tomando $Y = C$ y $X = D$ en el primer caso y análogamente en los otros dos. □

Queda claro que, con un proceso inductivo, se podría incluso extender el Teorema 2.2.5 y la Observación 2.2.6 a una cantidad arbitraria de conjuntos de variables.

Algunas de estas identidades tienen una interpretación interesante en ciertos casos particulares. Precisamente, el Teorema 2.2.2 (1) y el Teorema 2.2.5 (1), para el caso $|B| = d$, pueden verse como un proceso de agregar en la expresión un conjunto superfluo A suficientemente grande mostrando, en particular, que la suma no depende de A, sino sólo de su tamaño:

Observación 2.2.7. Sean B un subconjunto finito de un cuerpo K y X un conjunto de variables.

1. Si A es otro subconjunto de K con $|A| \geq |B| + |X|$, entonces

$$\mathcal{R}(X, B) = \sum_{\substack{A_1 \cup A_2 = A \\ |A_1|=|B|, |A_2|=|A|-|B|}} \frac{\mathcal{R}(A_2, B)\mathcal{R}(X, A_1)}{\mathcal{R}(A_2, A_1)}.$$

2. Sean Y otro conjunto de variables y $p, q \geq 0$ tales que $|B| = p + q$. Si A es otro subconjunto de K con $|A| \geq \max\{|X| + p, |Y| + q, |B|\}$, entonces

$$\sum_{\substack{B_1 \cup B_2 = B \\ |B_1|=p, |B_2|=q}} \frac{\mathcal{R}(Y, B_2)\mathcal{R}(X, B_1)}{\mathcal{R}(B_1, B_2)} = \sum_{\substack{A_1 \cup A_2 \cup A_3 = A \\ |A_1|=p, |A_2|=q, |A_3|=|A|-|B|}} \frac{\mathcal{R}(A_3, B)\mathcal{R}(Y, A_2)\mathcal{R}(X, A_1)}{\mathcal{R}(A_3, A_1)\mathcal{R}(A_3, A_2)\mathcal{R}(A_1, A_2)}.$$

El caso (2) de esta observación se encuentra en [DKSV2017, Prop. 2.1]. Éste es otro recurso en la misma dirección de la Observación 2.2.4, reescribiendo una suma en términos de subconjuntos de otro conjunto para poder permitir multiplicidades. Por ejemplo, en la Observación 2.2.7 (2), mientras que la expresión de la izquierda no tiene sentido si B es un multiconjunto, la expresión de la derecha sí lo tiene. Además aquí se puede explotar fuertemente el hecho que el conjunto A auxiliar es cualquiera mientras tenga tamaño suficientemente grande. Esto también lo aprovecharemos en los Capítulos 4 y 5.

Notemos también que esta última observación puede entenderse como una generalización del proceso de escribir a un polinomio simétrico vía interpolación, que es lo que dice la Proposición 2.1.4. En efecto, la Observación 2.2.7 (1) en el caso $|A| = |B| + |X|$ es exactamente la Proposición 2.1.4 aplicada al polinomio $h = \mathcal{R}(X, B)$, interpolando en los puntos del conjunto A. Más aún, la Observación 2.2.7 (1) también puede generalizarse a cualquier polinomio simétrico, extendiendo en algún sentido la Proposición 2.1.4. Tanto el siguiente lema, como todos los resultados del resto del capítulo, son originales de esta tesis.

Lema 2.2.8. *Sean K un cuerpo y X un conjunto de variables. Sea G un polinomio de $K[X]$ simétrico con grado acotado por n en cada variable; es decir, $h \in S_{(|X|,n)}$. Si A es un conjunto tal que $|A| \geq n + |X|$, entonces*

$$G(X) = \sum_{\substack{A_1 \cup A_2 = A \\ |A_1|=|A|-|X|, |A_2|=|X|}} \frac{G(A_2)\mathcal{R}(X, A_1)}{\mathcal{R}(A_2, A_1)}.$$

Demostración. Llamemos $r := |X|$. La idea será agrandar el grado n para estar en las hipótesis de la Proposición 2.1.4, con el recurso de agregar variables que ya hemos usado. Justamente, si $|A| = n+r$, el resultado vale por dicha proposición. Supongamos $|A| > n+r$ y llamemos $s := |A| - n - r$. Sea $Y = (y_1, \ldots, y_s)$ y definamos $H(X) := G(X)\mathcal{R}(Y, X) \in S_{(r,n+s)}$. Entonces

$$G(X) = \operatorname{coeff}_{y_1^r \cdots y_s^r}(H(X)) = \operatorname{coeff}_{y_1^r \cdots y_s^r} \left(\sum_{\substack{A' \subset A \\ |A'|=n+s}} H(A \backslash A') \frac{\mathcal{R}(X, A')}{\mathcal{R}(A \backslash A', A')} \right) \tag{2.5}$$

$$= \operatorname{coeff}_{y_1^r \cdots y_s^r} \left(\sum_{\substack{A' \subset A \\ |A'|=|A|-r}} G(A \backslash A')\mathcal{R}(Y, A \backslash A') \frac{\mathcal{R}(X, A')}{\mathcal{R}(A \backslash A', A')} \right)$$

$$= \sum_{\substack{A' \subset A \\ |A'|=|A|-r}} G(A \backslash A') \frac{\mathcal{R}(X, A')}{\mathcal{R}(A \backslash A', A')},$$

usando en (2.5) la Proposición 2.1.4 para $H \in S_{(r,n+s)}$. □

Este lema generaliza en efecto la Observación 2.2.7 (1), ya que el Lema 2.2.8 en el caso $G(X) = \mathcal{R}(X, B)$ implica la Observación 2.2.7 (1) si se intercambian en esta observación los roles de X y de B. Por otro lado el Lema 2.2.8 relaja la hipótesis para el tamaño de A respecto de la Proposición 2.1.4, pero en esta escritura no hay unicidad como en dicha proposición.

Ahora veremos una generalización del Teorema 2.2.2 en otro sentido y que también nos será de gran utilidad en el Capítulo 5.

Proposición 2.2.9. *Sea $d \geq 0$. Sean A y B subconjuntos finitos de un cuerpo K con $|A| \geq d$, y sean X' y X'' dos conjuntos de variables tales que* $\max\{|X'|, |X''|\} \leq |A| + |B| - 2d$. *Entonces, para cada $p, q \geq 0$ tales que $p + q = d$, se tiene*

1. *Si $|B| \geq d$, entonces*

$$\sum_{\substack{A'_1 \cup A''_1 \cup A_2 = A \\ |A'_1|=p,\, |A''_1|=q \\ |A_2|=|A|-d}} \frac{\mathcal{R}(A_2, B)\mathcal{R}(X', A'_1)\mathcal{R}(X'', A''_1)}{\mathcal{R}(A_2, A'_1 \cup A''_1)}$$

$$= (-1)^{p(|A|-d)} \sum_{\substack{A' \cup A'' = A \\ |A'|=p, |A''|=|A|-p}} \sum_{\substack{B' \cup B'' = B \\ |B'|=q,\, |B''|=|B|-q}} \frac{\mathcal{R}(A', B')\mathcal{R}(A'', B'')\mathcal{R}(X', A')\mathcal{R}(X'', B')}{\mathcal{R}(A', A'')\mathcal{R}(B', B'')}$$

$$= \sum_{\substack{B'_1 \cup B''_1 \cup B_2 = B \\ |B'_1|=p, |B''_1|=q, \\ |B_2|=|B|-d}} \frac{\mathcal{R}(A, B_2)\mathcal{R}(X', B'_1)\mathcal{R}(X'', B''_1)}{\mathcal{R}(B'_1 \cup B''_1, B_2)}.$$

2. *Si $|B| < d$, entonces*

$$\sum_{\substack{A'_1 \cup A''_1 \cup A_2 = A \\ |A'_1|=p, |A''_1|=q \\ |A_2|=|A|-d}} \frac{\mathcal{R}(A_2, B)\mathcal{R}(X', A'_1)\mathcal{R}(X'', A''_1)}{\mathcal{R}(A_2, A'_1 \cup A''_1)} = 0.$$

Demostración. (1) Multiplicando y dividiendo por $\mathcal{R}(A'_1, A''_1)$ y llamando $A' := A'_1$ y $A'' := A''_1 \cup A_2$, tenemos

$$\sum_{\substack{A'_1 \cup A''_1 \cup A_2 = A \\ |A'_1|=p, |A''_1|=q \\ |A_2|=|A|-d}} \frac{\mathcal{R}(A_2, B)\mathcal{R}(X', A'_1)\mathcal{R}(X'', A''_1)}{\mathcal{R}(A_2, A'_1 \cup A''_1)}$$

$$= (-1)^{pq} \sum_{\substack{A'\cup A''=A\\ |A'|=p,|A''|=|A|-p}} \frac{\mathcal{R}(X',A')}{\mathcal{R}(A'',A')} \sum_{\substack{A_1''\cup A_2=A''\\ |A_1''|=q,\,|A_2|=|A|-d}} \frac{\mathcal{R}(A_2,B)\mathcal{R}(X''\cup A',A_1'')}{\mathcal{R}(A_2,A_1'')}$$

$$= (-1)^{pq} \sum_{\substack{A'\cup A''=A\\ |A'|=p,|A''|=|A|-p}} \frac{\mathcal{R}(X',A')}{\mathcal{R}(A'',A')} \sum_{\substack{B'\cup B''=B\\ |B'|=q,\,|B''|=|B|-q}} \frac{\mathcal{R}(A'',B'')\mathcal{R}(X''\cup A',B')}{\mathcal{R}(B',B'')} \tag{2.6}$$

$$= (-1)^{p(|A|-d)} \sum_{\substack{A'\cup A''=A\\ |A'|=p,|A''|=|A|-p}} \sum_{\substack{B'\cup B''=B\\ |B'|=q,\,|B''|=|B|-q}} \frac{\mathcal{R}(A',B')\mathcal{R}(A'',B'')\mathcal{R}(X',A')\mathcal{R}(X'',B')}{\mathcal{R}(A',A'')\mathcal{R}(B',B'')} \tag{2.7}$$

$$= (-1)^{p(|A|-d)+pq+p(|A|-p)} \sum_{\substack{B'\cup B''=B\\ |B'|=q,\,|B''|=|B|-q}} \frac{\mathcal{R}(X'',B')}{\mathcal{R}(B',B'')} \sum_{\substack{A'\cup A''=A\\ |A'|=p,|A''|=|A|-p}} \frac{\mathcal{R}(A'',B'')\mathcal{R}(X'\cup B',A')}{\mathcal{R}(A'',A')}$$

$$= \sum_{\substack{B_1''\cup B''=B\\ |B_1''|=q,\,|B''|=|B|-q}} \frac{\mathcal{R}(X'',B_1'')}{\mathcal{R}(B_1'',B'')} \sum_{\substack{B_1'\cup B_2=B''\\ |B_1'|=p,|B_2|=|B''|-p}} \frac{\mathcal{R}(A,B_2)\mathcal{R}(X'\cup B_1'',B_1')}{\mathcal{R}(B_1',B_2)} \tag{2.8}$$

$$= \sum_{\substack{B_1'\cup B_1''\cup B_2=B\\ |B_1'|=p,|B_1''|=q,\\ |B_2|=|B|-d}} \frac{\mathcal{R}(A,B_2)\mathcal{R}(X',B_1')\mathcal{R}(X'',B_1'')}{\mathcal{R}(B_1'\cup B_1'',B_2)}.$$

donde la igualdad (2.6) se sigue del Teorema 2.2.2 dado que $|X''\cup A'| = |X''| + p \leq |A| + |B| - 2d + p \leq |A''| + |B| - p - 2q \leq |A''| + |B| - 2q$ y $|B| \geq d \geq q$, y la igualdad (2.8) es consecuencia del mismo resultado, pues $|X'\cup B'| = |X'| + q \leq |A| + |B| - 2d + q \leq |A| + |B| - 2p - q \leq |A| + |B''| - 2p$ y $|B''| = |B| - q \geq p$. La identidad (2.7) prueba la igualdad intermedia.

(2) Si $|B| < d$, considerando los casos $|B| < q$ y $|B| \geq q$, que en cuyo último caso $|B''| < p$, ambas posibilidades resultan dar 0 en la identidad (2.6) y (2.8) respectivamente. □

Observemos que en la Proposición 2.2.9, si tomamos $X' = X'' =: X$ recuperamos el Teorema 2.2.2, pues

$$\sum_{\substack{A_1'\cup A_1''\cup A_2=A\\ |A_1'|=p,\,|A_1''|=q\\ |A_2|=|A|-d}} \frac{\mathcal{R}(A_2,B)\mathcal{R}(X,A_1')\mathcal{R}(X,A_1'')}{\mathcal{R}(A_2,A_1'\cup A_1'')} = \binom{d}{p} \sum_{\substack{A_1\cup A_2=A\\ |A_1|=d,|A_2|=|A|-d}} \frac{\mathcal{R}(A_2,B)\mathcal{R}(X,A_1)}{\mathcal{R}(A_2,A_1)},$$

y el mismo factor aparece en la tercera expresión del enunciado. Esto muestra que esta proposición es en efecto una leve generalización del Teorema 2.2.2.

La Proposición 2.2.9 también admite, en el caso $|B| = d$, una interpretación como la de la Observación 2.2.7:

Observación 2.2.10. Sea B un subconjunto finito de un cuerpo K. Sean X' y X'' dos conjuntos finitos de variables y $p, q \geq 0$ tales que $|B| = p + q$. Si A es otro subconjunto

finito de K tal que $|A| \geq \max\{|X'|+|B|, |X''|+|B|\}$, entonces

$$\sum_{\substack{B'\cup B''=B\\ |B'|=p,\,|B''|=q}} \mathcal{R}(X',B')\mathcal{R}(X'',B'') = \sum_{\substack{A_1'\cup A_1''\cup A_2=A\\ |A_1'|=p,\,|A_1''|=q,|A_2|=|A|-|B|}} \frac{\mathcal{R}(A_2,B)\mathcal{R}(X',A_1')\mathcal{R}(X'',A_1'')}{\mathcal{R}(A_2,A_1'\cup A_1'')}.$$

Así como el Teorema 2.2.5 es una extensión del Teorema 2.2.2 a mayor cantidad de variables, la Proposición 2.2.9 también puede extenderse del mismo modo. Como no necesitaremos dicha extensión con tal generalidad, sólo enunciaremos su caso particular $|B| = d$. De modo que puede verse directamente como una extensión de la Observación 2.2.10.

Proposición 2.2.11. *Sea B un subconjunto finito de un cuerpo K. Sean X', X'' y Y, tres conjuntos finitos de variables y $p, q \geq 0$ tales que $|B| = p+q$. Si A es otro subconjunto finito de K tal que $|A| \geq \max\{|X'|+p, |X''|+p, |Y|+q, |B|\}$, entonces, para cada $p', p'' \geq 0$ tales que $p'+p''=p$, se tiene*

$$\sum_{\substack{B_1'\cup B_1''\cup B_2=B\\ |B_1'|=p',|B_1''|=p'',|B_2|=q}} \frac{\mathcal{R}(Y,B_2)\mathcal{R}(X',B_1')\mathcal{R}(X'',B_1'')}{\mathcal{R}(B_1'\cup B_1'',B_2)}$$
$$= \sum_{\substack{A_1'\cup A_1''\cup A_2\cup A_3=A\\ |A_1'|=p',|A_1''|=p'',|A_2|=q,|A_3|=|A|-|B|}} \frac{\mathcal{R}(B,A_3)\mathcal{R}(Y,A_2)\mathcal{R}(X',A_1')\mathcal{R}(X'',A_1'')}{\mathcal{R}(A_1'\cup A_1'',A_2)\mathcal{R}(A_1'\cup A_1'',A_3)\mathcal{R}(A_2,A_3)}.$$

En particular, la suma del miembro derecho no depende del conjunto A si su cardinal es suficientemente grande.

Demostración. Partiendo del segundo miembro, llamemos $A'' = A_1'\cup A_1''\cup A_3$ y escribamos

$$\sum_{\substack{A_1'\cup A_1''\cup A_2\cup A_3=A\\ |A_1'|=p',|A_1''|=p'',|A_2|=q,|A_3|=|A|-|B|}} \frac{\mathcal{R}(B,A_3)\mathcal{R}(Y,A_2)\mathcal{R}(X',A_1')\mathcal{R}(X'',A_1'')}{\mathcal{R}(A_1'\cup A_1'',A_2)\mathcal{R}(A_1'\cup A_1'',A_3)\mathcal{R}(A_2,A_3)}$$
$$= \sum_{\substack{A_2\cup A''=A\\ |A_2|=q,|A''|=|A|-q}} \frac{\mathcal{R}(Y,A_2)}{\mathcal{R}(A'',A_2)} \sum_{\substack{A_1'\cup A_1''\cup A_3=A''\\ |A_1'|=p',|A_1''|=p'',|A_3|=|A|-|B|}} \frac{\mathcal{R}(A_3,B)\mathcal{R}(X',A_1')\mathcal{R}(X'',A_1'')}{\mathcal{R}(A_3,A_1'\cup A_1'')} \tag{2.9}$$
$$= \sum_{\substack{A_2\cup A''=A\\ |A_2|=q,|A''|=|A|-q}} \frac{\mathcal{R}(Y,A_2)}{\mathcal{R}(A'',A_2)} \sum_{\substack{B_1'\cup B_1''\cup B_2=B\\ |B_1'|=p',|B_1''|=p'',|B_2|=q}} \frac{\mathcal{R}(A'',B_2)\mathcal{R}(X',B_1')\mathcal{R}(X'',B_1'')}{\mathcal{R}(B_1'\cup B_1'',B_2)} \tag{2.10}$$
$$= \sum_{\substack{B_1'\cup B_1''\cup B_2=B\\ |B_1'|=p',|B_1''|=p'',|B_2|=q}} \frac{\mathcal{R}(X',B_1')\mathcal{R}(X'',B_1'')}{\mathcal{R}(B_1'\cup B_1'',B_2)} \sum_{\substack{A_2\cup A''=A\\ |A_2|=q,|A''|=|A|-q}} \frac{\mathcal{R}(A'',B_2)\mathcal{R}(Y,A_2)}{\mathcal{R}(A'',A_2)}$$
$$= \sum_{\substack{B_1'\cup B_1''\cup B_2=B\\ |B_1'|=p',|B_1''|=p'',|B_2|=q}} \frac{\mathcal{R}(Y,B_2)\mathcal{R}(X',B_1')\mathcal{R}(X'',B_1'')}{\mathcal{R}(B_1'\cup B_1'',B_2)}, \tag{2.11}$$

usando en (2.10) la Proposición 2.2.9(1), para $A = A''$ y $d = p$, pues $\max\{|X'|, |X''|\} \leq m-p = m-q+d-2p = |A''|+|B|-2p$; y en (2.11) el Teorema 2.2.2 para $B = B_2$, $X = Y$ y $d = q$, en efecto $|Y| \leq |A| - q = |A| + |B_2| - 2q$, que se da en el caso límite $|B_2| = q$. Observemos además que en (2.9) hicimos varios cambios de signos que se compensan. □

Efectivamente la Proposición 2.2.11 extiende la Observación 2.2.10, pues esta última es el caso $q = 0$ de la primera.

Para terminar este capítulo observaremos cómo algunas de las sumas con las que hemos trabajado pueden escribirse a través de expresiones determinantales. Recordemos, para un conjunto ordenado $A = (\alpha_1, \ldots, \alpha_m)$, la *matriz de Vandermonde* definida por

$$\mathcal{V}(A) := \begin{pmatrix} \alpha_1^{m-1} & \ldots & \alpha_m^{m-1} \\ \vdots & & \vdots \\ 1 & \ldots & 1 \end{pmatrix}. \tag{2.12}$$

Es conocido que: $V(A) = \det(\mathcal{V}(A)) = \prod_{1 \leq i < j \leq m}(\alpha_i - \alpha_j)$. Tenemos entonces la siguiente formulación matricial.

Observación 2.2.12. Sean K un cuerpo y $A = \{\alpha_1, \ldots, \alpha_m\} \subset K$. Sea $0 \leq d \leq m$ y sean X y Y dos conjuntos de variables. Entonces

$$\sum_{\substack{A_1 \cup A_2 = A \\ |A_1| = d, |A_2| = m-d}} \frac{\mathcal{R}(Y, A_2)\mathcal{R}(X, A_1)}{\mathcal{R}(A_1, A_2)} = \frac{1}{V(A)} \cdot \det \begin{array}{|ccc|} \multicolumn{3}{c}{\overset{m}{}} \\ \hline \alpha_1^{d-1}\mathcal{R}(X, \alpha_1) & \ldots & \alpha_m^{d-1}\mathcal{R}(X, \alpha_m) \\ \vdots & & \vdots \\ \mathcal{R}(X, \alpha_1) & \ldots & \mathcal{R}(X, \alpha_m) \\ \hline \alpha_1^{m-d-1}\mathcal{R}(Y, \alpha_1) & \ldots & \alpha_m^{m-d-1}\mathcal{R}(Y, \alpha_m) \\ \vdots & & \vdots \\ \mathcal{R}(Y, \alpha_1) & \ldots & \mathcal{R}(Y, \alpha_m) \\ \hline \end{array} \begin{matrix} \\ \\ d \\ \\ \\ \\ m-d \end{matrix}.$$

Demostración. Desarrollando por el primer bloque de d filas y el segundo bloque de $m-d$ filas el determinante del miembro derecho de la igualdad es fácil ver que

$$\det \begin{array}{|ccc|} \multicolumn{3}{c}{\overset{m}{}} \\ \hline \alpha_1^{d-1}\mathcal{R}(X, \alpha_1) & \ldots & \alpha_m^{d-1}\mathcal{R}(X, \alpha_m) \\ \vdots & & \vdots \\ \mathcal{R}(X, \alpha_1) & \ldots & \mathcal{R}(X, \alpha_m) \\ \hline \alpha_1^{m-d-1}\mathcal{R}(Y, \alpha_1) & \ldots & \alpha_m^{m-d-1}\mathcal{R}(Y, \alpha_m) \\ \vdots & & \vdots \\ \mathcal{R}(Y, \alpha_1) & \ldots & \mathcal{R}(Y, \alpha_m) \\ \hline \end{array} \begin{matrix} \\ \\ d \\ \\ \\ \\ m-d \end{matrix}$$

$$= \sum_{\substack{A_1 \cup A_2 = A \\ |A_1| = d, |A_2| = m-d}} \operatorname{sg}(A_1, A_2)\mathcal{R}(Y, A_2)\mathcal{R}(X, A_1)V(A_1)V(A_2),$$

donde $\operatorname{sg}(A_1, A_2) = (-1)^\sigma$, siendo σ el número de transposiciones que se necesitan para llevar el conjunto ordenado A al conjunto ordenado $A_1 \cup A_2$. La demostración concluye observando que dados A_1 y A_2 fijos, se tiene

$$V(A) = \operatorname{sg}(A_1, A_2)V(A_1 \cup A_2) = \operatorname{sg}(A_1, A_2)V(A_1)V(A_2)\mathcal{R}(A_1, A_2).$$

□

Como corolario obtenemos una versión matricial del Teorema 2.2.2(1), que no parecería sencilla de probar valiéndose sólo de propiedades de determinantes.

Corolario 2.2.13. *Sean K un cuerpo y $A = \{\alpha_1, \ldots, \alpha_m\}$, $B = \{\beta_1, \ldots, \beta_n\} \subset K$. Sean $0 \leq d \leq \min\{m, n\}$ y X un conjunto de variables con $|X| \leq m + n - 2d$. Entonces*

$$\frac{1}{V(A)} \cdot \det \begin{array}{|ccc|} \multicolumn{3}{c}{\overbrace{\phantom{\alpha_1^{d-1}\mathcal{R}(X,\alpha_1) \quad \ldots \quad \alpha_m^{d-1}\mathcal{R}(X,\alpha_m)}}^{m}} \\ \alpha_1^{d-1}\mathcal{R}(X,\alpha_1) & \ldots & \alpha_m^{d-1}\mathcal{R}(X,\alpha_m) \\ \vdots & & \vdots \\ \mathcal{R}(X,\alpha_1) & \ldots & \mathcal{R}(X,\alpha_m) \\ \hline \alpha_1^{m-d-1}\mathcal{R}(B,\alpha_1) & \ldots & \alpha_m^{m-d-1}\mathcal{R}(B,\alpha_m) \\ \vdots & & \vdots \\ \mathcal{R}(B,\alpha_1) & \ldots & \mathcal{R}(B,\alpha_m) \end{array} \begin{array}{l} \\ \\ d \\ \\ \\ m-d \end{array}$$

$$= (-1)^{(m-d)(n-d)} \frac{1}{V(B)} \cdot \det \begin{array}{|ccc|} \multicolumn{3}{c}{\overbrace{\phantom{\beta_1^{d-1}\mathcal{R}(X,\beta_1) \quad \ldots \quad \beta_n^{d-1}\mathcal{R}(X,\beta_n)}}^{n}} \\ \beta_1^{d-1}\mathcal{R}(X,\beta_1) & \ldots & \beta_n^{d-1}\mathcal{R}(X,\beta_n) \\ \vdots & & \vdots \\ \mathcal{R}(X,\beta_1) & \ldots & \mathcal{R}(X,\beta_n) \\ \hline \beta_1^{n-d-1}\mathcal{R}(A,\beta_1) & \ldots & \beta_n^{n-d-1}\mathcal{R}(A,\beta_n) \\ \vdots & & \vdots \\ \mathcal{R}(A,\beta_1) & \ldots & \mathcal{R}(A,\beta_n) \end{array} \begin{array}{l} \\ \\ d \\ \\ \\ n-d \end{array} .$$

Demostración. Es simplemente una reformulación del Teorema 2.2.2 usando la Observación 2.2.12 con $Y = B$ para el miembro izquierdo, con $A = B$, $Y = A$ para el miembro derecho, y mirando con cuidado el signo. □

De un modo más general, así como lo hicimos en el Teorema 2.2.5, también podemos escribir mediante una expresión determinantal una suma que involucra mayor cantidad de conjuntos de variables. La demostración es idéntica desarrollando esta vez el determinante por tres bloques de filas en lugar de dos:

Observación 2.2.14. Sean K un cuerpo y $A = \{\alpha_1, \ldots, \alpha_m\} \subset K$. Sean $p, q \geq 0$ y $d := p + q$ y sean X, Y y Z conjuntos de variables. Entonces

$$\sum_{\substack{A_1 \cup A_2 \cup A_3 = A \\ |A_1| = p, |A_2| = q, |A_3| = m-d}} \frac{\mathcal{R}(Z, A_3)\mathcal{R}(Y, A_2)\mathcal{R}(X, A_1)}{\mathcal{R}(A_1, A_2)\mathcal{R}(A_1, A_3)\mathcal{R}(A_2, A_3)}$$

$$= \frac{1}{V(A)} \cdot \det \begin{array}{|ccc|c} \multicolumn{3}{c}{\overset{m}{}} & \\ \alpha_1^{p-1}\mathcal{R}(X,\alpha_1) & \dots & \alpha_m^{p-1}\mathcal{R}(X,\alpha_m) & \\ \vdots & & \vdots & p \\ \mathcal{R}(X,\alpha_1) & \dots & \mathcal{R}(X,\alpha_m) & \\ \hline \alpha_1^{q-1}\mathcal{R}(Y,\alpha_1) & \dots & \alpha_m^{q-1}\mathcal{R}(Y,\alpha_m) & \\ \vdots & & \vdots & q \\ \mathcal{R}(Y,\alpha_1) & \dots & \mathcal{R}(Y,\alpha_m) & \\ \hline \alpha_1^{m-d-1}\mathcal{R}(Z,\alpha_1) & \dots & \alpha_m^{m-d-1}\mathcal{R}(Z,\alpha_m) & \\ \vdots & & \vdots & m-d \\ \mathcal{R}(Z,\alpha_1) & \dots & \mathcal{R}(Z,\alpha_m) & \\ \hline \end{array} .$$

Capítulo 3

Otra demostración del Teorema 1.2.6

En este capítulo mostramos la primera aplicación del lema de intercambio. En el Teorema 1.2.6 se da la descripción completa de las sumas dobles $\mathrm{Syl}_{p,q}(A,B)(x)$ para todos los posibles valores de p y q. En particular, se obtiene la relación entre las subresultantes y las sumas de Sylvester. Aquí daremos una demostración alternativa de dicho teorema de un modo natural desde el punto de vista de la interpolación simétrica y aplicando el lema de intercambio. Muchos autores han trabajado en la relación entre la suma simple $\mathrm{Syl}_{d,0}(A,B)(x)$ y la subresultante $\mathrm{Sres}_d(f,g)(x)$ en el caso $0 \leq d < \mathrm{mín}\{m,n\}$ o $d = \mathrm{mín}\{m,n\}$ si $m \neq n$, pero todas las descripciones que involucran las sumas dobles o los otros casos de p y q son mucho más complicadas y no muy naturales. En [DHKS2009], el Teorema 1.2.6 se obtiene vía el determinante de una intrincada expresión matricial, mientras que en [KrSz2012] se obtiene mediante una rigurosa inducción a partir de ciertos casos extremales. Daremos aquí una nueva demostración del Teorema 1.2.6 trabajando detalladamente cada caso de dicho teorema. Una de las grandes diferencias entre la demostración que damos en esta tesis y las anteriores demostraciones es que aquí mostramos una relación natural entre las sumas simples y las sumas dobles de Sylvester, sin pasar por la relación que tienen unas y otras con la subresultante.

En la Sección 3.1 trabajamos con la suma simple y en la Sección 3.2 con la sumas dobles mostrando, en particular, la relación entre éstas y las sumas simples. La mayoría de los resultados de este capítulo se encuentran en el trabajo [KSV2017]. Aclaramos en cada caso cuáles son aquellos que son originales de esta tesis.

3.1. Suma simple de Sylvester y subresultante

Para lograr la descripción del Teorema 1.2.6 trabajaremos primero con la suma simple. Probaremos con técnicas de interpolación simétrica y el lema de intercambio el caso particular del Teorema 1.2.5 y además describiremos el resultado de la suma simple para otros valores de d.

El primer resultado inmediato que obtenemos a partir del lema de intercambio es la

igualdad de la Proposición 1.2.4:

$$\mathrm{Syl}_{d,0}(A,B)(x) = (-1)^{d(m-d)}\mathrm{Syl}_{0,d}(A,B)(x).$$

Aquí la prueba, que difiere de la publicada en [KSV2017].

Demostración de la Proposición 1.2.4. La igualdad que queremos probar es exactamente

$$\sum_{A'\subset A,\,|A'|=d} \mathcal{R}(A\backslash A',B)\frac{\mathcal{R}(x,A')}{\mathcal{R}(A',A\backslash A')} = (-1)^{d(m-d)} \sum_{B'\subset B,\,|B'|=d} \mathcal{R}(A,B\backslash B')\frac{\mathcal{R}(x,B')}{\mathcal{R}(B',B\backslash B')},$$

y esto es una aplicación del lema incluso en su primera formulación: el Lema 2.2.1, para el caso $|X| = 1$. Sólo hay que acomodar el signo según la Observación 1.2.2. □

Notemos que, de hecho, el lema de intercambio puede interpretarse como una generalización de la igualdad $\mathrm{Syl}_{d,0}(A,B)(x) = (-1)^{d(m-d)}\mathrm{Syl}_{0,d}(A,B)(x)$ a mayor cantidad de variables.

La Proposición 1.2.4 nos permite trabajar indistintamente con cualquiera de las dos sumas simples. Por comodidad trabajaremos con la suma simple $\mathrm{Syl}_{0,d}(A,B)(x)$.

La idea principal para probar el Teorema 1.2.5 será llevar la suma $\mathrm{Syl}_{0,d}(A,B)(x)$ al contexto de la interpolación simétrica. Haremos esto agregando variables y luego recuperando la expresión tomando un coeficiente adecuado. Fijemos dos subconjutos A y B de un cuerpo K con $|A| = m$ y $|B| = n$. Definimos $f := \mathcal{R}(x,A)$ y $g := \mathcal{R}(x,B)$.

Notación 3.1.1. Sean $0 \le d \le n-1$ y $X := (x_1,\dots,x_{n-d})$. Definimos

$$\mathrm{MSyl}_{0,d}(A,B)(X) := (-1)^{(m-d)(n-d)} \sum_{B'\subset B,|B'|=d} \mathcal{R}(B\backslash B',A)\frac{\mathcal{R}(X,B')}{\mathcal{R}(B\backslash B',B')}.$$

Observación 3.1.2. Por la Proposición 2.1.4, $\mathrm{MSyl}_{0,d}(A,B)(X) \in S_{(n-d,d)}$ es el único polinomio de $S_{(n-d,d)}$ que satisface las $\binom{n}{d}$ condiciones

$$\mathrm{MSyl}_{0,d}(A,B)(B\backslash B') = (-1)^{(m-d)(n-d)}\mathcal{R}(B\backslash B',A) \text{ para todo } B'\subset B, |B'| = d.$$

En particular,

$$\mathrm{MSyl}_{0,d}(A,B)(X) = (-1)^{(m-d)(n-d)} f(x_1)\cdots f(x_{n-d}) \text{ si } m \le d. \tag{3.1}$$

La elección de la notación $\mathrm{MSyl}_{0,d}(A,B)(X)$ se refiere a *suma de Sylvester multivariada*, pues el polinomio coincide con $\mathrm{Syl}_{0,d}(A,B)(x)$ cuando $X = \{x\}$, es decir, $d = n-1$. O visto de otro modo, el segundo es un coeficiente del primero cuando hay más de una variable, o sea, $d < n-1$:

Observación 3.1.3. Sean $0 \le d \le n-1$ y $X := (x_1,\dots,x_{n-d})$. Entonces

$$\mathrm{Syl}_{0,d}(A,B)(x_{n-d}) = \begin{cases} \mathrm{coeff}_{x_1^d\cdots x_{n-d-1}^d}\big(\mathrm{MSyl}_{0,d}(A,B)(X)\big) & \text{si} \quad 0 \le d < n-1 \\ \mathrm{MSyl}_{0,d}(A,B)(x_{n-d}) & \text{si} \quad d = n-1. \end{cases}$$

Aquí, $\mathrm{coeff}_{x_1^d\cdots x_{n-d-1}^d}$ denota el coeficiente en $K[x_{n-d}]$ del monomio $x_1^d\cdots x_{n-d-1}^d$ de $\mathrm{MSyl}_{0,d}(A,B)(X)$.

Junto con (3.1), esto implica inmediatamente el siguiente corolario.

Corolario 3.1.4. *Sea $0 \leq d \leq n-1$. Si $m \leq d$ entonces*

$$\mathrm{Syl}_{0,d}(A,B)(x) = \begin{cases} 0 & si \quad m < d < n-1 \\ (-1)^{(m-d)(n-d)}\, f & si \quad m < d = n-1 \ o \ m = d \leq n-1. \end{cases}$$

Vamos a calcular $\mathrm{Syl}_{0,d}(A,B)(x)$ para el caso restante $d \leq m$ de dos formas parecidas. Aquí la primera que está publicada en [KSV2017], presentando una formulación matricial para el polinomio $\mathrm{MSyl}_{0,d}(A,B)(X)$.

Proposición 3.1.5. *Sean $0 \leq d \leq \min\{n-1, m\}$ y $X := (x_1, \ldots, x_{n-d})$. El polinomio $\mathrm{MSyl}_{0,d}(A,B)(X)$ de la Notación 3.1.1 satisface la siguiente expresión determinantal:*

$$\mathrm{MSyl}_{0,d}(A,B)(X) = \frac{1}{V(X)} \cdot \det \begin{array}{|cccccc|ccc|l} \multicolumn{6}{c|}{\overbrace{}^{m-d}} & \multicolumn{3}{c|}{\overbrace{}^{n-d}} & \\ a_m & \cdots & & \cdots & a_{d+1} & & x_1^{n-d-1}f(x_1) & \cdots & x_{n-d}^{n-d-1}f(x_{n-d}) & \\ & \ddots & & & \vdots & & \vdots & & \vdots & n-d \\ & & a_m & \cdots & a_n & & f(x_1) & \cdots & f(x_{n-d}) & \\ \hline b_n & \cdots & & \cdots & b_{n-(m-d-1)} & & x_1^{m-d-1}g(x_1) & \cdots & x_{n-d}^{m-d-1}g(x_{n-d}) & \\ & & \ddots & & \vdots & & \vdots & & \vdots & m-d \\ & & & & b_n & & g(x_1) & \cdots & g(x_{n-d}) & \\ \end{array}.$$

Demostración. En virtud de la definición de $\mathrm{MSyl}_{0,d}(A,B)(X)$, basta que verifiquemos que la expresión del miembro derecho de la igualdad es un polinomio simétrico de grado acotado por d en cada variable x_k, y tal que al especializar en $(\beta_{i_1}, \ldots, \beta_{i_{n-d}})$, se obtiene $(-1)^{(m-d)(n-d)} f(\beta_{i_1}) \cdots f(\beta_{i_{n-d}})$, para cada $B' = \{\beta_{i_1}, \ldots, \beta_{i_{n-d}}\} \subset B$.

En efecto es un polinomio puesto que $V(X)$ divide al segundo factor: para cada $j > i$ el término $x_j - x_i$ de $V(X)$ divide al determinante de la matriz (haciendo $x_i = x_j$ es claro que se anula el determinante).

El polinomio es simétrico porque al permutar x_i con x_j cambia el signo tanto en el determinante de la matriz como en $V(X)$.

Mostremos ahora la cota del grado para x_1 que, por la simetría, será suficiente. Notemos $C(j)$ a la columna j-ésima de la matriz. Al hacer el reemplazo

$$C(m-d+1) \mapsto C(m-d+1) - x_1^{m+n-d-1}C(1) - \cdots - x_1^n C(m-d) =: C'(m-d+1)$$

el determinante no se altera. Pero tenemos

$$\begin{cases} C'(m-d+1)_1 = a_d x_1^{n-1} + \cdots \\ \qquad \vdots \\ C'(m-d+1)_{n-d} = a_{n-1}x_1^{n-1} + \cdots \\ C'(m-d+1)_{n-d+1} = b_{n-(m-d-1)-1}x_1^{n-1} + \cdots \\ \qquad \vdots \\ C'(n-d+1)_{m+n-2d} = b_{n-1}x_1^{n-1} + \cdots \end{cases}$$

De este modo el grado en x_1 del determinante de la matriz está acotado por $n-1$, mientras que el grado en x_1 de $V(X)$ es exactamente $n-d-1$, lo cual implica que el grado en x_1 del producto está acotado por $n-1-(n-d-1)=d$.

Por último, evaluemos el polinomio del miembro derecho en una $(n-d)$-upla $(\beta_{i_1},\dots,\beta_{i_{n-d}})$ para $1\le i_1<\cdots<i_{n-d}\le n$ fijos. Es claro que el determinante de la matriz da

$$(-1)^{(m-d)(n-d)}V(\beta_{i_1},\dots,\beta_{i_{n-d}})f(\beta_{i_1})\cdots f(\beta_{i_{n-d}}),$$

y dado que $V(X)$ da $V(\beta_{i_1},\dots,\beta_{i_{n-d}})$, esto concluye la demostración.

□

Notemos que la expresión de la Proposición 3.1.5 tiene una forma bastante similar a la definición matricial de la subresultante, de hecho, coinciden cuando $d=n-1$. Con esta perspectiva, el principal resultado que queremos probar en esta subsección resulta bastante natural y ya podemos hacerlo.

Proposición 3.1.6. *Sea* $0\le d\le n-1$. *Si* $d\le m$, *se tiene*

$$\mathrm{Syl}_{0,d}(A,B)(x)=\mathrm{Sres}_d(f,g)(x).$$

Demostración. Notemos $S(X)$ al determinante de la matriz del Teorema 3.1.5 y $c_d(x_{n-d})\in K[x_{n-d}]$ al coeficiente de $x_1^d\cdots x_{n-d-1}^d$ en $\mathrm{MSyl}_{0,d}(A,B)(X)$. Bastará probar que este último es igual a $\mathrm{Sres}_d(f,g)(x_{n-d})$, de acuerdo a la Observación 3.1.3.

Dado que $\mathrm{MSyl}_{0,d}(A,B)(X)=S(X)/V(X)$, tenemos

$$\begin{aligned}
S(X)&=\mathrm{MSyl}_{0,d}(A,B)(X)V(X)\\
&=(c_d(x_{n-d})\,x_1^d\cdots x_{n-d-1}^d+\cdots)(x_1^{n-d-1}x_2^{n-d-2}\cdots x_{n-d-1}+\cdots)\\
&=c_d(x_{n-d})\,x_1^{n-1}x_2^{n-2}\cdots x_{n-d-1}^{d+1}+\cdots
\end{aligned}$$

Por lo tanto,

$$c_d(x_{n-d})=\mathrm{coeff}_{x_1^{n-1}x_2^{n-2}\cdots x_{n-d-1}^{d+1}}(S(X)).$$

Es claro que el coeficiente de $x_1^{n-1}\cdots x_{n-d-1}^{d+1}$ en el determinante se obtiene, por multilinealidad, a partir del coeficiente del determinante de la matriz en donde la columna de x_1 tiene todos sus exponentes iguales a $n-1$, la columna de x_2 tiene todos sus exponentes iguales a $n-2$, y así sucesivamente hasta la columna de x_{n-d-1}, con exponentes iguales a $d+1$. Esto es, $\mathrm{coeff}_{x_1^{n-1}\cdots x_{n-d-1}^{d+1}}(S(X))$ es igual a

$$\det\left(\begin{array}{cccc|cccc}
\multicolumn{4}{c|}{\scriptstyle m-d} & \multicolumn{4}{c}{\scriptstyle n-d}\\
a_m & \cdots & \cdots & a_{d+1} & a_d & \cdots & a_{d+1-(n-d-1)} & x_{n-d}^{n-d-1}f(x_{n-d})\\
 & \ddots & & \vdots & \vdots & \vdots & & \vdots\\
 & & a_m\ \ \cdots & a_n & a_{n-1} & \cdots & a_{d+1} & f(x_{n-d})\\
\hline
b_n & \cdots & \cdots & b_{n-(m-d-1)} & b_{n-(m-d)} & \cdots & b_{d+1-(m-d-1)} & x_{n-d}^{m-d-1}g(x_{n-d})\\
 & & \ddots & \vdots & \vdots & \vdots & & \vdots\\
 & & & b_n & b_{n-1} & \cdots & b_{d+1} & g(x_{n-d})
\end{array}\right)\begin{array}{l}\\ \\ \scriptstyle n-d\\ \\ \\ \scriptstyle m-d\\ \\ \end{array}.$$

Luego,

$$\mathrm{coeff}_{x_1^{n-1}x_2^{n-2}\cdots x_{n-d-1}^{d+1}}(S(X))=\mathrm{Sres}_d(f,g)(x_{n-d}),$$

lo cual implica $c_d(x_{n-d})=\mathrm{Sres}_d(f,g)(x_{n-d})$, como queríamos probar. □

Juntando lo que probamos en el Corolario 3.1.4, la Proposición 3.1.6 y el valor de $\mathrm{Syl}_{0,d}(A,B)(x)$ para el caso $d=n$, esta técnica de interpolación nos ha permitido construir de un modo muy natural la descripción total de la suma simple de Sylvester $\mathrm{Syl}_{0,d}(A,B)(x)$ para todo $0 \leq d \leq n$ y cualquier m:

$$\mathrm{Syl}_{0,d}(A,B)(x) = \begin{cases} \mathrm{Sres}_d(f,g)(x) & \text{si} \quad 0 \leq d \leq \{m-1,n\} \text{ o } d=m<n \\ 0 & \text{si} \quad m<d<n-1 \\ (-1)^{m+n-1}f & \text{si} \quad m<d=n-1 \\ g & \text{si} \quad m \leq d=n. \end{cases}$$

Vamos a presentar ahora la segunda demostración de la Proposición 3.1.6, original de esta tesis. Usaremos directamente el lema de intercambio y la demostración resultará ser un poco más simétrica en cuanto a los roles de A y de B. La idea es la siguiente. Tenemos que $\mathrm{Syl}_{d,0}(A,B)(x)$ y $\mathrm{Syl}_{0,d}(A,B)(x)$ son sumas indexadas en subconjuntos de A y de B respectivamente. En la primera, el conjunto B aparece sólo en el numerador y sin particionar: $\mathcal{R}(A\backslash A', B)$, que puede escribirse en la forma $g(\alpha_1)\cdots g(\alpha_{m-d})$, mientras que el polinomio f no puede rescatarse en dicha suma. Análogamente, en $\mathrm{Syl}_{0,d}(A,B)(x)$ aparece en la escritura el polinomio f, pero no puede escribirse en términos de g. ¿Cómo lograr escribir la suma de modo que tanto A como B estén en el numerador y sin particionar para que la expresión quede escrita en términos de f y de g? Es decir, queremos escribirlo como una suma indexada en otros subconjuntos. Para eso el truco será agrandar de nuevo la variabe x, pero ahora lo suficiente como para que se cumplan las hipótesis del lema de intercambio y la suma pueda indexarse en subconjuntos de X.

Notación 3.1.7. Sean $0 \leq d \leq n-1$ y $X' := (x_1, \ldots, x_{m+n-2d})$. Definimos

$$\mathrm{MSyl}_{0,d}(A,B)(X') := \sum_{B' \subset B, |B'|=d} \mathcal{R}(A, B\backslash B') \frac{\mathcal{R}(X', B')}{\mathcal{R}(B', B\backslash B')}.$$

Aquí tenemos la misma situación de la Observación 3.1.3:

$$\mathrm{Syl}_{0,d}(A,B)(x_{m+n-2d}) = \begin{cases} \mathrm{coeff}_{x_1^d \cdots x_{m+n-2d-1}^d}\big(\mathrm{MSyl}_{0,d}(A,B)(X')\big) & \text{si} \quad 0 \leq d < n-1 \\ \mathrm{MSyl}_{0,d}(A,B)(x_{m+n-2d}) & \text{si} \quad d=m=n-1. \end{cases}$$

Se trata entonces de encontrar dicho coeficiente. Pero ahora tenemos la siguiente reescritura.

Lema 3.1.8.

$$\mathrm{MSyl}_{0,d}(A,B)(X') = (-1)^{(m+n-2d)d} \sum_{\substack{X_1 \cup X_2 = X' \\ |X_1|=n-d, |X_2|=m-d}} \frac{\mathcal{R}(B,X_2)\mathcal{R}(A,X_1)}{\mathcal{R}(X_1,X_2)}.$$

Demostración.

$$\begin{aligned}\mathrm{MSyl}_{0,d}(A,B)(X') &= \sum_{B'\subset B,|B'|=d} \mathcal{R}(A,B\backslash B')\frac{\mathcal{R}(X',B')}{\mathcal{R}(B',B\backslash B')}\\ &= (-1)^{(m+n-2d)d} \sum_{\substack{B_1\cup B_2=B\\ |B_1|=d,|B_2|=n-d}} \frac{\mathcal{R}(B_1,X')\mathcal{R}(A,B_2)}{\mathcal{R}(B_1,B_2)}\\ &= (-1)^{(m+n-2d)d} \sum_{\substack{X_1\cup X_2=X'\\ |X_1|=n-d,|X_2|=m-d}} \frac{\mathcal{R}(B,X_2)\mathcal{R}(A,X_1)}{\mathcal{R}(X_1,X_2)}, \qquad (3.2)\end{aligned}$$

usando en (3.2) el Teorema 2.2.2 con B en lugar de A, X' en lugar de B y A en lugar de X. En efecto, la hipótesis necesaria $|A| \leq |B|+|X'|-2(n-d)$ se cumple en las condiciones que impusimos. □

Aprovechando la formulación matricial de la Observación 2.2.12 tenemos la siguiente demostración alternativa de la Proposición 3.1.6.

Demostración alternativa de la Proposición 3.1.6. Tenemos

$$\mathrm{Syl}_{0,d}(A,B)(x_{m+n-2d}) = \mathrm{coeff}_{x_1^d\cdots x_{m+n-2d-1}^d}\big(\mathrm{MSyl}_{0,d}(A,B)(X')\big).$$

Pero por el Lema 3.1.8 y la Observación 2.2.12 resulta

$$\mathrm{MSyl}_{0,d}(A,B)(X') = (-1)^{(m+n-2d)d} \sum_{\substack{X_1\cup X_2=X'\\ |X_1|=n-d,|X_2|=m-d}} \frac{\mathcal{R}(B,X_2)\mathcal{R}(A,X_1)}{\mathcal{R}(X_1,X_2)}$$

$$= (-1)^{(m+n-2d)d}\frac{1}{V(X')}\cdot \det \begin{array}{|ccc|}\multicolumn{3}{c}{\overbrace{}^{m+n-2d}}\\ \hline x_1^{n-d-1}\mathcal{R}(A,x_1) & \dots & x_{m+n-2d}^{n-d-1}\mathcal{R}(A,x_{m+n-2d})\\ \vdots & & \vdots\\ \mathcal{R}(A,x_1) & \dots & \mathcal{R}(A,x_{m+n-2d})\\ \hline x_1^{m-d-1}\mathcal{R}(B,x_1) & \dots & x_{m+n-2d}^{m-d-1}\mathcal{R}(B,x_{m+n-2d})\\ \vdots & & \vdots\\ \mathcal{R}(B,x_1) & \dots & \mathcal{R}(B,x_{m+n-2d})\\ \hline \end{array} \begin{array}{l}\\ \\ n-d\\ \\ \\ m-d\end{array}$$

$$= \frac{1}{V(X')}\cdot \det \begin{array}{|ccc|}\multicolumn{3}{c}{\overbrace{}^{m+n-2d}}\\ \hline x_1^{n-d-1}f(x_1) & \dots & x_{m+n-2d}^{n-d-1}f(x_{m+n-2d})\\ \vdots & & \vdots\\ f(x_1) & \dots & f(x_{m+n-2d})\\ \hline x_1^{m-d-1}g(x_1) & \dots & x_{m+n-2d}^{m-d-1}g(x_{m+n-2d})\\ \vdots & & \vdots\\ g(x_1) & \dots & g(x_{m+n-2d})\\ \hline \end{array} \begin{array}{l}\\ \\ n-d\\ \\ \\ m-d\end{array}. \qquad (3.3)$$

Notemos que, si bien es claro, no tenemos que probar que este producto es efectivamente un polinomio como sí lo tuvimos que hacer con la expresión matricial de la primera demostración de la Proposición 3.1.6 que dimos, pues ya sabemos que coincide con

$\mathrm{MSyl}_{0,d}(A,B)(X')$. Queremos identificar en este polinomio el coeficiente $c_d(x_{m+n-2d})$ de $x_1^d \cdots x_{m+n-2d-1}^d$, pero del mismo modo que lo hicimos en la primera demostración de la Proposición 3.1.6, tenemos que

$$c_d(x_{m+n-2d}) = \mathrm{coeff}_{x_1^{m+n-d-1} x_2^{m+n-d-2} \cdots x_{m+n-2d-1}^{d+1}}(S(X')),$$

siendo $S(X')$ el polinomio del segundo factor de (3.3). Y como lo hicimos en dicha demostración, es claro que este coeficiente se obtiene, por multilinealidad, a partir del coeficiente del determinante de la matriz en donde la columna de x_1 tiene todos sus exponentes iguales a $m+n-d-1$, la columna de x_2 tiene todos sus exponentes iguales a $m+n-d-2$, y así sucesivamente hasta la columna de $x_{m+n-2d-1}$, con exponentes iguales a $d+1$. Esto es, $\mathrm{coeff}_{x_1^{m+n-d-1} x_2^{m+n-d-2} \cdots x_{m+n-2d-1}^{d+1}}(S(X'))$ es igual a

$$\det \begin{array}{c|cccccc} & & & & & \overset{m+n-2d}{\overbrace{}} & \\ a_m & \cdots & & \cdots & a_{d+1-(n-d-1)} & x_{m+n-2d}^{n-d-1} f(x_{m+n-2d}) & \\ & \ddots & & & \vdots & \vdots & \overset{n-d}{\overbrace{}} \\ & & a_m & \cdots & a_{d+1} & f(x_{m+n-2d}) & \\ \hline b_n & \cdots & & \cdots & b_{d+1-(m-d-1)} & x_{m+n-2d}^{m-d-1} g(x_{m+n-2d}) & \\ & \ddots & & & \vdots & \vdots & \overset{m-d}{\overbrace{}} \\ & & b_n & \cdots & b_{d+1} & g(x_{m+n-2d}) & \end{array},$$

que es lo que queríamos obtener. □

En el Capítulo 4 unificaremos las nociones de las Notaciones 3.1.1 y 3.1.7 y usaremos estas construcciones para otra aplicación.

3.2. Descripción de las sumas dobles de Sylvester

Ahora podremos dar nuestra demostración del Teorema 1.2.6 en su totalidad. Trabajaremos con las sumas dobles $\mathrm{Syl}_{p,q}(A,B)(x)$ y veremos cómo, mediante el lema de intercambio, todos los casos se reducen a expresiones que dependen de los casos extremales $\mathrm{Syl}_{0,d}(A,B)(x)$ y $\mathrm{Syl}_{m,d-m}(A,B)(x)$. Las demostraciones de esta sección difieren de las publicadas en [KSV2017] ya que usan herramientas del Capítulo 2 que fueron desarrolladas con posterioridad.

3.2.1. El caso $m+n \geq 2d+1$

Este caso se simplifica de manera inmediata con una de las versiones que vimos del lema de intercambio. La sumas dobles se reducen a sumas simples según el siguiente resultado.

Proposición 3.2.1. *Sean A y B dos subconjuntos de un cuerpo K, con $|A| = m$ y $|B| = n$. Sean $0 \leq p \leq m$, $0 \leq q \leq n$ y sea $d := p+q$. Supongamos que $m+n \geq 2d+1$ y $d \leq n$. Entonces*

$$\mathrm{Syl}_{p,q}(A,B)(x) = (-1)^{p(m-d)} \binom{d}{p} \mathrm{Syl}_{0,d}(A,B)(x).$$

Demostración. La igualdad que queremos probar es

$$\sum_{\substack{A'\subset A,\, B'\subset B\\ |A'|=p,\,|B'|=q}} \mathcal{R}(A',B')\,\mathcal{R}(A\backslash A',B\backslash B')\,\frac{\mathcal{R}(x,A')\,\mathcal{R}(x,B')}{\mathcal{R}(A',A\backslash A')\,\mathcal{R}(B',B\backslash B')}$$

$$= (-1)^{p(m-d)}\binom{d}{p}\sum_{B'\subset B,\,|B'|=d}\mathcal{R}(A,B\backslash B')\frac{\mathcal{R}(x,B')}{\mathcal{R}(B',B\backslash B')},$$

y esto es una aplicación directa de la Proposición 2.2.9(1). Pues es exactamente la igualdad entre la segunda y la tercera expresión de dicha proposición en el caso $X' = X'' = x$. La hipótesis que necesitamos es $1 \le m + n - 2d$ y estamos en ese caso. □

En particular, la Proposición 3.2.1, junto con la Proposición 3.1.6, implican inmediatamente:

Corolario 3.2.2. *Sean A y B dos subconjuntos de un cuerpo K con $|A| = m$ y $|B| = n$. Sean $0 \le p \le m$ y $0 \le q \le n$ y sea $d := p + q$, con $d \le \min\{m-1, n-1\}$. Entonces*

$$\mathrm{Syl}_{p,q}(A,B)(x) = (-1)^{p(m-d)}\binom{d}{p}\mathrm{Sres}_d(f,g)(x).$$

3.2.2. El caso $m + n \le 2d + 1$

En este caso la reescritura de la suma doble nos dará un poco más de trabajo, ya que el lema de intercambio no puede aplicarse directamente. Para poder aplicarlo tendremos que cambiar el rol de la variable.

Proposición 3.2.3. *Sean A y B dos subconjuntos de un cuerpo K, con $|A| = m$ y $|B| = n$. Sean $0 \le p \le m$, $0 \le q \le n$ y sea $d := p + q$. Supongamos que $m + n \le 2d + 1$. Entonces*

$$\mathrm{Syl}_{p,q}(A,B)(x) = \begin{cases} (-1)^c\tbinom{k}{n-q}\mathrm{Syl}_{0,k}(A,B)(x) + (-1)^e\tbinom{k+1}{m-p}\mathrm{Syl}_{m,d-m}(A,B)(x) & si \quad d > m-1\\ (-1)^c\tbinom{k}{n-q}\mathrm{Syl}_{0,k}(A,B)(x) & si \quad d = m-1\\ 0 & si \quad d < m-1, \end{cases}$$

donde $k := m + n - d - 1$, $c := (d-m)(n-q) + d - n$ y $e := (d-m)(q+1)$.

Demostración. Fijado un $B' \subset B$ con $|B'| = q$, reescribimos

$$\sum_{\substack{A'\subset A\\ |A'|=p}} \mathcal{R}(B',A')\mathcal{R}(B\backslash B',A\backslash A')\frac{\mathcal{R}(x,A')}{\mathcal{R}(A',A\backslash A')} = \sum_{\substack{A'\subset A\\ |A'|=p}} \mathcal{R}(B'\cup x,A')\frac{\mathcal{R}(B\backslash B',A\backslash A')}{\mathcal{R}(A',A\backslash A')}$$

$$= (-1)^{p(q+1)}\sum_{\substack{A''\subset A\\ |A''|=m-p}} \mathcal{R}(A\backslash A'',B'\cup x)\frac{\mathcal{R}(B\backslash B',A'')}{\mathcal{R}(A\backslash A'',A'')}$$

$$= \begin{cases} (-1)^{p(q+1)}\displaystyle\sum_{\substack{C''\subset B'\cup x\\ |C''|=m-p}} \mathcal{R}(A,(B'\cup x)\backslash C'')\frac{\mathcal{R}(B\backslash B',C'')}{\mathcal{R}(C'',(B'\cup x)\backslash C'')} & \text{si} \quad d \ge m-1\\ 0 & \text{si} \quad d < m-1, \end{cases}$$

usando en la última igualdad el Teorema 2.2.2 con $X = B\backslash B'$, de tamaño $n-q$, y $B'\cup x$, de tamaño $q+1$, en lugar de B. La hipótesis que necesitamos es $n-q \leq m+(q+1)-2(m-p)$, que se cumple en el caso que estamos tratando. En el caso $m \leq d+1$ llamando $\zeta := (m-p)(n-q)$, tenemos

$$\begin{aligned}\mathrm{Syl}_{p,q}(A,B)(x) &= (-1)^{\zeta+pq} \sum_{\substack{B'\subset B\\|B'|=q}} \Big(\sum_{\substack{A'\subset A\\|A'|=p}} \mathcal{R}(B',A')\mathcal{R}(B\backslash B', A\backslash A')\frac{\mathcal{R}(x,A')}{\mathcal{R}(A',A\backslash A')}\Big)\frac{\mathcal{R}(x,B')}{\mathcal{R}(B',B\backslash B')}\\ &= (-1)^{\zeta+p} \sum_{\substack{B'\subset B\\|B'|=q}} \Big(\sum_{\substack{C''\subset B'\cup x\\|C''|=m-p}} \mathcal{R}(A,(B'\cup x)\backslash C'')\frac{\mathcal{R}(B\backslash B', C'')}{\mathcal{R}(C'',(B'\cup x)\backslash C'')}\Big)\frac{\mathcal{R}(x,B')}{\mathcal{R}(B',B\backslash B')}.\end{aligned}$$

Ahora separamos esta suma (sin considerar por ahora el signo $(-1)^{\zeta+p}$) en dos sumas, de acuerdo a los casos $x \in C''$ y $x \notin C''$. Hay dos casos extremos: $|C''| = 0$ y $|C''| = q+1$, que se dan cuando $p = m$ y $d = m-1$. En el primer caso sólo ocurre $x \notin C''$, mientras que en el segundo, sólo ocurre $x \in C''$. Asumamos por ahora que $p < m$ y $d > m-1$. La primera suma S_1, cuando $x \in C''$, resulta

$$\begin{aligned}S_1 &= \sum_{\substack{B'\subset B,|B'|=q\\C'\subset B',|C'|=m-p-1}} \mathcal{R}(A,B'\backslash C')\frac{\mathcal{R}(B\backslash B', C'\cup x)}{\mathcal{R}(C'\cup x, B'\backslash C')}\frac{\mathcal{R}(x,B')}{\mathcal{R}(B',B\backslash B')}\\ &= (-1)^{n-q+(n-q)q} \sum_{\substack{B'\subset B,|B'|=q\\C'\subset B',|C'|=m-p-1}} \mathcal{R}(A,B'\backslash C')\frac{\mathcal{R}(x,(B\backslash B')\cup C')}{\mathcal{R}((B\backslash B')\cup C', B'\backslash C')}\\ &= (-1)^{n(q+1)} \sum_{\substack{B'\subset B,|B'|=q\\C'\subset B',|C'|=m-p-1}} \mathcal{R}(A,B\backslash((B\backslash B')\cup C')\frac{\mathcal{R}(x,(B\backslash B')\cup C')}{\mathcal{R}((B\backslash B')\cup C', B\backslash((B\backslash B')\cup C'))}.\end{aligned}$$

Reescribiendo la suma en B' como una suma en $D = (B\backslash B')\cup C' \subset B$, con $|D| = n-q+m-p-1 = m+n-d-1 = k$, tenemos

$$\begin{aligned}S_1 &= (-1)^{n(q+1)} \sum_{\substack{D\subset B,|D|=k\\C'\subset D,|C'|=m-p-1}} \mathcal{R}(A,B\backslash D)\frac{\mathcal{R}(x,D)}{\mathcal{R}(D,B\backslash D)}\\ &= (-1)^{n(q+1)}\binom{k}{m-p-1} \sum_{D\subset B,|D|=k} \mathcal{R}(A,B\backslash D)\frac{\mathcal{R}(x,D)}{\mathcal{R}(D,B\backslash D)}\\ &= (-1)^{n(q+1)}\binom{k}{n-q}\mathrm{Syl}_{0,k}(A,B)(x).\end{aligned}$$

Notemos ahora S_2 a la segunda suma (sin el signo $(-1)^{\zeta+p}$ por ahora), cuando $x \notin C''$. Tenemos

$$
\begin{aligned}
S_2 &= \sum_{\substack{B'\subset B,|B'|=q\\ C''\subset B',|C''|=m-p}} \mathcal{R}(A,(B'\cup x)\backslash C'')\frac{\mathcal{R}(B\backslash B',C'')}{\mathcal{R}(C'',(B'\cup x)\backslash C'')}\frac{\mathcal{R}(x,B')}{\mathcal{R}(B',B\backslash B')}\\
&= (-1)^{\varepsilon} f(x) \sum_{\substack{B'\subset B,|B'|=q\\ C''\subset B',|C''|=m-p}} \mathcal{R}(A,B'\backslash C'')\frac{\mathcal{R}(x,B'\backslash C'')}{\mathcal{R}(B'\backslash C'',(B\backslash B')\cup C'')}\\
&= (-1)^{\varepsilon} f(x) \sum_{\substack{B'\subset B,|B'|=q\\ C''\subset B',|C''|=m-p}} \mathcal{R}(A,B\backslash((B\backslash B')\cup C''))\frac{\mathcal{R}(x,B\backslash((B\backslash B')\cup C''))}{\mathcal{R}(B\backslash((B\backslash B')\cup C''),(B\backslash B')\cup C'')}\\
&= (-1)^{\varepsilon} f(x) \sum_{\substack{D\subset B,|D|=k+1\\ C''\subset D,|C''|=m-p}} \mathcal{R}(A,B\backslash D)\frac{\mathcal{R}(x,B\backslash D)}{\mathcal{R}(B\backslash D,D)}\\
&= (-1)^{\varepsilon}\binom{k+1}{m-p} f(x) \sum_{D\subset B,|D|=k+1} \mathcal{R}(A,B\backslash D)\frac{\mathcal{R}(x,B\backslash D)}{\mathcal{R}(B\backslash D,D)}\\
&= (-1)^{\varepsilon}\binom{k+1}{m-p} f(x) \sum_{D'\subset B,|D'|=d-m} \mathcal{R}(A,D')\frac{\mathcal{R}(x,D')}{\mathcal{R}(D',B\backslash D'))}\\
&= (-1)^{\varepsilon}\binom{k+1}{m-p}\mathrm{Syl}_{m,d-m}(A,B)(x),
\end{aligned}
$$

donde $\varepsilon := m+m-p+(m-p)(n-q)+(m-p)(q+p-m) \equiv m+n(m-p) \pmod 2$, $D=(B\backslash B')\cup C''$, con $|D| = m+n-d-1+1 = k+1$; y $D' = B\backslash D$ con $|D'| = n-(k+1) = d-m$, y hemos usado la definición de $\mathrm{Syl}_{m,d-m}(A,B)(x)$.

Por último, miremos cómo queda el signo:

$$
\begin{aligned}
c &:= \zeta + p + n(q+1) \equiv (d-m)(n-q)+d-n \pmod 2\\
e &:= \zeta + p + \varepsilon = (m-p)(n-q)+m+n(m-p) \equiv (d-m)(q+1) \pmod 2
\end{aligned}
$$

Los casos $p=m$ y $d=m-1$, que son excluyentes y que dejamos de lado, simplemente corresponden a los casos en que la sumas S_1 y S_2 son vacías respectivamente. El cálculo de S_2 sirve también para probar el caso $d=m-1$, y asumiendo la convención de que $\binom{a}{b}=0$ si $a<b$, el caso $p=m$ también queda demostrado. □

Con este resultado, cualquier suma doble depende de dos sumas del tipo $\mathrm{Syl}_{0,q}(A,B)(x)$ y $\mathrm{Syl}_{m,q}(A,B)(x)$. Es decir, una suma simple y una suma en el caso $p=m$. Dado que las primeras ya las hemos descripto en su totalidad, sólo resta describir las segundas. Esto lo hacemos en la siguiente proposición.

Proposición 3.2.4. *Sean A y B dos subconjuntos de un cuerpo K con $|A|=m$ y $|B|=n$, y sea $0 \le d \le \min\{m-1, n-1\}$. Entonces*

$$
\mathrm{Syl}_{m,n-d-1}(A,B)(x) = (-1)^{m+(n-d)(d+1)+1} F_d(f,g)\, f,
$$

donde $F_d(f,g)$ es uno de los coeficientes polinomiales de la identidad de Bézout descriptos en la Proposición 1.1.4.

Demostración. Supongamos primero que $A \cap B \neq 0$. Dado que $\mathrm{Syl}_{m,n-d-1}(A,B)(x)$ y $f\, F_d(f,g)$ son ambos polinomios de grados menores o iguales que $m+n-d-1$, basta probar que toman los mismos valores en los elementos del conjunto $A \cup B$. Es claro que ambos polinomios se anulan en cada $\alpha \in A$, de modo que sólo resta evaluarlos en cada $\beta \in B$. Tenemos

$$\begin{aligned}
\mathrm{Syl}_{m,n-d-1}(A,B)(\beta) &= f(\beta) \sum_{\substack{B' \subset B, |B'|=n-d-1 \\ \beta \notin B'}} \mathcal{R}(A,B')\ \frac{\mathcal{R}(\beta,B')}{\mathcal{R}(B',B\backslash B')} \\
&= f(\beta) \sum_{\substack{B' \subset B\backslash\beta \\ |B'|=n-d-1}} \mathcal{R}(A,B')\ \frac{\mathcal{R}(\beta,B')}{\mathcal{R}(B',\beta)\mathcal{R}(B',B\backslash(\beta\cup B'))} \\
&= (-1)^{n-d-1} f(\beta) \sum_{\substack{B' \subset B\backslash\beta \\ |B'|=n-d-1}} \frac{\mathcal{R}(A,B')}{\mathcal{R}(B',B\backslash(\beta\cup B'))}.
\end{aligned}$$

Por otro lado, dado que $g(\beta)=0$,

$$(F_d(f,g)\, f)(\beta) = (F_d(f,g)\, f + G_d(f,g)\, g)(\beta) = \mathrm{Sres}_d(f,g)(x)(\beta) = \mathrm{Syl}_{0,d}(A,B)(\beta),$$

por la Proposición 3.1.6. Luego, necesitamos calcular $\mathrm{Syl}_{0,d}(A,B)(\beta)$. Pero

$$\begin{aligned}
\mathrm{Syl}_{0,d}(A,B)(\beta) &= \sum_{D \subset B, |D|=d} \mathcal{R}(A,B\backslash D)\ \frac{\mathcal{R}(\beta,D)}{\mathcal{R}(D,B\backslash D)} \\
&= \sum_{D \subset B\backslash\beta, |D|=d} \mathcal{R}(A,\beta)\mathcal{R}(A,B\backslash(\beta\cup D))\ \frac{\mathcal{R}(\beta,D)}{\mathcal{R}(D,\beta)\mathcal{R}(D,B\backslash(\beta\cup D))} \\
&= (-1)^{m-d} f(\beta) \sum_{D \subset B\backslash\beta, |D|=d} \frac{\mathcal{R}(A,B\backslash(\beta\cup D))}{\mathcal{R}(D,B\backslash(\beta\cup D))} \\
&= (-1)^{m-d} f(\beta) \sum_{\substack{B' \subset B\backslash\beta \\ |B'|=n-d-1}} \frac{\mathcal{R}(A,B')}{\mathcal{R}(B\backslash(\beta\cup B'),B')} \\
&= (-1)^{m-d+(n-d-1)d} f(\beta) \sum_{\substack{B' \subset B\backslash\beta \\ |B'|=n-d-1}} \frac{\mathcal{R}(A,B')}{\mathcal{R}(B',B\backslash(\beta\cup B'))},
\end{aligned}$$

llamando $B' := B\backslash(\beta \cup D)$. Hemos visto entonces que

$$\mathrm{Syl}_{m,n-d-1}(A,B)(\beta) = (-1)^{(n-d-1)+m-d+(n-d-1)d} \mathrm{Syl}_{0,d}(A,B)(\beta).$$

La demostración termina observando que

$$(n-d-1)+m-d+(n-d-1)d \equiv m+(n-d)(d+1)+1 \pmod 2.$$

El caso general se sigue del hecho que las dos expresiones coinciden genéricamente. □

Nos parece interesante dar una demostración alternativa, original de esta tesis, para calcular las sumas del tipo $\mathrm{Syl}_{m,q}(A,B)(x)$ usando el lema de intercambio y deduciendo además de la misma cuenta el valor de las sumas del tipo $\mathrm{Syl}_{p,n}(A,B)(x)$. Pero lo haremos bajo la hipótesis $\mathrm{Sres}_d(f,g)(x) \neq 0$.

Proposición 3.2.5. *Sean A y B dos subconjuntos de un cuerpo K con $|A| = m$ y $|B| = n$, y sean $f = \mathcal{R}(x,A)$ y $g = \mathcal{R}(x,B)$. Sea $0 \leq d \leq \min\{m-1, n-1\}$ con $\mathrm{Sres}_d(f,g)(x) \neq 0$. Entonces*

$$\begin{cases} \mathrm{Syl}_{m-d-1,n}(A,B)(x) &= (-1)^{m-d-1} g\, G_d(f,g) \\ \\ \mathrm{Syl}_{m,n-d-1}(A,B)(x) &= (-1)^{m+(n-d)(d+1)+1} f\, F_d(f,g), \end{cases}$$

donde $F_d(f,g)$ y $G_d(f,g)$ son los coeficientes polinomiales de la identidad de Bézout descriptos en la Proposición 1.1.4.

Demostración.

$$\begin{aligned} \mathrm{Syl}_{m-d-1,n}(A,B)(x) &= (-1)^{m-d-1} \sum_{\substack{A' \subseteq A \\ |A'|=m-d-1}} \frac{\mathcal{R}(A',B)\mathcal{R}(A',x)\mathcal{R}(x,B)}{\mathcal{R}(A', A\backslash A')} \\ &= (-1)^{m-d-1}\mathcal{R}(x,B) \sum_{\substack{A'' \subseteq A \\ |A''|=d+1}} \frac{\mathcal{R}(A\backslash A'', B\cup x)}{\mathcal{R}(A\backslash A'', A'')} \\ &= (-1)^{m-d-1}\mathcal{R}(x,B) \sum_{\substack{B' \subseteq B\cup x \\ |B'|=d+1}} \frac{\mathcal{R}(A, (B\cup x)\backslash B')}{\mathcal{R}(B', (B\cup x)\backslash B')}, \end{aligned} \tag{3.4}$$

usando en (3.4) el Teorema 2.2.2 con $B \cup x$ en lugar de B y $r = 0$. Separando la suma de acuerdo a los casos $x \in B'$ y $x \notin B'$, y dejando de lado el signo $(-1)^{m-d-1}$ por un momento, podemos reescribir la suma como

$$\begin{aligned} &\mathcal{R}(x,B)\left(\sum_{B'\subseteq B,\, |B'|=d} \frac{\mathcal{R}(A,B\backslash B')}{\mathcal{R}(B'\cup x, B\backslash B')} + \sum_{B'\subseteq B,\, |B'|=d+1} \frac{\mathcal{R}(A,(B\backslash B')\cup x)}{\mathcal{R}(B',(B\backslash B')\cup x)} \right) \\ &= \sum_{B'\subseteq B,\, |B'|=d} \frac{\mathcal{R}(A,B\backslash B')\mathcal{R}(x,B')}{\mathcal{R}(B',B\backslash B')} + (-1)^{d+1} \sum_{B'\subseteq B,\, |B'|=d+1} \frac{\mathcal{R}(A,(B\backslash B')\cup x)\mathcal{R}(x,B\backslash B')}{\mathcal{R}(B',B\backslash B')} \\ &= \sum_{\substack{B'\subseteq B \\ |B'|=d}} \frac{\mathcal{R}(A,B\backslash B')\mathcal{R}(x,B')}{\mathcal{R}(B',B\backslash B')} + (-1)^{(d+1)+m+(n-d-1)(d+1)} \sum_{\substack{B''\subseteq B \\ |B''|=n-d-1}} \frac{\mathcal{R}(A,B'')\mathcal{R}(x,A)\mathcal{R}(x,B'')}{\mathcal{R}(B'',B\backslash B'')} \\ &= \mathrm{Syl}_{0,d}(A,B)(x) + (-1)^{m+(n-d)(d+1)}\mathrm{Syl}_{m,n-d-1}(A,B)(x). \end{aligned}$$

Usando la descripción de la suma simple en la Proposición 3.1.6, hemos visto entonces que

$$\mathrm{Syl}_{m-d-1,n}(A,B)(x) = (-1)^{m-d-1}\mathrm{Sres}_d(f,g)(x) + (-1)^{(m-d-1)+m+(n-d)(d+1)}\mathrm{Syl}_{m,n-d-1}(A,B)(x).$$

O sea

$$\mathrm{Sres}_d(f,g)(x) = (-1)^{m-d-1}\mathrm{Syl}_{m-d-1,n}(A,B)(x) + (-1)^{m+(n-d)(d+1)+1}\mathrm{Syl}_{m,n-d-1}(A,B)(x).$$

Pero $\mathrm{Syl}_{m-d-1,n}(A,B)(x)$ y $\mathrm{Syl}_{m,n-d-1}(A,B)(x)$ son respectivamente polinomios de la forma $g\,G$ y $f\,F$ con G y F polinomios con $\deg(G) < m-d$ y $\deg(F) < n-d$. Luego, dado que asumimos $\mathrm{Sres}_d(f,g)(x) \neq 0$, por la Proposición 1.1.4, necesariamente:

$$\begin{cases} (-1)^{m+(n-d)(d+1)+1}\mathrm{Syl}_{m,n-d-1}(A,B)(x) &= f\,F_d(f,g) \\ (-1)^{m-d-1}\mathrm{Syl}_{m-d-1,n}(A,B)(x) &= g\,G_d(f,g), \end{cases}$$

probando lo que queríamos. □

Con esto hemos descripto las sumas del tipo $\mathrm{Syl}_{m,q}(A,B)(x)$ para el caso $q < n$. Pero el caso $q = n$ es trivial, pues ya observamos que $Syl_{m,n}(A,B)(x)$ consta de un solo término.

La última proposición nos permite obtener expresiones en términos de las raíces para los polinomios $F_d(f,g)$ y $G_d(f,g)$. Estas identidades pueden encontrarse en [Syl1853, Art. 29], y más recientemente en [KrSz2012] y [DKS2015].

Corolario 3.2.6. *Sea* $0 \leq d \leq \min\{m-1, n-1\}$. *Entonces*

$$F_d(f,g) = (-1)^{m-d} \sum_{B'\subset B, |B'|=d+1} \mathcal{R}(A, B\backslash B')\frac{\mathcal{R}(x, B\backslash B')}{\mathcal{R}(B', B\backslash B')}$$

$$G_d(f,g) = (-1)^{m-d+1} \sum_{A'\subset A, |A'|=d+1} \mathcal{R}(A\backslash A', B)\frac{\mathcal{R}(x, A\backslash A')}{\mathcal{R}(A\backslash A', A')}.$$

Demostración. Por la Proposición 3.2.4 sabemos que

$$f\,F_d(f,g) = (-1)^{m+(n-d)(d+1)+1}\mathrm{Syl}_{m,n-d-1}(A,B)(x).$$

O sea

$$f\,F_d(f,g) = (-1)^{m+(n-d)(d+1)+1} \sum_{B'\subset B, |B'|=n-d-1} \mathcal{R}(A, B')\frac{\mathcal{R}(x, B')\mathcal{R}(x, A)}{\mathcal{R}(B', B\backslash B')}.$$

Luego

$$\begin{aligned} F_d(f,g) &= (-1)^{m+(n-d)(d+1)+1} \sum_{B'\subset B, |B'|=n-d-1} \mathcal{R}(A, B')\frac{\mathcal{R}(x, B')}{\mathcal{R}(B', B\backslash B')} \\ &= (-1)^{m+(n-d)(d+1)+1} \sum_{B''\subset B, |B''|=d+1} \mathcal{R}(A, B\backslash B'')\frac{\mathcal{R}(x, B\backslash B'')}{\mathcal{R}(B\backslash B'', B'')} \\ &= (-1)^{m+(n-d)(d+1)+1+(n-d-1)(d+1)} \sum_{B''\subset B, |B''|=d+1} \mathcal{R}(A, B\backslash B'')\frac{\mathcal{R}(x, B\backslash B'')}{\mathcal{R}(B'', B\backslash B'')}, \end{aligned}$$

que prueba lo que queremos ya que $m + (n-d)(d+1) + 1 + (n-d-1)(d+1) \equiv m-d$ (mód 2). La igualdad para $G_d(f,g)$ puede verse de manera análoga, o bien deducirla de la relación entre $F_d(f,g)$ y $G_d(g,f)$ vista en (1.3). □

Finalmente, las Proposiciones 3.2.3, 3.1.6 y 3.2.4 implican:

Corolario 3.2.7. *Sean A y B dos subconjuntos de un cuerpo K. Sean $0 \leq p \leq m$ y $0 \leq q \leq n$ y sea $d := p + q$, con $\max\{m, n\} \leq d \leq m + n - 1$. Entonces*

$$\mathrm{Syl}_{p,q}(A, B)(x) = (-1)^{(d-m)(n-q)+d-n}\Big(\binom{k}{n-q}\mathrm{Sres}_k(f, g)(x) - \binom{k+1}{m-p}F_k(f, g)\, f\Big),$$

donde $k := m + n - d - 1$.

Demostración. Tenemos

$$\begin{aligned}\mathrm{Syl}_{p,q}(A, B)(x) &= (-1)^c\binom{k}{n-q}\mathrm{Syl}_{0,k}(A, B)(x) + (-1)^e\binom{k+1}{m-p}\mathrm{Syl}_{m,d-m}(A, B)(x)\\ &= (-1)^c\binom{k}{n-q}\mathrm{Sres}_k(f, g)(x) + (-1)^e(-1)^{(d-m)n+m+n-1}\binom{k+1}{m-p}F_k(f, g)\, f,\end{aligned}$$

donde $c := (d - m)(n - q) + d - n$ and $e := (d - m)(q + 1)$. La demostración concluye observando que $e + (d - m)n + m + n \equiv (d - m)(n - q) + d - n$ (mód 2). □

El Corolario 3.2.7, junto con las Proposiciones 3.2.3 y 3.2.4, el Corolario 3.1.4 y la Proposición 3.1.6, más los casos triviales, termina de describir todos los casos del Teorema 1.2.6, quedando éste demostrado.

Capítulo 4

Fórmula cerrada en raíces para la subresultante en el caso general

En este capítulo presentamos los resultados centrales de la primera parte de esta tesis.

En la Sección 4.1 definimos una extensión de la suma simple $\mathrm{Syl}_{d,0}(A,B)(x)$, para multiconjuntos A y B, que coincide con $\mathrm{Syl}_{d,0}(A,B)(x)$ si A y B son conjuntos, y que tiene la misma relación que tiene $\mathrm{Syl}_{d,0}(A,B)(x)$ con $\mathrm{Sres}_d(f,g)(x)$ si $f=\mathcal{R}(x,A)$ y $g=\mathcal{R}(x,B)$. Como consecuencia obtenemos escrituras para las subresultantes en términos de las raíces de los polinomios admitiendo raíces múltiples. Trabajamos por separado el caso d suficientemente grande dado que este caso es más sencillo; en el caso general necesitamos usar polinomios de Schur. Al final de la sección damos un link de acceso a un archivo en el que desarrollamos un código con el programa Maple ([Map2016]) para computar estas fórmulas. Los resultados de esta sección se encuentran en el trabajo [DKSV2017]. En la Sección 4.2 presentamos una extensión de las sumas dobles $\mathrm{Syl}_{p,q}(A,B)(x)$ para multiconjuntos A y B en el caso p y q suficientemente grandes. De igual modo que con la suma simple, esta construcción efectivamente extiende a la sumas dobles $\mathrm{Syl}_{p,q}(A,B)(x)$ ya que coinciden si A y B son conjuntos, y también guarda la misma relación que las sumas $\mathrm{Syl}_{p,q}(A,B)(x)$ tienen con $\mathrm{Sres}_d(f,g)(x)$, con $d=p+q$, si $f=\mathcal{R}(x,A)$ y $g=\mathcal{R}(x,B)$. Los resultados de la Sección 4.2 son originales de esta tesis.

4.1. Extensión de la suma simple de Sylvester

Hemos visto que las igualdades

$$\begin{cases} \mathrm{Syl}_{p,q}(A,B)(x) & = (-1)^{p(m-d)}\binom{d}{p}\mathrm{Sres}_d(f,g)(x) \\ \mathrm{Syl}_{d,0}(A,B)(x) & = (-1)^{d(m-d)}\mathrm{Sres}_d(f,g)(x), \end{cases}$$

del Teorema 1.2.5, pueden considerarse como generalizaciones para las subresultantes de la fórmula de Poisson de la resultante. Y hemos mencionado la limitación que tienen, que es que no admiten multiplicidad en las raíces de f y g, pues A y B no pueden ser ambos multiconjuntos. Si bien $\mathrm{Syl}_{d,0}(A,B)(x)$ sí admite que B sea un multiconjunto, A no puede serlo. Y la situación simétrica se da en $\mathrm{Syl}_{0,d}(A,B)(x)$. En esta sección extenderemos la

definición de la suma simple $\mathrm{Syl}_{d,0}(A,B)(x)$ para el caso A y B multiconjuntos, y veremos que esta extensión tiene la misma relación con la subresultante. Para esto volverá a ser central el papel del lema de intercambio y sus corolarios. En algunos casos usaremos también polinomios de Schur, que introduciremos más adelante.

Si perseguimos el objetivo de obtener una fórmula para la subresultante en términos de las raíces para el caso general, podemos pensar que la fórmula de Apéry y Jouanolou, que se prueba en [ApJo2006, Prop.91], es una primera aproximación:

Proposición 4.1.1. *Sean f y g dos polinomios de grados m y n respectivamente y sean A y B sus respectivos conjuntos de raíces. Sea E un conjunto tal que $|E| = m+n-d$ y $0 \leq d < \min\{m,n\}$ o $d = \min\{m,n\}$ si $m \neq n$. Entonces*

$$\mathrm{Sres}_d(f,g)(x) = \sum_{\substack{E_1 \cup E_2 \cup E_3 = E \\ |E_1|=d, |E_2|=m-d, |E_3|=n-d}} \frac{\mathcal{R}(E_3,A)\mathcal{R}(E_2,B)\mathcal{R}(x,E_1)}{\mathcal{R}(E_2,E_1)\mathcal{R}(E_3,E_1)\mathcal{R}(E_3,E_2)}.$$

Esta fórmula tiene dos ingredientes interesantes. En primer lugar, la suma tiene sentido incluso si A o B son multiconjuntos. Por otro lado, lo interesante es que no depende del conjunto E, sino sólo de su cardinal. Esto no sólo nos remite a uno de los corolarios del lema de intercambio; sino que más aún, dicho corolario generaliza la fórmula de Apéry y Jouanolou. Precisamente:

Proposición 4.1.2. *Sean A y B subconjuntos de un cuerpo K con $|A| = m$ y $|B| = n$ y sea $0 \leq d \leq m$. Sean X un conjunto de variables y $E \subset K$ un conjunto finito tal que*

$$|E| \geq \max\{|X| + d, m+n-d, m\}.$$

Entonces

$$\sum_{\substack{A_1 \cup A_2 = A \\ |A_1|=d,\, |A_2|=m-d}} \frac{\mathcal{R}(A_2,B)\mathcal{R}(X,A_1)}{\mathcal{R}(A_1,A_2)}$$
$$= \sum_{\substack{E_1 \cup E_2 \cup E_3 = E \\ |E_1|=d, |E_2|=m-d, |E_3|=|E|-m}} \frac{\mathcal{R}(A,E_3)\mathcal{R}(E_2,B)\mathcal{R}(X,E_1)}{\mathcal{R}(E_1,E_2)\mathcal{R}(E_1,E_3)\mathcal{R}(E_2,E_3)}.$$

Demostración. Es consecuencia inmediata de la Observación 2.2.7 tomando $A = E$, $B = A$, $Y = B$ y $p = d$ y mirando con cuidado el signo. □

La fórmula de Apéry y Jouanolou se deduce de la Proposición 4.1.2 en el caso $|X| = 1$, $|E| = m+n-d$, d en el rango de dicha fórmula y usando la relación entre la suma simple de Sylvester y la subresultante de la Proposición 3.1.6.

La Proposición 4.1.2 será la que nos permitirá obtener las fórmulas que buscamos aprovechando la libertad que tenemos para elegir un conjunto E adecuado.

4.1.1. El caso d suficientemente grande

La idea será, como dijimos, a partir de la Proposición 4.1.2, elegir un conjunto E adecuado para obtener la fórmula que buscamos para la subresultante en términos de las raíces. Un primer caso será aquél en el que la cantidad de raíces distintas de f y g sean suficientes como para poder tomar como E al conjunto formado por ellas. Debido a la hipótesis para el cardinal de E en la Proposición 4.1.2, esta condición puede darse en términos del valor de d, que cuanto mayor sea, se podrá tomar un conjunto E de tamaño menor. En esta dirección definiremos ahora una generalización $\mathrm{SylM}_{d,0}(A,B)(x)$ de la noción de suma simple de Sylvester $\mathrm{Syl}_{d,0}(A,B)(x)$, para multiconjuntos A y B y d suficientemente grande.

Dado un cuerpo K y un multiconjunto $Y \subset K$, notamos $|Y|$ a su tamaño (la cantidad de elementos contados con su multiplicidad).

Definición 4.1.3. Sea K un cuerpo, sean A, $B \subset K$ multiconjuntos con $|A| = m$, $|B| = n$ y sean $\overline{A} \subset A$ y $\overline{B} \subset B$ los conjuntos de elementos distintos de A y B respectivamente, con $|\overline{A}| = \overline{m}$, $|\overline{B}| = \overline{n}$. Sean $m' := m - \overline{m}$ y $n' := n - \overline{n}$. Para d tal que $m'+n' \leq d < \min\{m,n\}$ o $m'+n' \leq d \leq \min\{m,n\}$ si $m \neq n$, definimos

$$\mathrm{SylM}_{d,0}(A,B)(x) := (-1)^{m'(m-d)} \sum_{\substack{A' \subset \overline{A} \\ |A'|=d-m'}} \sum_{\substack{B' \subset \overline{B} \\ |B'|=m'}} \frac{\mathcal{R}(A\backslash\overline{A}, \overline{B}\backslash B')\mathcal{R}(\overline{A}\backslash A', B\backslash B')\mathcal{R}(x,A')\mathcal{R}(x,B')}{\mathcal{R}(A', \overline{A}\backslash A')\mathcal{R}(B', \overline{B}\backslash B')}.$$

Esta definición sólo tiene sentido cuando A y B tienen pocos elementos repetidos y d está en el rango mencionado. Para esos valores de d tenemos:

Teorema 4.1.4. *Sean K un cuerpo y $f, g \in K[x]$ polinomios mónicos de grados m y n respectivamente, con multiconjuntos de raíces A y B, y conjuntos de raíces distintas $\overline{A}$ y $\overline{B}$ respectivamente, y sean $m' := m - \overline{m}$ y $n' := n - \overline{n}$. Dado d tal que $m'+n' \leq d < \min\{m,n\}$ o $m'+n' \leq d \leq \min\{m,n\}$, se tiene*

$$\mathrm{Sres}_d(f,g)(x) = (-1)^{d(m-d)}\mathrm{SylM}_{d,0}(A,B)(x).$$

Antes de probar el Teorema 4.1.4 vamos a hacer algunas observaciones. En primer lugar, uno podría preguntarse si la cota inferior para d en el Teorema 4.1.4 es óptima, dado que la definición de $\mathrm{SylM}_{d,0}(A,B)(x)$ tiene sentido aún para $m' \leq \min\{d, \overline{n}\}$. El siguiente ejemplo ilustra un caso en donde el resultado se cumple con d en el rango del enunciado y muestra que la restricción sobre d es necesaria.

Ejemplo 4.1.5. Sean $f = (x-\alpha_1)(x-\alpha_2)^2$ y $g = (x-\beta_1)^2$, de modo que $A = (\alpha_1, \alpha_2, \alpha_2)$ con $\overline{A} = \{\alpha_1, \alpha_2\}$ y $B = (\beta_1, \beta_1)$ con $\overline{B} = \{\beta_1\}$. Para $d = 2$, dado que $(3-2)+(2-1) \leq 2 \leq \min\{3,2\}$, tenemos $\mathrm{Sres}_2(f,g)(x) = g(x)$, mientras que

$$\begin{aligned}
\mathrm{SylM}_{2,0}(A,B)(x) &= -\Big(\frac{(\alpha_2-\beta_1)(x-\alpha_1)(x-\beta_1)}{\alpha_1-\alpha_2} + \frac{(\alpha_1-\beta_1)(x-\alpha_2)(x-\beta_1)}{\alpha_2-\alpha_1}\Big) \\
&= \frac{\big((\alpha_2-\beta_1)(x-\alpha_1) - (\alpha_1-\beta_1)(x-\alpha_2)\big)(x-\beta_1)}{\alpha_2-\alpha_1} \\
&= (x-\beta_1)(x-\beta_1) = g(x),
\end{aligned}$$

con lo cual el Teorema 4.1.4 se cumple en este caso.

Ahora tomemos $f = (x-\alpha_1)(x-\alpha_2)^2$ y $g = (x-\beta_1)^3$. En este caso, $A = (\alpha_1, \alpha_2, \alpha_2)$ con $\overline{A} = \{\alpha_1, \alpha_2\}$ y $B = (\beta_1, \beta_1, \beta_1)$ con $\overline{B} = \{\beta_1\}$. Para $d = 2 < (3-2)+(3-1)$ tenemos $\mathrm{Sres}_2(f,g)(x) = g(x) - f(x)$ y $\mathrm{SylM}_{2,0}(A,B)(x)$ puede definirse de acuerdo a la Definición 4.1.3 puesto que $m' = 1 \leq \min\{d, \overline{n}\}$, pero resulta ser un múltiplo de $x - \beta_1$, por lo que las dos expresiones obviamente no coinciden.

El Teorema 4.1.4 será consecuencia del siguiente teorema, que no trata aún con multiconjuntos.

Teorema 4.1.6. *Sean A y B subconjuntos de un cuerpo K con $|A| = m$ y $|B| = n$. Sean $\overline{A} \subset A$ y $\overline{B} \subset B$ subconjuntos no vacíos de A y B, con $|\overline{A}| = \overline{m}$ y $|\overline{B}| = \overline{n}$ y sean $m' := m - \overline{m}$ y $n' := n - \overline{n}$. Sea d tal que $m' + n' \leq d \leq \min\{m, n\}$ y sea X un conjunto de variables con $|X| \leq m + n - 2d$. Entonces*

$$\sum_{\substack{A_1 \cup A_2 = A \\ |A_1| = d,\, |A_2| = m-d}} \frac{\mathcal{R}(A_2, B)\mathcal{R}(X, A_1)}{\mathcal{R}(A_1, A_2)}$$

$$= (-1)^{m'(m-d)} \sum_{\substack{A' \subset \overline{A} \\ |A'| = d - m'}} \sum_{\substack{B' \subset \overline{B} \\ |B'| = m'}} \frac{\mathcal{R}(A \backslash \overline{A}, \overline{B} \backslash B')\mathcal{R}(\overline{A} \backslash A', B \backslash B')\mathcal{R}(X, A')\mathcal{R}(X, B')}{\mathcal{R}(A', \overline{A} \backslash A')\mathcal{R}(B', \overline{B} \backslash B')}.$$

Demostración. Supongamos primero que $A \cap B = \emptyset$. Por la Proposición 4.1.2 tomando $E := \overline{A} \cup \overline{B}$, pues $|E| = \overline{m} + \overline{n} \geq m + n - d$ por hipótesis, tenemos

$$\sum_{\substack{A_1 \cup A_2 = A \\ |A_1| = d,\, |A_2| = m-d}} \frac{\mathcal{R}(A_2, B)\mathcal{R}(X, A_1)}{\mathcal{R}(A_1, A_2)} = \sum_{\substack{E_1 \cup E_2 \cup E_3 = \overline{A} \cup \overline{B} \\ |E_1| = d, |E_2| = m-d \\ |E_3| = \overline{m} + \overline{n} - m}} \frac{\mathcal{R}(A, E_3)\mathcal{R}(E_2, B)\mathcal{R}(X, E_1)}{\mathcal{R}(E_1, E_2)\mathcal{R}(E_1, E_3)\mathcal{R}(E_2, E_3)}.$$

Ahora, $\mathcal{R}(A, E_3) = \emptyset$ cuando $A \cap E_3 \neq \emptyset$ y $\mathcal{R}(E_2, B) = \emptyset$ cuando $E_2 \cap B \neq \emptyset$. Luego $E_3 \subset \overline{B}$ y $E_2 \subset \overline{A}$. Llamando $A' = \overline{A} \backslash E_2$ y $B' = \overline{B} \backslash E_3$, tenemos que $E_3 = \overline{B} \backslash B'$, $E_2 = \overline{A} \backslash A'$ y $E_1 = A' \cup B'$, y por lo tanto podemos escribir la suma como

$$\sum_{\substack{A' \subset \overline{A} \\ |A'| = d - m'}} \sum_{\substack{B' \subset \overline{B} \\ |B'| = m'}} \frac{\mathcal{R}(A, \overline{B} \backslash B')\mathcal{R}(\overline{A} \backslash A', B)\mathcal{R}(X, A')\mathcal{R}(X, B')}{\mathcal{R}(A' \cup B', \overline{A} \backslash A')\mathcal{R}(A' \cup B', \overline{B} \backslash B')\mathcal{R}(\overline{A} \backslash A', \overline{B} \backslash B')}$$

$$= \sum_{\substack{A' \subset \overline{A} \\ |A'| = d - m'}} \sum_{\substack{B' \subset \overline{B} \\ |B'| = m'}} \frac{\mathcal{R}(A, \overline{B} \backslash B')\mathcal{R}(\overline{A} \backslash A', B)\mathcal{R}(X, A')\mathcal{R}(X, B')}{\mathcal{R}(A', \overline{A} \backslash A')\mathcal{R}(B', \overline{A} \backslash A')\mathcal{R}(\overline{A}, \overline{B} \backslash B')\mathcal{R}(B', \overline{B} \backslash B')}$$

$$= (-1)^{|B'|\,|\overline{A} \backslash A'|} \sum_{\substack{A' \subset \overline{A} \\ |A'| = d - m'}} \sum_{\substack{B' \subset \overline{B} \\ |B'| = m'}} \frac{\mathcal{R}(A \backslash \overline{A}, \overline{B} \backslash B')\mathcal{R}(\overline{A} \backslash A', B \backslash B')\mathcal{R}(X, A')\mathcal{R}(X, B')}{\mathcal{R}(A', \overline{A} \backslash A')\mathcal{R}(B', \overline{B} \backslash B')},$$

como queríamos, dado que $|B'|\,|\overline{A} \backslash A'| = m'(m-d)$. El caso general se sigue del hecho que las dos expresiones coinciden genéricamente. □

Observemos que si en el Teorema 4.1.6 tomamos $\overline{A} = A$, el miembro derecho de la igualdad coincide claramente con el miembro izquierdo, con lo cual no obtenemos nada nuevo. Sin embargo el miembro derecho tiene sentido incluso cuando A y B son multiconjuntos; sólo necesitamos que $\overline{A}$ y $\overline{B}$ sean conjuntos. Si $X = \{x\}$ podemos definir la noción de suma simple de Sylvester para multiconjuntos A y B con d en el rango del Teorema 4.1.6, que extiende la noción usual de la suma simple de Sylvester para conjuntos, como enunciamos en la Definición 4.1.3. Ahora podemos probar el Teorema 4.1.4.

Demostración del Teorema 4.1.4. Supongamos $A = (\underbrace{a_1, \dots, a_1}_{j_1}, \dots, \underbrace{a_{\overline{m}}, \dots, a_{\overline{m}}}_{j_{\overline{m}}})$ con $m = j_1 + \cdots + j_{\overline{m}}$ y $B = (\underbrace{b_1, \dots, b_1}_{\ell_1}, \dots, \underbrace{b_{\overline{n}}, \dots, b_{\overline{n}}}_{\ell_{\overline{n}}})$ con $n = \ell_1 + \cdots + \ell_{\overline{n}}$, de modo que $f = \prod_{a\in A}(x-a)$ y $g = \prod_{b\in B}(x-b)$. Definamos dos conjuntos de variables $Y = \{y_{1,1}, \dots, y_{1,j_1}, \dots, y_{\overline{m},1}, \dots, y_{\overline{m},j_{\overline{m}}}\}$ y $Z = \{z_{1,1}, \dots, z_{1,\ell_1}, \dots, z_{\overline{n},1}, \dots, z_{\overline{n},\ell_{\overline{n}}}\}$, y sean $f^y := (x-y_{1,1})\cdots(x-y_{\overline{m},j_{\overline{m}}})$ y $g^z := (x-z_{1,1})\cdots(x-z_{\overline{n},s\ell_{\overline{n}}})$. Luego, si llamamos $\overline{Y} = \{y_{1,1}, \dots, y_{\overline{m},1}\}$ y $\overline{Z} = \{z_{1,1}, \dots, z_{\overline{n},1}\}$, dado que $m' + n' \le d < \text{mín}\{m,n\}$ o $m'+n' \le d \le \text{mín}\{m,n\}$, de acuerdo al Teorema 4.1.6 tenemos

$$\mathrm{Syl}_{d,0}(Y,Z)(x) = (-1)^{m'(m-d)} \sum_{\substack{Y'\subset\overline{Y}\\|Y'|=d-m'}} \sum_{\substack{Z'\subset\overline{Z}\\|Z'|=m'}} \frac{\mathcal{R}(Y\backslash\overline{Y}, \overline{Z}\backslash Z')\mathcal{R}(\overline{Y}\backslash Y', Z\backslash Z')\mathcal{R}(x,Y')\mathcal{R}(x,Z')}{\mathcal{R}(Y',\overline{Y}\backslash Y')\mathcal{R}(Z',\overline{Z}\backslash Z')}.$$

Por otro lado, por el Teorema 1.2.5, $\mathrm{Sres}_d(f^y, g^z) = (-1)^{d(m-d)}\mathrm{Syl}_{d,0}(Y,Z)(x)$. Luego, con d en el rango del enunciado,

$$\mathrm{Sres}_d(f^y, g^z) = (-1)^{(d-m')(m-d)} \sum_{\substack{Y'\subset\overline{Y}\\|Y'|=d-m'}} \sum_{\substack{Z'\subset\overline{Z}\\|Z'|=m'}} \frac{\mathcal{R}(Y\backslash\overline{Y}, \overline{Z}\backslash Z')\mathcal{R}(\overline{Y}\backslash Y', Z\backslash Z')\mathcal{R}(x,Y')\mathcal{R}(x,Z')}{\mathcal{R}(Y',\overline{Y}\backslash Y')\mathcal{R}(Z',\overline{Z}\backslash Z')}.$$

Terminamos la demostración haciendo $y_{1,i} \to a_1, \dots, y_{\overline{m},i} \to a_{\overline{m}}$, $z_{1,i} \to b_1, \dots, z_{\overline{n},i} \to b_{\overline{n}}$ y observando que ambos miembros de la igualdad están bien definidos. □

4.1.2. El caso general: d arbitrario

Ahora nos ocuparemos de extender la definición de $\mathrm{SylM}_{d,0}(A,B)(x)$ al caso general. En el caso anterior, al ser d suficientemente grande, pudimos tomar $\overline{A}\cup\overline{B}$ para el conjunto E. Si d es más grande, el cardinal de E no puede cubrirse con $\overline{A}\cup\overline{B}$, de modo que la construcción será un poco más compleja. La idea será volver a considerar $\overline{A}\cup\overline{B}$, pero para llegar a cubrir el cardinal de E, completaremos con un conjunto de variables T y luego haremos un proceso de identificar un coeficiente preciso en esas variables. Para esto necesitaremos trabajar con polinomios de Schur, de los que recordaremos aquí su definición. Antes introducimos la siguiente notación.

Notación 4.1.7. Sea $X = (x_1, \dots, x_k)$ una k-upla de indeterminadas o de elementos distintos. Denotamos la matriz de Vandermonde *rectangular* de tamaño $\ell \times k$ correspondiente

a X por

$$\mathcal{V}_\ell(X) := \overset{k}{\begin{bmatrix} x_1^{\ell-1} & \dots & x_k^{\ell-1} \\ \vdots & & \vdots \\ 1 & \dots & 1 \end{bmatrix}}\ \ell\ .$$

Cuando $\ell = k$ escribimos simplemente $\mathcal{V}(X)$, pues es la matriz de Vandermonde usual de la Observación 2.2.12.

Ahora recordemos la construcción de los polinomios de Schur. Dada una partición

$$\lambda = (\lambda_1, \lambda_2, \dots, \lambda_r),\ \lambda_i \in \mathbb{Z}_{\geq 0} \text{ para } 1 \leq i \leq r, \text{ con } \lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_r,$$

el polinomio de Schur $s_\lambda(X)$ para un conjunto $X = \{x_1, \dots, x_r\}$ se define como el cociente

$$s_\lambda(X) = \frac{\det \begin{pmatrix} x_1^{\lambda_1+r-1} & x_2^{\lambda_1+r-1} & \dots & x_r^{\lambda_1+r-1} \\ x_1^{\lambda_2+r-2} & x_2^{\lambda_2+r-2} & \dots & x_r^{\lambda_2+r-2} \\ \vdots & \vdots & \ddots & \vdots \\ x_1^{\lambda_r} & x_2^{\lambda_r} & \dots & x_r^{\lambda_r} \end{pmatrix}}{\det \begin{pmatrix} x_1^{r-1} & \dots & x_r^{r-1} \\ \vdots & & \vdots \\ 1 & \dots & 1 \end{pmatrix}}.$$

Esto es, los polinomios de Schur son cocientes de determinantes de matrices del tipo Vandermonde, donde en el numerador se saltean algunas filas de una matriz de Vandermonde rectangular. Notemos que los polinomios de Schur son simétricos en $x_1, \dots, x_r$, por lo que tiene sentido escribir $s_\lambda(X)$ para un conjunto X. Observemos también que, por ejemplo, si $\lambda = (0, \dots, 0)$, se tiene $s_\lambda(X) = 1$.

Por conveniencia, aquí no usaremos esta notación usual para polinomios de Schur dada por particiones, sino que introduciremos una notación con un conjunto de exponentes como sigue. Dado $R = \{i_1, \dots, i_{k-r}\} \subset \{1, \dots, k\}$ un subconjunto de índices, denotaremos $\mathcal{V}_k^{(R)}(X)$ a la submatriz cuadrada de $\mathcal{V}_k(X)$ que se obtiene al quitar de ella las filas correspondientes a los índices en R. Definimos así

$$S_k^{(R)}(X) := \frac{V_k^{(R)}(X)}{V(X)}, \tag{4.1}$$

donde $V_k^{(R)}(X) := \det(\mathcal{V}_k^{(R)}(X))$. Así, $S_k^{(R)}(X)$ es el polinomio de Schur asociado al conjunto de índices que están en $\{1, \dots, k\} \setminus R$.

Más generalmente, si $X = (\underbrace{x_1, \dots, x_1}_{j_1}, \dots, \underbrace{x_{\overline{r}}, \dots, x_{\overline{r}}}_{j_{\overline{r}}})$ es un multiconjunto con $r = j_1 + \cdots + j_{\overline{r}}$, definimos la matriz de Vandermonde *generalizada* de tamaño $k \times r$ como (c.f. [Kal1984])

$$\mathcal{V}_k(X) = \begin{pmatrix} \mathcal{V}_k(x_1, j_1) & \dots & \mathcal{V}_k(x_{\overline{r}}, j_{\overline{r}}) \end{pmatrix}, \tag{4.2}$$

donde, para cada j, $\mathcal{V}_k(x_i, j)$ de tamaño $k \times j$ está definido por

$$\mathcal{V}_k(x_i, j) := \begin{pmatrix} x_i^{k-1} & (k-1)x_i^{k-2} & (k-1)(k-2)x_i^{k-3} & \dots & \frac{(k-1)!}{(k-j)!}x_i^{k-j} \\ \vdots & \vdots & \vdots & & \vdots \\ x_i^2 & 2x_i & 2 & \dots & 0 \\ x_i & 1 & 0 & \dots & 0 \\ 1 & 0 & 0 & \dots & 0 \end{pmatrix},$$

y cuando $k = r$ escribimos $\mathcal{V}(X)$ como en la Notación 4.1.7. Es conocido el hecho que $\mathcal{V}(X)$ es inversible si $x_i \neq x_j$ para $i \neq j$.

Así podemos definir también los polinomios de Schur generalizados del mismo modo: dado $R = \{i_1, \dots, i_{k-r}\} \subset \{1, \dots, k\}$ un subconjunto de índices, notamos $\mathcal{V}_k^{(R)}(X)$ a la submatriz cuadrada de $\mathcal{V}_k(X)$ que se obtiene al quitar de ella las filas correspondientes a los índices en R, y definimos

$$S_k^{(R)}(X) := \frac{V_k^{(R)}(X)}{V(X)}, \tag{4.3}$$

Donde, como antes, $V_k^{(R)}(X) := \det(\mathcal{V}_k^{(R)}(X))$. Notemos que en principio $S_k^{(R)}(X)$ es una función racional. El siguiente resultado muestra que es un polinomio.

Lema 4.1.8. *$S_k^{(R)}(X)$ es un polinomio en las variables X con coeficientes en K.*

Demostración. Si X es un conjunto en vez de un multiconjunto, el cociente definido en (4.3) coincide con el polinomio de Schur definido en (4.1), de modo que no hay nada que probar. Para el caso general, consideremos el conjunto $X = \{x_{1,1}, \dots, x_{1,j_1}, \dots, x_{\overline{r},1}, \dots, x_{\overline{r},i_{\overline{r}}}\}$ que "convergerá" a un multiconjunto Y haciendo $x_{1,i} \to y_1$ para $1 \leq i \leq j_1$, $\dots$, $x_{\overline{r},i} \to y_{\overline{r}}$, para $1 \leq i \leq j_{\overline{r}}$. Luego

$$S_k^{(R)}(X) \to S_k^{(R)}(Y)$$

como puede verse, por ejemplo, calculando los límites para $x_{1,2} \to x_{1,1}$ por la regla de L'Hopital, para $x_{i,3} \to x_{i,1}$ si es necesario, y repitiendo el proceso para los demás términos $x_{k,2} \to x_{k,1}$, etc. Esto prueba que $S_k^{(R)}(Y)$ es en efecto un polinomio. □

Para un conjunto $R \subset \{1, \dots, r\}$ dado en orden creciente, definimos $\mathrm{sg}_r(R) := (-1)^\sigma$, donde σ es el número de transposiciones necesarias para llevar este conjunto a los primeros lugares de $\{1, \dots, r\}$, i.e. si $R = \{i_1, \dots i_s\}$ con $1 \leq i_1 < \dots < i_s \leq r$, entonces σ es la paridad del número de transposiciones necesarias para llevar $(1, \dots, r)$ a $(i_1, \dots i_s, \dots)$, sin cambiar el orden relativo de los otros elementos.

También, para una partición dada $R := R_1 \sqcup R_2 \sqcup \dots \sqcup R_\ell$ de $\{1, \dots, r\}$, notamos $\mathrm{sg}(R) = \mathrm{sg}(R_1, \dots, R_\ell) := (-1)^\sigma$, donde σ es la paridad del número de transposiciones necesarias para llevar el conjunto ordenado $(R_1, \dots, R_\ell)$ (asumimos que cada uno de ellos también está ordenado en forma creciente) a $\{1, \dots, r\}$.
Ahora sí podemos extender la Definición 4.1.3.

Definición 4.1.9. Sean K un cuerpo y $A, B \subset K$ multiconjuntos con $|A| = m$ y $|B| = n$ y sean $\overline{A} \subset A$ y $\overline{B} \subset B$ los conjuntos de distintos elementos de A y B respectivamente,

con $|\overline{A}| = \overline{m}$ y $|\overline{B}| = \overline{n}$. Sean $m' := m - \overline{m}$ y $n' := n - \overline{n}$. Para $0 \leq d < \text{mín}\{m, n\}$ o $d = \text{mín}\{m, n\}$ si $m \neq n$, definimos

$$\begin{aligned}\text{SylM}_{d,0}(A, B)(x) = \sum (-1)^{\sigma_R} \frac{\mathcal{R}(A\backslash\overline{A}, \overline{B}\backslash B')\mathcal{R}(\overline{A}\backslash A', B\backslash B')\mathcal{R}(x, A')\mathcal{R}(x, B')}{\mathcal{R}(A', \overline{A}\backslash A')\mathcal{R}(B', \overline{B}\backslash B')} \\ \cdot\ S_{d+1}^{(\widetilde{R}_1)}(A' \cup B' \cup x) S_{m+n-d}^{(R_2)}((\overline{A}\backslash A') \cup B) S_{m+n-d}^{(R_3)}(A \cup (\overline{B}\backslash B')),\end{aligned}$$

donde la suma está indexada por:

- todas las particiones $R := R_1 \sqcup R_2 \sqcup R_3$ del conjunto $\{1, \ldots, m' + n' - d\}$ con $R_1 \subset \{m + n - 2d, \ldots, m' + n' - d\}$, $|R_1| \leq d - (\overline{m} + \overline{n}) + 1$, $m' - d \leq |R_2| \leq m - d$ y $n' - d \leq |R_3| \leq n - d$,
- todos los subconjuntos $A' \subset \overline{A}$, $|A'| = |R_2| + d - m'$,
- todos los subconjuntos $B' \subset \overline{B}$, $|B'| = |R_3| + \text{mín}\{m', d - n'\}$,

y donde σ_R se especifica más adelante, en (4.4), y $\widetilde{R}_1 := \{i - (m + n - 2d - 1) : i \in R_1\}$.

Es fácil verificar que esta expresión generaliza en efecto la Definición 4.1.3, pues cuando $m' + n' \leq d$, se tiene $m' + n' - d \leq 0$, de modo que los conjuntos R_1, R_2 y R_3 de la suma son vacíos y además $|B'| = m'$. Así uno recupera la suma anterior con una sencilla operatoria.

El resultado principal de este capítulo es la siguiente generalización del Teorema 4.1.4, que muestra que $\text{SylM}_{d,0}(A, B)(x)$ coincide, salvo signo, con la subresultante en todos los casos.

Teorema 4.1.10. *Sean K un cuerpo y $f, g \in K[x]$ polinomios mónicos de grados m y n respectivamente, con multiconjuntos de raíces A y B, y $0 \leq d < \text{mín}\{m, n\}$ o $d = \text{mín}\{m, n\}$ si $m \neq n$. Entonces*

$$\text{Sres}_d(f, g)(x) = (-1)^{d(m-d)} \text{SylM}_{d,0}(A, B)(x).$$

Antes de demostrar el teorema volvamos a considerar el Ejemplo 4.1.5 para ilustrar cómo ahora, bajo la definición 4.1.9, el Teorema 4.1.10 efectivamente se cumple.

Ejemplo 4.1.11. Sean $f = (x - \alpha_1)(x - \alpha_2)^2$ y $g = (x - \beta_1)^3$ asociados a los multiconjuntos $A = (\alpha_1, \alpha_2, \alpha_2)$ con $\overline{A} = \{\alpha_1, \alpha_2\}$ y $B = (\beta_1, \beta_1, \beta_1)$ con $\overline{B} = \{\beta_1\}$, y tomemos $d = 2$. Tenemos $\text{Sres}_2(f, g)(x) = g(x) - f(x)$, y en este caso $\text{SylM}_{2,0}(A, B)(x)$ es igual a

$$\begin{aligned}(\alpha_2 - \beta_1)(x - \alpha_1)(x - \alpha_2) - \frac{(\alpha_1 - \beta_1)(\alpha_1 - \beta_1)(x - \alpha_2)(x - \beta_1)}{\alpha_2 - \alpha_1} \\ - \frac{(\alpha_2 - \beta_1)(\alpha_2 - \beta_1)(x - \alpha_1)(x - \beta_1)}{\alpha_1 - \alpha_2}.\end{aligned}$$

Es fácil verificar que estas dos expresiones coinciden.

El Teorema 4.1.10 será consecuencia inmediata del siguiente teorema.

Teorema 4.1.12. *Sean A y B subconjuntos de un cuerpo K, con $|A| = m$ y $|B| = n$. Sean $\overline{A} \subset A$ y $\overline{B} \subset B$ subconjuntos no vacíos de A y B respectivamente, con $|\overline{A}| = \overline{m}$ y $|\overline{B}| = \overline{n}$ y sean $m' := m - \overline{m}$ y $n' := n - \overline{n}$. Supongamos que $0 \leq d < \min\{m, n\}$ o $d = \min\{m, n\}$ si $m \neq n$, y que satisface además $d < m' + n'$. Entonces:*

(1) Si $0 \leq d < \overline{m} + \overline{n}$ se tiene

$$\sum_{\substack{A_1 \cup A_2 = A,\, |A_1| = d,\\ |A_2| = m-d}} \frac{\mathcal{R}(A_2, B)\mathcal{R}(x, A_1)}{\mathcal{R}(A_1, A_2)} = \sum_{\substack{R_2 \cup R_3 = \{1,\ldots,m'+n'-d\}\\ |R_2| = r_2,\, m'-d \leq r_2 \leq m-d\\ |R_3| = r_3,\, n'-d \leq r_3 \leq n-d}} (-1)^{\sigma_R}$$

$$\cdot \sum_{\substack{A' \subset \overline{A}\\ |A'| = r_2 - (m'-d)}} \sum_{\substack{B' \subset \overline{B}\\ |B'| = r_3 - (n'-d)}} \frac{\mathcal{R}(A \backslash \overline{A}, \overline{B} \backslash B')\mathcal{R}(\overline{A} \backslash A', B \backslash B')\mathcal{R}(x, A')\mathcal{R}(x, B')}{\mathcal{R}(A', \overline{A} \backslash A')\mathcal{R}(B', \overline{B} \backslash B')}$$

$$\cdot\, S^{(R_2)}_{m+n-d}((\overline{A} \backslash A') \cup B) S^{(R_3)}_{m+n-d}(A \cup (\overline{B} \backslash B')),$$

donde, para la partición $R := R_2 \sqcup R_3$ de $\{1, \ldots, m' + n' - d\}$,

$$(-1)^{\sigma_R} = (-1)^{m'(m-d) + r_2(\overline{m}-1) + r_3(m'+n'-d-1) + r_2 r_3} \mathrm{sg}(R).$$

(2) Si $\overline{m} + \overline{n} \leq d < m' + n'$,

$$\sum_{\substack{A_1 \cup A_2 = A\\ |A_1| = d,\, |A_2| = m-d}} \frac{\mathcal{R}(A_2, B)\mathcal{R}(x, A_1)}{\mathcal{R}(A_1, A_2)} = \sum_{\substack{R_1 \cup R_2 \cup R_3 = \{1,\ldots,m'+n'-d\}\\ R_1 \subset \{m+n-2d,\ldots,m'+n'-d\},\\ |R_1| = r_1,\, r_1 \leq d - (\overline{m}+\overline{n}) + 1\\ |R_2| = r_2,\, m'-d \leq r_2 \leq m-d\\ |R_3| = r_3,\, n'-d \leq r_3 \leq n-d}} (-1)^{\sigma_R}$$

$$\cdot \sum_{\substack{A' \subset \overline{A}\\ |A'| = r_2 - (m'-d)}} \sum_{\substack{B' \subset \overline{B}\\ |B'| = r_3 - (n'-d)}} \frac{\mathcal{R}(A \backslash \overline{A}, \overline{B} \backslash B')\mathcal{R}(\overline{A} \backslash A', B \backslash B')\mathcal{R}(x, A')\mathcal{R}(x, B')}{\mathcal{R}(A', \overline{A} \backslash A')\mathcal{R}(B', \overline{B} \backslash B')}$$

$$\cdot\, S^{(\widetilde{R}_1)}_{d+1}(A' \cup B' \cup x) S^{(R_2)}_{m+n-d}((\overline{A} \backslash A') \cup B) S^{(R_3)}_{m+n-d}(A \cup (\overline{B} \backslash B')),$$

donde, para la partición $R = R_1 \sqcup R_2 \sqcup R_3$ de $\{1, \ldots, m' + n' - d\}$,

$$(-1)^{\sigma_R} = (-1)^{m'(m-d) + r_1(n-d+r_2+r_3) + r_2(\overline{m}-1) + r_3(m'+n'-d-1) + r_2 r_3} \mathrm{sg}(R), \tag{4.4}$$

y $\widetilde{R}_1 := \{i - (m + n - 2d - 1) : i \in R_1\}$.

Demostración. Como en la demostración del Teorema 4.1.6, podemos suponer que $A \cap B = \emptyset$. Como dijimos, la idea de la demostración es agregar un conjunto auxiliar de variables $T = \{t_1, \cdots, t_r\}$ con $r = m' + n' - d$, de modo que el conjunto $E := \overline{A} \cup \overline{B} \cup T$ tiene tamaño $|E| = m + n - d$, lo cual nos permite aplicar la Proposición 4.1.2 a E y $X = \{x\}$, y luego comparar coeficientes en la expresión que se obtiene.

Aplicando la Proposición 4.1.2 tenemos

$$\sum_{\substack{A_1 \cup A_2 = A\\ |A_1| = d,\, |A_2| = m-d}} \frac{\mathcal{R}(A_2, B)\mathcal{R}(x, A_1)}{\mathcal{R}(A_1, A_2)} = \sum_{\substack{E_1 \cup E_2 \cup E_3 = \overline{A} \cup \overline{B} \cup T\\ |E_1| = d, |E_2| = m-d\\ |E_3| = n-d}} \frac{\mathcal{R}(A, E_3)\mathcal{R}(E_2, B)\mathcal{R}(x, E_1)}{\mathcal{R}(E_1, E_2)\mathcal{R}(E_1, E_3)\mathcal{R}(E_2, E_3)}.$$

Como en la demostración del Teorema 4.1.6, $\mathcal{R}(A, E_3) = \emptyset$ si $E_3 \cap A \neq \emptyset$ y $\mathcal{R}(E_2, B) = \emptyset$ si $E_2 \cap B \neq \emptyset$. Luego $E_3 \subset \overline{B} \cup T$ y $E_2 \subset \overline{A} \cup T$. Escribamos $E_2 = (\overline{A} \backslash A') \cup T_2$ con $A' \subset \overline{A}$ y $T_2 \subset T$, $E_3 = (\overline{B} \backslash B') \cup T_3$ con $B' \subset \overline{B}$ y $T_3 \subset T$ con $T_2 \cap T_3 = \emptyset$. Entonces $E_1 = (A' \cup B') \cup T_1$ donde $T_1 = T \backslash (T_2 \cup T_3)$, y podemos reescribir la suma como hicimos en el Teorema 4.1.6:

$$\sum_{\substack{T_1 \cup T_2 \cup T_3 = T \\ |T_1| = r_1, 0 \leq r_1 \leq d \\ |T_2| = r_2, 0 \leq r_2 \leq m-d \\ |T_3| = r_3, 0 \leq r_3 \leq n-d}} \sum_{\substack{A' \subset \overline{A} \\ |A'| = r_2 + d - m' \\ 0 \leq |A'| \leq \overline{m}}} \sum_{\substack{B' \subset \overline{B} \\ |B'| = r_3 + d - n' \\ 0 \leq |B'| \leq \overline{n}}}$$

$$\frac{\mathcal{R}(A, (\overline{B} \backslash B') \cup T_3) \mathcal{R}((\overline{A} \backslash A') \cup T_2, B) \mathcal{R}(x, (A' \cup B') \cup T_1)}{\mathcal{R}((A' \cup B') \cup T_1, (\overline{A} \backslash A') \cup T_2) \mathcal{R}((A' \cup B') \cup T_1, (\overline{B} \backslash B') \cup T_3) \mathcal{R}((\overline{A} \backslash A') \cup T_2, (\overline{B} \backslash B') \cup T_3)}$$

$$= \sum_{\substack{T_1 \cup T_2 \cup T_3 = T \\ |T_1| = r_1, 0 \leq r_1 \leq d \\ |T_2| = r_2, \max\{0, m'-d\} \leq r_2 \leq m-d \\ |T_3| = r_3, \max\{0, n'-d\} \leq r_3 \leq n-d}} \sum_{\substack{A' \subset \overline{A} \\ |A'| = r_2 - (m'-d)}} \sum_{\substack{B' \subset \overline{B} \\ |B'| = r_3 - (n'-d)}}$$

$$\frac{\mathcal{R}(A, (\overline{B} \backslash B') \cup T_3) \mathcal{R}((\overline{A} \backslash A') \cup T_2, B) \mathcal{R}(x, (A' \cup B') \cup T_1)}{\mathcal{R}((A' \cup B') \cup T_1, (\overline{A} \backslash A') \cup T_2) \mathcal{R}((A' \cup B') \cup T_1, (\overline{B} \backslash B') \cup T_3) \mathcal{R}((\overline{A} \backslash A') \cup T_2, (\overline{B} \backslash B') \cup T_3)}.$$

Aquí, para cada elección de T_1, T_2, T_3 y A', B', el numerador es igual a

$$\mathcal{R}(A, \overline{B} \backslash B') \mathcal{R}(A, T_3) \mathcal{R}(\overline{A} \backslash A', B) \mathcal{R}(T_2, B) \mathcal{R}(x, A') \mathcal{R}(x, B') \mathcal{R}(x, T_1),$$

mientras que el denominador puede reescribirse como

$$\begin{aligned} &\mathcal{R}(A' \cup B', \overline{A} \backslash A') \mathcal{R}(A' \cup B', T_2) \mathcal{R}(T_1, \overline{A} \backslash A') \mathcal{R}(T_1, T_2) \\ &\cdot \mathcal{R}(A' \cup B', \overline{B} \backslash B') \mathcal{R}(A' \cup B', T_3) \mathcal{R}(T_1, \overline{B} \backslash B') \mathcal{R}(T_1, T_3) \\ &\cdot \mathcal{R}(\overline{A} \backslash A', \overline{B} \backslash B') \mathcal{R}(\overline{A} \backslash A', T_3) \mathcal{R}(T_2, \overline{B} \backslash B') \mathcal{R}(T_2, T_3). \end{aligned}$$

Por lo tanto, la parte del cociente que es independiente de los T_ℓ es igual a, como en el Teorema 4.1.6,

$$(-1)^{\sigma_1} \sum_{\substack{A' \subset \overline{A} \\ |A'| = r_2 - (m'-d)}} \sum_{\substack{B' \subset \overline{B} \\ |B'| = r_3 - (n'-d)}} \frac{\mathcal{R}(A \backslash \overline{A}, \overline{B} \backslash B') \mathcal{R}(\overline{A} \backslash A', B \backslash B') \mathcal{R}(x, A') \mathcal{R}(x, B')}{\mathcal{R}(A', \overline{A} \backslash A') \mathcal{R}(B', \overline{B} \backslash B')},$$

donde $\sigma_1 := |B'|\,|\overline{A} \backslash A'|$.

Nos ocuparemos ahora de la parte del cociente que involucra algún T_ℓ. Multiplicando y dividiendo por $\mathcal{R}(T_1, A' \cup B') \mathcal{R}(T_2, \overline{A} \backslash A') \mathcal{R}(T_3, \overline{B} \backslash B')$, el cociente resulta

$$(-1)^{\sigma_2} \frac{\mathcal{R}(T_3, A \cup (\overline{B} \backslash B')) \mathcal{R}(T_2, (\overline{A} \backslash A') \cup B) \mathcal{R}(T_1, A' \cup B' \cup x)}{\mathcal{R}(T, \overline{A} \cup \overline{B}) \mathcal{R}(T_1, T_2) \mathcal{R}(T_1, T_3) \mathcal{R}(T_2, T_3)},$$

donde $\sigma_2 := |T_3|\,|\overline{A} \backslash A'| + (|T_2| + |T_3|)|A' \cup B'| + |T_3|\,|A| + |T_1|$.
Ahora multiplicamos y dividimos por el producto de los determinantes de Vandermonde

$V(T_1)V(T_2)V(T_3)$, donde consideramos en cada T_ℓ los elementos t_i con los índices i en orden creciente, y tenemos

$$\frac{\mathcal{R}(T_3, A \cup (\overline{B}\backslash B'))\mathcal{R}(T_2, (\overline{A}\backslash A') \cup B)\mathcal{R}(T_1, A' \cup B' \cup x)V(T_1)V(T_2)V(T_3)}{\mathcal{R}(T, \overline{A} \cup \overline{B})\mathcal{R}(T_1, T_2)\mathcal{R}(T_1, T_3)\mathcal{R}(T_2, T_3)V(T_1)V(T_2)V(T_3)}$$
$$= \operatorname{sg}(T_1, T_2, T_3)\frac{\mathcal{R}(T_3, A \cup (\overline{B}\backslash B'))\mathcal{R}(T_2, (\overline{A}\backslash A') \cup B)\mathcal{R}(T_1, A' \cup B' \cup x)V(T_1)V(T_2)V(T_3)}{\mathcal{R}(T, \overline{A} \cup \overline{B})V(T)},$$

con $\operatorname{sg}(T_1, T_2, T_3) := (-1)^\sigma$, donde σ es la paridad del número de transposiciones necesarias para llevar el conjunto ordenado $T_1 \cup T_2 \cup T_3$ a $\{t_1, \ldots, t_r\}$.

Dado que el denominador es independiente de las elecciones de los T_ℓ, volviendo a la primera expresión, tenemos

$$\begin{aligned}
\mathcal{R}(T, \overline{A} \cup \overline{B})V(T) & \sum_{\substack{A_1 \cup A_2 = A \\ |A_1| = d,\, |A_2| = m-d}} \frac{\mathcal{R}(A_2, B)\mathcal{R}(x, A_1)}{\mathcal{R}(A_1, A_2)} \\
&= \sum_{\substack{T_1 \cup T_2 \cup T_3 = T \\ |T_1| = r_1, 0 \le r_1 \le d \\ |T_2| = r_2, \max\{0, m'-d\} \le r_2 \le m-d \\ |T_3| = r_3, \max\{0, n'-d\} \le r_3 \le n-d}} (-1)^{\sigma'} \operatorname{sg}(T_1, T_2, T_3) \\
&\cdot \sum_{\substack{A' \subset \overline{A} \\ |A'| = r_2 - (m'-d))}} \sum_{\substack{B' \subset \overline{B} \\ |B'| = r_3 - (n'-d)}} \frac{\mathcal{R}(A\backslash\overline{A}, \overline{B}\backslash B')\mathcal{R}(\overline{A}\backslash A', B\backslash B')\mathcal{R}(x, A')\mathcal{R}(x, B')}{\mathcal{R}(A', \overline{A}\backslash A')\mathcal{R}(B', \overline{B}\backslash B')} \\
&\cdot \mathcal{R}(T_3, A \cup (\overline{B}\backslash B'))\mathcal{R}(T_2, (\overline{A}\backslash A') \cup B)\mathcal{R}(T_1, A' \cup B' \cup x)V(T_1)V(T_2)V(T_3),
\end{aligned}$$

donde

$$\begin{aligned}
\sigma' :&= \sigma_1 + \sigma_2 \\
&= (|B'| + |T_3|)|\overline{A}\backslash A'| + (|T_2| + |T_3|)|A' \cup B'| + |T_3|\,|A| + |T_1| \\
&\equiv (n' - d)(m - d) + r_1 + r_2(m' - d + 1) + r_3(n' - \overline{m} + 1) \pmod 2 \\
&\equiv m'(m - d) + r_1(m - d - 1) + r_2(\overline{m} - 1) + r_3(m' + n' - d - 1) \pmod 2.
\end{aligned}$$

(La última fila está escrita de modo que coincide con el exponente en el Teorema 4.1.6; cuando $r < 0$ interpretamos $r_1 = r_2 = r_3 = 0$.)

Para recuperar la suma que queremos, tomamos un coeficiente específico en $(t_1, \ldots, t_r)$ a ambos lados. Notemos que el coeficiente principal de $\mathcal{R}(T, \overline{A} \cup \overline{B})V(T)$ con respecto al orden lexicográfico $t_1 > \cdots > t_r$, es igual a

$$\operatorname{coeff}_{t_1^{m+n-d-1} t_2^{m+n-d-2} \cdots t_r^{m+n-d-r}} \left(\mathcal{R}(T, \overline{A} \cup \overline{B})V(T)\right) = 1.$$

Miremos ahora este coeficiente en el miembro derecho de toda la expresión: lo haremos considerando las variables t_i que pertenecen a cada T_ℓ. Miremos primero las variables en T_2, y luego en T_3, ya que se comportan de manera similar.
Observemos que

$$\mathcal{R}(T_2, (\overline{A}\backslash A') \cup B)V(T_2) = \frac{V(T_2 \cup (\overline{A}\backslash A') \cup B)}{V((\overline{A}\backslash A') \cup B)},$$

y

$$\mathcal{R}(T_3, A \cup (\overline{B}\backslash B'))V(T_3) = \frac{V(T_3 \cup A \cup (\overline{B}\backslash B'))}{V(A \cup (\overline{B}\backslash B'))},$$

donde las matrices del numerador de los miembros derechos son ambas de tamaño $(m+n-d)\times(m+n-d)$. El coeficiente del monomio $\prod_{t_i\in T_2} t_i^{m+n-d-i}$ corresponde en el numerador a la submatriz de $\mathcal{V}_{m+n-d}((\overline{A}\backslash A')\cup B)$ en donde se han quitado las filas indexadas por $R_2 := \{i : t_i \in T_2\}$. Luego

$$\begin{aligned}\operatorname{coeff}_{\prod_{t_i\in T_2} t_i^{m+n-d-i}}\left(\frac{V(T_2\cup(\overline{A}\backslash A')\cup B)}{V((\overline{A}\backslash A')\cup B)}\right) &= \operatorname{sg}_{m+n-d}(R_2)S^{(R_2)}_{m+n-d}((\overline{A}\backslash A')\cup B)\\ &= \operatorname{sg}_{m'+n'-d}(R_2)S^{(R_2)}_{m+n-d}((\overline{A}\backslash A')\cup B),\end{aligned}$$

pues $R_2 \subset \{1,\dots,m'+n'-d\}$. Análogamente

$$\operatorname{coeff}_{\prod_{t_i\in T_3} t_i^{m+n-d-i}}\left(\frac{V(T_3\cup A\cup(\overline{B}\backslash B'))}{V(A\cup(\overline{B}\backslash B'))}\right) = \operatorname{sg}_{m'+n'-d}(R_3)S^{(R_3)}_{m+n-d}(A\cup(\overline{B}\backslash B')),$$

donde $R_3 := \{i : t_i \in T_3\}$.

Ahora vemos qué pasa con las variables en T_1. Observemos que

$$\mathcal{R}(T_1, A'\cup B'\cup x)V(T_1) = \frac{V(T_1\cup A'\cup B'\cup x)}{V(A'\cup B'\cup x)}.$$

Aquí la matriz del numerador es una matriz de Vandermonde de tamaño $(d+1)\times(d+1)$ y el máximo exponente de t_i para $t_i \in T_1$ que puede aparecer es t_i^d. Sea $R_1 := \{i : t_i \in T_1\}$. Entonces, para cada $i \in R_1$ necesitamos $m+n-d-i \subset \{0,1,\dots,d\}$, i.e. $m+n-2d \le i \le m+n-d$. Dado que i satisface $i \le r = m'+n'-d$, necesitamos que $m+n-2d \le m'+n'-d$ y $R_1 \subset \{m+n-2d,\dots,m'+n'-d\}$.
En particular, cuando $m+n-2d > m'+n'-d$, i.e. cuando $d < \overline{m}+\overline{n}$, no hay ninguna elección para R_1. En este caso concluimos

$$\begin{aligned}\sum_{\substack{A_1\cup A_2=A\\ |A_1|=d,\,|A_2|=m-d}} \frac{\mathcal{R}(A_2,B)\mathcal{R}(x,A_1)}{\mathcal{R}(A_1,A_2)} &= \sum_{\substack{R_2\cup R_3=\{1,\dots,m'+n'-d\}\\ |R_2|=r_2,\,\max\{0,m'-d\}\le r_2\le m-d\\ |R_3|=r_3,\,\max\{0,n'-d\}\le r_3\le n-d}} (-1)^\sigma \operatorname{sg}(R_2,R_3)\\ &\cdot \sum_{\substack{A'\subset\overline{A}\\ |A'|=r_2-(m'-d)}}\ \sum_{\substack{B'\subset\overline{B}\\ |B'|=r_3-(n'-d)}} \frac{\mathcal{R}(A\backslash\overline{A},\overline{B}\backslash B')\mathcal{R}(\overline{A}\backslash A',B\backslash B')\mathcal{R}(x,A')\mathcal{R}(x,B')}{\mathcal{R}(A',\overline{A}\backslash A')\mathcal{R}(B',\overline{B}\backslash B')}\\ &\cdot S^{(R_2)}_{m+n-d}((\overline{A}\backslash A')\cup B)S^{(R_3)}_{m+n-d}(A\cup(\overline{B}\backslash B')),\end{aligned}$$

donde

$$\sigma = m'(m-d) + r_2(\overline{m}-1) + r_3(m'+n'-d-1) + r_2r_3,$$

pues es fácil ver que $\operatorname{sg}_{m'+n'-d}(R_2)\operatorname{sg}_{m'+n'-d}(R_3) = (-1)^{r_2r_3}$ ya que R_2 y R_3 son conjuntos complementarios en $\{1,\dots,m'+n'-d\}$ (o ver el Lema 4.1.13 más abajo).

Ahora, si $d \ge \overline{m}+\overline{n}$ y $R_1 = \{i : t_i \in T_1\} \subset \{m+n-2d,\dots,m'+n'-d\}$ tenemos

$$\operatorname{coeff}_{\prod_{t_i\in T_1} t_i^{m+n-d-i}}\left(\frac{V(T_1\cup A'\cup B'\cup x)}{V(A'\cup B'\cup x)}\right) = \operatorname{sg}_{d+1}(\widetilde{R}_1)S^{(\widetilde{R}_1)}_{d+1}(A'\cup B'\cup x),$$

donde $\widetilde{R}_1 := \{i-(m+n-2d-1) : i \in R_1\} \subset \{1,\dots,d+1-(\overline{m}+\overline{n})\}$. Probamos en el Lema 4.1.13 más abajo que

$$\mathrm{sg}_{d+1}(\widetilde{R}_1)\mathrm{sg}_{m'+n'-d}(R_2)\mathrm{sg}_{m'+n'-d}(R_3) = (-1)^{r_1(r_2+r_3+m+n-1)+r_2r_3}.$$

De este modo, tenemos

$$\sum_{\substack{A_1\cup A_2=A\\ |A_1|=d,\,|A_2|=m-d}} \frac{\mathcal{R}(A_2,B)\mathcal{R}(x,A_1)}{\mathcal{R}(A_1,A_2)} = \sum_{\substack{R_1\cup R_2\cup R_3=\{1,\dots,m'+n'-d\}\\ R_1\subset\{m+n-2d,\dots,m'+n'-d\},\\ |R_1|=r_1,0\le r_1\le d-(\overline{m}+\overline{n})+1\\ |R_2|=r_2,\max\{0,m'-d\}\le r_2\le m-d\\ |R_3|=r_3,\max\{0,n'-d\}\le r_3\le n-d}} (-1)^{\sigma}\,\mathrm{sg}(R_1,R_2,R_3)$$

$$\cdot \sum_{\substack{A'\subset\overline{A}\\ |A'|=r_2-(m'-d)}} \sum_{\substack{B'\subset\overline{B}\\ |B'|=r_3-(n'-d)}} \frac{\mathcal{R}(A\backslash\overline{A},\overline{B}\backslash B')\mathcal{R}(\overline{A}\backslash A',B\backslash B')\mathcal{R}(x,A')\mathcal{R}(x,B')}{\mathcal{R}(A',\overline{A}\backslash A')\mathcal{R}(B',\overline{B}\backslash B')}$$

$$\cdot\, S_{d+1}^{(\widetilde{R}_1)}(A'\cup B'\cup x)\, S_{m+n-d}^{(R_2)}((\overline{A}\backslash A')\cup B)\, S_{m+n-d}^{(R_3)}(A\cup(\overline{B}\backslash B')),$$

donde

$$\sigma = m'(m-d)+r_1(n-d+r_2+r_3)+r_2(\overline{m}-1)+r_3(m'+n'-d-1)+r_2r_3.$$

□

Lema 4.1.13. *Sea $R_1\sqcup R_2\sqcup R_3$ una partición de $\{1,\dots,r\}$ con $|R_i|=r_i$ para $1\le i\le 3$, y sea $0\le s\le r$ tal que $\widetilde{R}_1=\{i-s : i\in R_1\}\subset\{1,\dots,r-s\}$. Entonces*

$$\mathrm{sg}_{r-s}(\widetilde{R}_1)\,\mathrm{sg}_r(R_2)\,\mathrm{sg}_r(R_3) = (-1)^{r_1(r_2+r_3+s)+r_2r_3}.$$

Demostración. Escribamos $R_1=\{i_1,\dots,i_{r_1}\}$, $R_2=\{j_1,\dots,j_{r_2}\}$ y $R_3=\{k_1,\dots,k_{r_3}\}$. Entonces

$$\begin{aligned}
\mathrm{sg}_{r-s}(\widetilde{R}_1)\,\mathrm{sg}_r(R_2)\,\mathrm{sg}_r(R_3) &= \sum_{1\le\ell\le r_1}(i_\ell-s-\ell)+\sum_{1\le\ell\le r_2}(j_\ell-\ell)+\sum_{1\le\ell\le r_3}(k_\ell-\ell)\\
&= \frac{r(r+1)}{2}-r_1s-\frac{r_1(r_1+1)}{2}-\frac{r_2(r_2+1)}{2}-\frac{r_3(r_3+1)}{2}\\
&= \frac{r^2-r_1^2-r_2^2-r_3^2}{2}-r_1s\\
&= \frac{r^2-(r_1+r_2+r_3)^2+2r_1r_2+2r_1r_3+2r_2r_3}{2}-r_1s\\
&\equiv r_1r_2+r_1r_3+r_2r_3+r_1s \pmod 2.
\end{aligned}$$

□

Podemos ahora probar el Teorema 4.1.10.

Demostración del Teorema 4.1.10. Primero notemos que la definición de $\mathrm{SylM}_{d,0}(A,B)(x)$ en la Definición 4.1.9 no sólo es una generalización de la Definición 4.1.3 como hemos mencionado, sino que además generaliza el término en el miembro derecho del Teorema 4.1.12(1) para conjuntos, pues cuando $d<\overline{m}+\overline{n}$, $R_1\subset\{m+n-2d,\dots,m'+n'-d\}=\emptyset$.

Luego, gracias a los Teoremas 4.1.6 y 4.1.12, tenemos que la siguiente igualdad se satisface para conjuntos A y B, cualesquiera subconjuntos $\overline{A} \subset A$ y $\overline{B} \subset B$ y cualquier $0 \leq d < \text{mín}\{m,n\}$ o $d = \text{mín}\{m,n\}$ si $m \neq n$:

$$\text{Sres}_d(f,g)(x) = (-1)^{d(m-d)}\text{SylM}_{d,0}(A,B)(x).$$

El pasaje de conjuntos a multiconjuntos es luego natural tomando límites de conjuntos a multiconjuntos, como en la demostración del Teorema 4.1.4, gracias al Lema 4.1.8 y su demostración, dado que ambas expresiones están bien definidas para multiconjuntos. □

La suma $\text{SylM}_{d,0}(A,B)(x)$ es fácilmente computable mediante el programa Maple ([Map2016]). Con dicho programa desarrollamos un código que la calcula. Se puede acceder a este archivo con el siguiente link: http://cms.dm.uba.ar/Members/mvaldettaro/code.mw

4.2. Extensión de las sumas dobles de Sylvester

En la Sección 4.1 dimos una extensión de la definición de la suma simple de Sylvester para multiconjuntos, y como consecuencia, una fórmula para la subresultante en raíces en el caso general. Aquí extenderemos las sumas dobles $\text{Syl}_{p,q}(A,B)(x)$ y, en particular, también obtendremos otra fórmula para la subresultante. En esta parte sólo nos limitaremos al caso p y q suficientemente grandes.

En la sección anterior el punto de partida de la construcción fue la Proposición 4.1.2, que generaliza la fórmula de Apéry y Jouanalou de la Proposición 4.1.1. Allí logramos introducir un conjunto E arbitrario en la suma simple de Sylvester y eligiendo un E conveniente construimos la fórmula. Así como la suma simple es un caso particular de las sumas dobles, con $p = 0$ o $q = 0$, vamos a dar ahora una fórmula para las sumas dobles que generaliza la de la Proposición 4.1.2.

Proposición 4.2.1. *Sean A y B subconjuntos de un cuerpo K con $|A| = m$ y $|B| = n$ y sean $0 \leq p \leq m$, $0 \leq q \leq n$, con $d := p + q$. Sean X un conjunto de variables y $E, F \subset K$ subconjuntos finitos tales que*

$$|E| \geq \text{máx}\{|X| + d, m + n - d, m\} \quad y \quad |F| \geq \text{máx}\{|X| + d, m + n - d, n\}.$$

Entonces

$$\sum_{\substack{A_1 \cup A_2 = A \\ |A_1| = p \\ |A_2| = m-p}} \sum_{\substack{B_1 \cup B_2 = B \\ |B_1| = q \\ |B_2| = n-q}} \mathcal{R}(A_1,B_1)\mathcal{R}(A_2,B_2)\frac{\mathcal{R}(X,A_1)\mathcal{R}(X,B_1)}{\mathcal{R}(A_1,A_2)\mathcal{R}(B_1,B_2)}$$

$$= \sum_{\substack{E_1 \cup E_2 \cup E_3 = E \\ |E_1| = p \\ |E_2| = m-p \\ |E_3| = |E|-m}} \sum_{\substack{F_1 \cup F_2 \cup F_3 = F \\ |F_1| = q \\ |F_2| = n-q \\ |F_3| = |F|-n}} \frac{\mathcal{R}(A,E_3)\mathcal{R}(B,F_3)\mathcal{R}(E_2,F_2)\mathcal{R}(E_1,F_1)\mathcal{R}(X,E_1)\mathcal{R}(X,F_1)}{\mathcal{R}(E_1,E_2)\mathcal{R}(E_1,E_3)\mathcal{R}(E_2,E_3)\mathcal{R}(F_1,F_2)\mathcal{R}(F_1,F_3)\mathcal{R}(F_2,F_3)}.$$

Demostración.

$$\sum_{\substack{A_1\cup A_2=A\\|A_1|=p\\|A_2|=m-p}}\sum_{\substack{B_1\cup B_2=B\\|B_1|=q\\|B_2|=n-q}}\mathcal{R}(A_1,B_1)\mathcal{R}(A_2,B_2)\frac{\mathcal{R}(X,A_1)\mathcal{R}(X,B_1)}{\mathcal{R}(A_1,A_2)\mathcal{R}(B_1,B_2)}$$

$$=(-1)^{pq}\sum_{\substack{B_1\cup B_2=B\\|B_1|=q\\|B_2|=n-q}}\frac{\mathcal{R}(X,B_1)}{\mathcal{R}(B_1,B_2)}\sum_{\substack{A_1\cup A_2=A\\|A_1|=p\\|A_2|=m-p}}\frac{\mathcal{R}(A_2,B_2)\,\mathcal{R}(X\cup B_1,A_1)}{\mathcal{R}(A_1,A_2)}$$

$$=(-1)^{pq}\sum_{\substack{B_1\cup B_2=B\\|B_1|=q\\|B_2|=n-q}}\frac{\mathcal{R}(X,B_1)}{\mathcal{R}(B_1,B_2)}\sum_{\substack{E_1\cup E_2\cup E_3=E\\|E_1|=p\\|E_2|=m-p\\|E_3|=|E|-m}}\frac{\mathcal{R}(A,E_3)\mathcal{R}(E_2,B_2)\mathcal{R}(X\cup B_1,E_1)}{\mathcal{R}(E_1,E_2)\mathcal{R}(E_1,E_3)\mathcal{R}(E_2,E_3)} \tag{4.5}$$

$$=(-1)^{(m-p)(n-q)}\sum_{\substack{E_1\cup E_2\cup E_3=E\\|E_1|=p\\|E_2|=m-p\\|E_3|=|E|-m}}\frac{\mathcal{R}(A,E_3)\mathcal{R}(X,E_1)}{\mathcal{R}(E_1,E_2)\mathcal{R}(E_1,E_3)\mathcal{R}(E_2,E_3)}\sum_{\substack{B_1\cup B_2=B\\|B_1|=q\\|B_2|=n-q}}\frac{\mathcal{R}(B_2,E_2)\mathcal{R}(X\cup E_1,B_1)}{\mathcal{R}(B_1,B_2)}$$

$$=(-1)^{(m-p)(n-q)}\sum_{\substack{E_1\cup E_2\cup E_3=E\\|E_1|=p\\|E_2|=m-p\\|E_3|=|E|-m}}\frac{\mathcal{R}(A,E_3)\mathcal{R}(X,E_1)}{\mathcal{R}(E_1,E_2)\mathcal{R}(E_1,E_3)\mathcal{R}(E_2,E_3)}$$
$$\cdot\sum_{\substack{F_1\cup F_2\cup F_3=F\\|F_1|=q\\|F_2|=n-q\\|F_3|=|F|-n}}\frac{\mathcal{R}(B,F_3)\mathcal{R}(F_2,E_2)\mathcal{R}(X\cup E_1,F_1)}{\mathcal{R}(F_1,F_2)\mathcal{R}(F_1,F_3)\mathcal{R}(F_2,F_3)} \tag{4.6}$$

$$=\sum_{\substack{E_1\cup E_2\cup E_3=E\\|E_1|=p\\|E_2|=m-p\\|E_3|=|E|-m}}\sum_{\substack{F_1\cup F_2\cup F_3=F\\|F_1|=q\\|F_2|=n-q\\|F_3|=|F|-n}}\frac{\mathcal{R}(A,E_3)\mathcal{R}(B,F_3)\mathcal{R}(E_2,F_2)\mathcal{R}(E_1,F_1)\mathcal{R}(X,E_1)\mathcal{R}(X,F_1)}{\mathcal{R}(E_1,E_2)\mathcal{R}(E_1,E_3)\mathcal{R}(E_2,E_3)\mathcal{R}(F_1,F_2)\mathcal{R}(F_1,F_3)\mathcal{R}(F_2,F_3)},$$

usando en (4.5) la Proposición 4.1.2 con $B=B_2$, $d=p$ y como conjunto de variables $X\cup B_1$, en efecto $|E|\geq \text{máx}\{|X|+d, m+n-d, m\}=\text{máx}\{(|X|+|B_1|)+p, m+|B_2|-p, m\}$, y usando en (4.6) la misma proposición con $A=B$, $B=E_2$, $d=q$ y conjunto de variables $X\cup E_1$, en efecto $|F|\geq \text{máx}\{|X|+d, m+n-d, n\}=\text{máx}\{(|X|+|E_1|)+q, |B|+|E_2|-q, |B|\}$. □

Observemos que el caso $|X|=1$, la Proposición 4.2.1 nos da en efecto una fórmula para la suma doble $\text{Syl}_{p,q}(A,B)(x)$ que generaliza la de la Proposición 4.1.2, pues esta última es el caso $p=d$ y $q=0$ de la primera. Si bien esto no se ve de manera inmediata en el enunciado, es consecuencia de que en ese caso la suma en F resulta

$$\sum_{\substack{F_2\cup F_3=F\\|F_2|=n,|F_3|=|F|-n}}\frac{\mathcal{R}(B,F_3)\mathcal{R}(E_2,F_2)}{\mathcal{R}(F_2,F_3)}=\mathcal{R}(E_2,B),$$

por el Teorema 2.2.2.

Del mismo modo que en la Proposición 4.1.2, la Proposición 4.2.1 nos brindará una fórmula ahora para la suma doble para multiconjuntos eligiendo conjuntos E y F convenientes. Efectivamente, la expresión de la Proposición 4.2.1 tiene sentido para A y B multiconjuntos. Pero antes observemos, como corolario, que podemos obtener expresiones similares para los polinomios de la identidad de Bézout, pues a éstos los tenemos escritos en términos de ciertas sumas dobles particulares.

Corolario 4.2.2. *Sean f y g dos polinomios de grados m y n respectivamente con A y B los multiconjuntos asociados a sus respectivas raíces. Sean $d \leq \min\{m-1, n-1\}$ y $F \subset K$ finito tal que $|F| \geq m+n-d$. Entonces*

$$F_d(f,g) = (-1)^{m+(n-d)(d+1)+1} \sum_{\substack{F_1 \cup F_2 \cup F_3 = F \\ |F_1|=n-d-1, |F_2|=d+1 \\ |F_3|=|F|-n}} \frac{\mathcal{R}(B,F_3)\mathcal{R}(A\cup x, F_1)}{\mathcal{R}(F_1,F_2)\mathcal{R}(F_1,F_3)\mathcal{R}(F_2,F_3)},$$

$$G_d(f,g) = (-1)^{(m-d-1)(n-1)} \sum_{\substack{F_1 \cup F_2 \cup F_3 = F \\ |F_1|=m-d-1, |F_2|=d+1 \\ |F_3|=|F|-m}} \frac{\mathcal{R}(A,F_3)\mathcal{R}(B\cup x, F_1)}{\mathcal{R}(F_1,F_2)\mathcal{R}(F_1,F_3)\mathcal{R}(F_2,F_3)},$$

donde $F_d(f,g)$ y $G_d(f,g)$ son los polinomios de la identidad de Bézout definidos en la Proposición 1.1.4.

Demostración. Probaremos el enunciado para $F_d(f,g)$. La expresión para $G_d(f,g)$ se sigue de la igualdad

$$G_d(f,g) = (-1)^{(m-d)(n-d)} F_d(g,f),$$

que vimos en (1.3).

Por la Proposición 3.2.4 sabemos que

$$\mathrm{Syl}_{m,n-d-1}(A,B)(x) = (-1)^{m+(n-d)(d+1)+1} F_d(f,g) f(x),$$

de modo que basta ver que

$$\mathrm{Syl}_{m,n-d-1}(A,B)(x) = f(x) \sum_{\substack{F_1 \cup F_2 \cup F_3 = F \\ |F_1|=n-d-1, |F_2|=d+1 \\ |F_3|=|F|-n}} \frac{\mathcal{R}(B,F_3)\mathcal{R}(A\cup x, F_1)}{\mathcal{R}(F_1,F_2)\mathcal{R}(F_1,F_3)\mathcal{R}(F_2,F_3)}.$$

Y en efecto, por la Proposición 4.2.1, dados $E, F \subset K$ tales que $|F| \geq |E| = m+n-d$, y $|X| = 1$ tenemos

$$\mathrm{Syl}_{m,n-d-1}(A,B)(x) = \sum_{\substack{E_1 \cup E_3 = E \\ |E_1|=m, \\ |E_3|=n-d}} \sum_{\substack{F_1 \cup F_2 \cup F_3 = F \\ |F_1|=n-d-1, \\ |F_2|=d+1, \\ |F_3|=|F|-n}} \frac{\mathcal{R}(A,E_3)\mathcal{R}(B,F_3)\mathcal{R}(E_1,F_1)\mathcal{R}(x,E_1)\mathcal{R}(x,F_1)}{\mathcal{R}(E_1,E_3)\mathcal{R}(F_1,F_2)\mathcal{R}(F_1,F_3)\mathcal{R}(F_2,F_3)}$$

$$= (-1)^{m(n-d-1)} \sum_{\substack{F_1 \cup F_2 \cup F_3 = F \\ |F_1|=n-d-1, \\ |F_2|=d+1, \\ |F_3|=|F|-n}} \frac{\mathcal{R}(B,F_3)\mathcal{R}(x,F_1)}{\mathcal{R}(F_1,F_2)\mathcal{R}(F_1,F_3)\mathcal{R}(F_2,F_3)} \sum_{\substack{E_1 \cup E_3 = E \\ |E_1|=m, \\ |E_3|=n-d}} \frac{\mathcal{R}(E_3,A)\mathcal{R}(F_1\cup x, E_1)}{\mathcal{R}(E_3,E_1)}$$

$$= (-1)^{m(n-d-1)} \sum_{\substack{F_1\cup F_2\cup F_3=F\\ |F_1|=n-d-1,\\ |F_2|=d+1,\\ |F_3|=|F|-n}} \frac{\mathcal{R}(B,F_3)\mathcal{R}(x,F_1)}{\mathcal{R}(F_1,F_2)\mathcal{R}(F_1,F_3)\mathcal{R}(F_2,F_3)}\mathcal{R}(F_1\cup x, A) \tag{4.7}$$

$$= f(x) \sum_{\substack{F_1\cup F_2\cup F_3=F\\ |F_1|=n-d-1,\\ |F_2|=d+1,\\ |F_3|=|F|-n}} \frac{\mathcal{R}(B,F_3)\mathcal{R}(A\cup x,F_1)}{\mathcal{R}(F_1,F_2)\mathcal{R}(F_1,F_3)\mathcal{R}(F_2,F_3)},$$

usando en (4.7) el Teorema 2.2.2 con $A = E$, $B = A$, $d = m$ y con la variable $F_1 \cup x$, pues $|F_1| + 1 = n - d \leq m + n - d = |E| + |A| - m$. □

Ahora, del mismo modo que lo hicimos para la suma simple, definiremos una generalización $\mathrm{SylM}_{p,q}(A,B)(x)$ de la noción de suma doble de Sylvester $\mathrm{Syl}_{p,q}(A,B)(x)$, para multiconjuntos A y B y p y q suficientemente grandes.

Definición 4.2.3. Sea K un cuerpo, sean A, $B \subset K$ multiconjuntos con $|A| = m$, $|B| = n$ y sean $\overline{A} \subset A$ y $\overline{B} \subset B$ los conjuntos de elementos distintos de A y B respectivamente, con $|\overline{A}| = \overline{m}$, $|\overline{B}| = \overline{n}$. Sean $m' := m - \overline{m}$ y $n' := n - \overline{n}$ y sean $m' \leq p \leq m$ y $n' \leq q \leq n$ tales que $d := p + q \leq \min\{m, n\}$. Llamemos $p' := p - m'$ y $q' = q - n'$. Definimos

$$\mathrm{SylM}_{p,q}(A,B)(x) =$$
$$(-1)^e \sum_{\substack{A'\subset\overline{A}\\ |A'|=p'+n'}} \sum_{\substack{B'\subset\overline{B}\\ |B'|=q'+m'}} \frac{\mathcal{R}(A\backslash\overline{A},\overline{B}\backslash B')\mathcal{R}(\overline{A}\backslash A',B\backslash\overline{B})\mathcal{R}(\overline{A}\backslash A',\overline{B}\backslash B')\mathcal{R}(x,A')\mathcal{R}(x,B')}{\mathcal{R}(A',\overline{A}\backslash A')\mathcal{R}(B',\overline{B}\backslash B')}$$
$$\cdot \sum_{\substack{C\subset A'\cup B'\\ |C|=p}} \sum_{\substack{C'\subset C\\ |C'|=p'}} \frac{\mathcal{R}(C',B')}{\mathcal{R}(C',C\backslash C')},$$

con $e := (m' + n')(m - p) + qm'$.

Dada la relación $\mathrm{Syl}_{p,q}(A,B)(x) = (-1)^{pq+(m-p)(n-q)}\mathrm{Syl}_{q,p}(B,A)(x)$, que observamos en el Capítulo 1, es esperable que $\mathrm{SylM}_{p,q}(A,B)(x)$ y $\mathrm{SylM}_{q,p}(B,A)(x)$ también difieran en un signo. Esto no es evidente a partir de la definición pero el siguiente lema, que probaremos más adelante, lo demuestra.

Lema 4.2.4. *En las condiciones de la Definición 4.2.3 se tiene*

$$\sum_{\substack{C\subset A'\cup B'\\ |C|=p}} \sum_{\substack{C'\subset C\\ |C'|=p'}} \frac{\mathcal{R}(C',B')}{\mathcal{R}(C',C\backslash C')} = (-1)^{p'q'} \sum_{\substack{C\subset A'\cup B'\\ |C|=q}} \sum_{\substack{C'\subset C\\ |C'|=q'}} \frac{\mathcal{R}(C',A')}{\mathcal{R}(C',C\backslash C')}.$$

Para los valores de p y q en el rango de la Definición 4.2.3, aquí también tenemos un teorema análogo al Teorema 4.1.4.

Teorema 4.2.5. *Sean K un cuerpo y $f, g \in K[x]$ polinomios mónicos de grados m y n respectivamente, con multiconjuntos de raíces A y B, y conjuntos de raíces distintas $\overline{A}$*

y $\overline{B}$ respectivamente. Sean p y q como en la Definición 4.2.3 y tales que si $d := p + q$, entonces $0 \leq d < \text{mín}\{m, n\}$ o $d = \text{mín}\{m, n\}$ si $m \neq n$. Entonces

$$\binom{d}{p}\text{Sres}_d(f, g)(x) = (-1)^{p(m-d)}\text{SylM}_{p,q}(A, B)(x).$$

Para probar el Teorema 4.2.5 seguiremos un proceso análogo al que hicimos para el caso suma simple en la sección anterior. Dicho teorema será consecuencia del siguiente.

Teorema 4.2.6. *Sean A y B subconjuntos de un cuerpo K con $|A| = m$ y $|B| = n$. Sean $\overline{A} \subset A$ y $\overline{B} \subset B$ subconjuntos no vacíos de A y B, con $|\overline{A}| = \overline{m}$ y $|\overline{B}| = \overline{n}$ y sean $m' := m - \overline{m}$ y $n' := n - \overline{n}$. Sean $m' \leq p \leq m$ y $n' \leq q \leq n$ tales que $d := p + q \leq \text{mín}\{m, n\}$ y llamemos $p' := p - m'$ y $q' = q - n'$. Sea X un conjunto de variables tal que $|X| \leq m + n - 2d$. Entonces*

$$\sum_{\substack{A_1 \cup A_2 = A \\ |A_1| = p \\ |A_2| = m-p}} \sum_{\substack{B_1 \cup B_2 = B \\ |B_1| = q \\ |B_2| = n-q}} \mathcal{R}(A_1, B_1)\mathcal{R}(A_2, B_2)\frac{\mathcal{R}(X, A_1)\mathcal{R}(X, B_1)}{\mathcal{R}(A_1, A_2)\mathcal{R}(B_1, B_2)}$$

$$= (-1)^e \sum_{\substack{A' \subset \overline{A} \\ |A'| = p' + n'}} \sum_{\substack{B' \subset \overline{B} \\ |B'| = q' + m'}} \frac{\mathcal{R}(A\backslash\overline{A}, \overline{B}\backslash B')\mathcal{R}(\overline{A}\backslash A', B\backslash\overline{B})\mathcal{R}(\overline{A}\backslash A', \overline{B}\backslash B')\mathcal{R}(X, A')\mathcal{R}(X, B')}{\mathcal{R}(A', \overline{A}\backslash A')\mathcal{R}(B', \overline{B}\backslash B')}$$

$$\cdot \sum_{\substack{C \subset A' \cup B' \\ |C| = p}} \sum_{\substack{C' \subset C \\ |C'| = p'}} \frac{\mathcal{R}(C', B')}{\mathcal{R}(C', C\backslash C')},$$

con $e := (m' + n')(m - p) + qm'$.

Demostración. Suponemos que $A \cap B = \emptyset$, que no nos hará perder generalidad, del mismo modo que lo hicimos en la demostración del Teorema 4.1.6. Tomemos dos conjuntos E y F suficientemente grandes como en el enunciado de la Proposición 4.2.1; podemos pensarlos como conjuntos de variables que después evaluaremos eventualmente. Tenemos, por dicha proposición,

$$\sum_{\substack{A_1 \cup A_2 = A \\ |A_1| = p \\ |A_2| = m-p}} \sum_{\substack{B_1 \cup B_2 = B \\ |B_1| = q \\ |B_2| = n-q}} \mathcal{R}(A_1, B_1)\mathcal{R}(A_2, B_2)\frac{\mathcal{R}(X, A_1)\mathcal{R}(X, B_1)}{\mathcal{R}(A_1, A_2)\mathcal{R}(B_1, B_2)}$$

$$= \sum_{\substack{E_1 \cup E_2 \cup E_3 = E \\ |E_1| = p \\ |E_2| = m-p \\ |E_3| = |E|-m}} \sum_{\substack{F_1 \cup F_2 \cup F_3 = F \\ |F_1| = q \\ |F_2| = n-q \\ |F_3| = |F|-n}} \frac{\mathcal{R}(A, E_3)\mathcal{R}(B, F_3)\mathcal{R}(E_2, F_2)\mathcal{R}(E_1, F_1)\mathcal{R}(X, E_1)\mathcal{R}(X, F_1)}{\mathcal{R}(E_1, E_2)\mathcal{R}(E_1, E_3)\mathcal{R}(E_2, E_3)\mathcal{R}(F_1, F_2)\mathcal{R}(F_1, F_3)\mathcal{R}(F_2, F_3)}$$

$$= \sum_{\substack{E_1 \cup E_2 \cup E_3 = E \\ |E_1| = p \\ |E_2| = m-p \\ |E_3| = |E|-m}} \frac{\mathcal{R}(A, E_3)\mathcal{R}(X, E_1)}{\mathcal{R}(E_1, E_2)\mathcal{R}(E_1, E_3)\mathcal{R}(E_2, E_3)} \sum_{\substack{F_1 \cup F_2 \cup F_3 = F \\ |F_1| = q \\ |F_2| = n-q \\ |F_3| = |F|-n}} \frac{\mathcal{R}(B, F_3)\mathcal{R}(E_2, F_2)\mathcal{R}(E_1 \cup X, F_1)}{\mathcal{R}(F_1, F_2)\mathcal{R}(F_1, F_3)\mathcal{R}(F_2, F_3)}$$

$$= (-1)^{(m-p)(n-q)} \sum_{\substack{E_1\cup E_2\cup E_3=E\\ |E_1|=p\\ |E_2|=m-p\\ |E_3|=|E|-m}} \frac{\mathcal{R}(A,E_3)\mathcal{R}(X,E_1)}{\mathcal{R}(E_1,E_2)\mathcal{R}(E_1,E_3)\mathcal{R}(E_2,E_3)}$$

$$\cdot \sum_{\substack{B_1\cup B_2=B\\ |B_1|=q,|B_2|=n-q}} \frac{\mathcal{R}(B_2,E_2)\mathcal{R}(E_1\cup X,B_1)}{\mathcal{R}(B_1,B_2)} \tag{4.8}$$

$$= (-1)^{(m-p)(n-q)+n'(n-q)} \sum_{\substack{E_1\cup E_2\cup E_3=E\\ |E_1|=p\\ |E_2|=m-p\\ |E_3|=|E|-m}} \frac{\mathcal{R}(A,E_3)\mathcal{R}(X,E_1)}{\mathcal{R}(E_1,E_2)\mathcal{R}(E_1,E_3)\mathcal{R}(E_2,E_3)}$$

$$\cdot \sum_{\substack{B''\subset\overline{B}\\ |B''|=q-n'}} \sum_{\substack{E_2'\subset E_2\\ |E_2'|=n'}} \frac{\mathcal{R}(B\backslash\overline{B},E_2\backslash E_2')\mathcal{R}(\overline{B}\backslash B'',E_2\backslash E_2')\mathcal{R}(E_1\cup X,B'')\mathcal{R}(E_1\cup X,E_2')}{\mathcal{R}(B'',\overline{B}\backslash B'')\mathcal{R}(E_2',E_2\backslash E_2')}. \tag{4.9}$$

Hemos usado en (4.8) la Proposición 4.1.2 con $A = B$, $B = E_2$, $d = q$ y como conjunto de variables $E_1 \cup X$, en efecto $|E_1| + |X| = p + |X| \leq p + m + n - 2d = |B| + |E_2| - 2q$; y en (4.9) el Teorema 4.1.6 con las mismas identificaciones y tomando $\overline{E_2} = E_2$, en efecto, en este caso, la hipótesis $m' + n' \leq d \leq \min\{m, n\}$ se traduce en $n' + 0 \leq q \leq \min\{m, n\}$, que es cierto. Llamamos ahora $E_2'' := E_2\backslash E_2'$ y reescribimos

$$(-1)^{\sigma} \sum_{\substack{B'\subset\overline{B}\\ |B''|=q'}} \frac{\mathcal{R}(X,B'')}{\mathcal{R}(B'',\overline{B}\backslash B'')} \sum_{\substack{E_1\cup E_2'\cup E_2''\cup E_3=E\\ |E_1|=p,|E_2'|=n'\\ |E_2''|=m-p-n'\\ |E_3|=|E|-m}} \frac{\mathcal{R}(A,E_3)\mathcal{R}(B\backslash B'',E_2'')\mathcal{R}(B''\cup X,E_1)\mathcal{R}(X,E_2')}{\mathcal{R}(E_1\cup E_2',E_2'')\mathcal{R}(E_1\cup E_2',E_3)\mathcal{R}(E_2'',E_3)},$$

con $\sigma := (m-p)(n-q) + n'(n-q) + pq'$. Ahora, dado un B'' fijo, la segunda suma es de la forma de la del miembro derecho de la igualdad de la Proposición 2.2.11 con $A = E$, donde la condición $|A| \geq \max\{|X'| + p, |X''| + p, |Y| + q, |B|\}$ del enunciado se traduce en

$$\begin{aligned} |E| &\geq \max\{(|B''| + |X|) + p + n', |X| + p + n', |\overline{B}\backslash B''| + m - p - n', m\} \\ &= \max\{(|B''| + |X|) + p + n', |\overline{B}\backslash B''| + m - p - n', m\} \\ &= \max\{q' + |X| + p + n', \overline{n} - q' + m - p - n', m\} \\ &= \max\{|X| + d, m + \overline{n} - d, m\}. \end{aligned} \tag{4.10}$$

En particular, por dicha proposición, la suma no depende de E si su tamaño es suficientemente grande. Por otro lado, la Proposición 4.2.1 que usamos al principio nos pedía

$$|E| \geq \max\{|X| + d, m + n - d, m\},$$

de modo que esta última condición implica (4.10). Además, bajo las hipótesis que tenemos: $\max\{|X| + d, m + n - d, m\} = m + n - d$. De esta manera, dicha suma tendrá un valor invariante si fijamos un conjunto E tal que $|E| \geq m + n - d$. Dado entonces B'' fijo, tomamos $E = \overline{A} \cup (\overline{B}\backslash B'')$. Verifiquemos que dicho conjunto tiene tamaño correcto. En efecto: $|\overline{A} \cup (\overline{B}\backslash B'')| = \overline{m} + \overline{n} - q' = \overline{m} + n - q$. Y tenemos

$$\overline{m} + n - q \geq m + n - d \iff p \geq m',$$

que es otra de las hipótesis. Tenemos entonces

$$(-1)^{\sigma} \sum_{\substack{B''\subset\overline{B}\\|B''|=q'}} \frac{\mathcal{R}(X,B'')}{\mathcal{R}(B'',\overline{B}\backslash B'')} \cdot \sum_{\substack{E_1\cup E_2'\cup E_2''\cup E_3=\overline{A}\cup(\overline{B}\backslash B'')\\|E_1|=p,|E_2'|=n'\\|E_2''|=m-p-n'\\|E_3|=n-q-m'}} \frac{\mathcal{R}(A,E_3)\mathcal{R}(B\backslash B'',E_2'')\mathcal{R}(B''\cup X,E_1)\mathcal{R}(X,E_2')}{\mathcal{R}(E_1\cup E_2',E_2'')\mathcal{R}(E_1\cup E_2',E_3)\mathcal{R}(E_2'',E_3)}.$$

Ahora, $\mathcal{R}(A,E_3)=0$ cuando $A\cap E_3\neq\emptyset$, y $\mathcal{R}(B\backslash B'',E_2'')=0$ cuando $\overline{B}\backslash B''\cap E_2''\neq\emptyset$. Luego $E_3\subset(\overline{B}\backslash B'')$ y $E_2''\subset\overline{A}$. Llamemos $A':=\overline{A}\backslash E_2''$ y $B'''':=(\overline{B}\backslash B'')\backslash E_3$. Tenemos $|A'|=\overline{m}-(m-p-n')=p'+n'$ y $|B''''|=\overline{n}-q'-(n-q-m')=m'$ y además $E_1\cup E_2'=A'\cup B''''$. Entonces queda

$$(-1)^{\sigma} \sum_{\substack{B''\subset\overline{B}\\|B''|=q'}} \frac{\mathcal{R}(X,B'')}{\mathcal{R}(B'',\overline{B}\backslash B'')} \sum_{\substack{A'\subset\overline{A}\\|A'|=p'+n'}} \sum_{\substack{B''''\subset\overline{B}\backslash B''\\|B''''|=m'}} \sum_{\substack{E_1\cup E_2'=A'\cup B''''\\|E_1|=p,|E_2'|=n'}} \frac{\mathcal{R}(A,\overline{B}\backslash(B''\cup B''''))\mathcal{R}(B\backslash B'',\overline{A}\backslash A')\mathcal{R}(B''\cup X,E_1)\mathcal{R}(X,E_2')}{\mathcal{R}(A'\cup B'''',\overline{A}\backslash A')\mathcal{R}(A'\cup B'''',\overline{B}\backslash(B''\cup B''''))\mathcal{R}(\overline{A}\backslash A',\overline{B}\backslash(B''\cup B''''))}.$$

Llamamos ahora $B':=B''\cup B''''$. Así $|B'|=q'+m'$ y reescribimos la expresión como

$$(-1)^{\sigma} \sum_{\substack{A'\subset\overline{A}\\|A'|=p'+n'}} \sum_{\substack{B'\subset\overline{B}\\|B'|=q'+m'}} \sum_{\substack{B''\cup B''''=B'\\|B''|=q',|B''''|=m'}} \sum_{\substack{E_1\cup E_2'=A'\cup B''''\\|E_1|=p,|E_2'|=n'}} \frac{\mathcal{R}(A,\overline{B}\backslash B')\mathcal{R}(B\backslash B'',\overline{A}\backslash A')\mathcal{R}(B''\cup X,E_1)\mathcal{R}(X,B'')\mathcal{R}(X,E_2')}{\mathcal{R}(A'\cup B'''',\overline{A}\backslash A')\mathcal{R}(A'\cup B'''',\overline{B}\backslash B')\mathcal{R}(\overline{A}\backslash A',\overline{B}\backslash B')\mathcal{R}(B'',\overline{B}\backslash B'')}.$$

Con una simple reescritura tenemos

$$\frac{\mathcal{R}(A,\overline{B}\backslash B')\mathcal{R}(B\backslash B'',\overline{A}\backslash A')\mathcal{R}(B''\cup X,E_1)\mathcal{R}(X,B'')\mathcal{R}(X,E_2')}{\mathcal{R}(A'\cup B'''',\overline{A}\backslash A')\mathcal{R}(A'\cup B'''',\overline{B}\backslash B')\mathcal{R}(\overline{A}\backslash A',\overline{B}\backslash B')\mathcal{R}(B'',\overline{B}\backslash B'')} = (-1)^{(n-(q'+m'))(\overline{m}-(p'+n'))}$$
$$\cdot \frac{\mathcal{R}(A\backslash\overline{A},\overline{B}\backslash B')\mathcal{R}(B\backslash\overline{B},\overline{A}\backslash A')\mathcal{R}(\overline{A}\backslash A',\overline{B}\backslash B')\mathcal{R}(B''\cup X,E_1)\mathcal{R}(X,B'')\mathcal{R}(X,E_2')}{\mathcal{R}(A',\overline{A}\backslash A')\mathcal{R}(B',\overline{B}\backslash B')\mathcal{R}(B'',B'''')}.$$

Llamando $\epsilon:=(n-(q'+m'))(\overline{m}-(p'+n'))$, toda la suma puede escribirse como

$$(-1)^{\sigma+\epsilon} \sum_{\substack{A'\subset\overline{A}\\|A'|=p'+n'}} \sum_{\substack{B'\subset\overline{B}\\|B'|=q'+m'}} \frac{\mathcal{R}(A\backslash\overline{A},\overline{B}\backslash B')\mathcal{R}(B\backslash\overline{B},\overline{A}\backslash A')\mathcal{R}(\overline{A}\backslash A',\overline{B}\backslash B')\mathcal{R}(X,A')\mathcal{R}(X,B')}{\mathcal{R}(A',\overline{A}\backslash A')\mathcal{R}(B',\overline{B}\backslash B')} \cdot \sum_{\substack{B''\cup B''''=B'\\|B''|=q',|B''''|=m'}} \sum_{\substack{E_1\cup E_2'=A'\cup B''''\\|E_1|=p,|E_2'|=n'}} \frac{\mathcal{R}(B'',E_1)}{\mathcal{R}(B'',B'''')}.$$

Finalmente,

$$\sum_{\substack{B''\cup B''''=B'\\|B''|=q',|B''''|=m'}} \sum_{\substack{E_1\cup E_2'=A'\cup B''''\\|E_1|=p,|E_2'|=n'}} \frac{\mathcal{R}(B'',E_1)}{\mathcal{R}(B'',B'''')} = \sum_{\substack{E_1\subset A'\cup B'\\|E_1|=p}} \sum_{\substack{B''\cup B''''=B'\\|B''|=q',|B''''|=m'}} \frac{\mathcal{R}(B'',E_1)}{\mathcal{R}(B'',B'''')},$$

y resulta

$$\sum_{\substack{B''\cup B'''=B' \\ |B''|=q',|B'''|=m'}} \frac{\mathcal{R}(B'',E_1)}{\mathcal{R}(B'',B''')} = \sum_{\substack{E_1'\subset E_1 \\ |E_1'|=p'}} \frac{\mathcal{R}(B',E_1')}{\mathcal{R}(E_1\backslash E_1',E_1')} = (-1)^{p'q'} \sum_{\substack{E_1'\subset E_1 \\ |E_1'|=p'}} \frac{\mathcal{R}(E_1',B')}{\mathcal{R}(E_1',E_1\backslash E_1')},$$

usando el Teorema 2.2.2 con $A = B'$, $B = E_1$ y $r = 0$. Llamando $C := E_1$ y $C' := E_1'$, se termina la demostración verificando que

$$(m-p)(n-q)+n'(n-q)+pq'+(n-(q'+m'))(\overline{m}-(p'+n'))+p'q' \text{ y } (m'+n')(m-p)+qm',$$

son congruentes módulo 2.

Sólo falta comentar que el caso general, A y B no necesariamente disjuntos, se sigue del hecho que las dos expresiones coinciden genéricamente. □

En el Teorema 4.2.6, del mismo modo que ocurre con el Teorema 4.1.6, si tomamos $\overline{A} = A$ y $\overline{B} = B$, el miembro derecho de la igualdad coincide con el miembro izquierdo sin obtener nada nuevo. En efecto, notemos que

$$\sum_{\substack{C\subset A'\cup B' \\ |C|=p}} \sum_{\substack{C'\subset C \\ |C'|=p'}} \frac{\mathcal{R}(C',B')}{\mathcal{R}(C',C\backslash C')} = \mathcal{R}(A',B'),$$

pues en ese caso $p' = p$, de modo que $C' = C$ es el único término de la segunda suma, mientras que la primera tiene como único término no nulo $C = A'$, pues si $C \cap B' \neq \emptyset$, resulta $\mathcal{R}(C, B') = 0$. Además el signo es el correcto ya que estamos en el caso $m' = n' = 0$.

Sin embargo, al igual que con la suma simple, el miembro derecho tiene sentido incluso cuando A y B son multiconjuntos; sólo necesitamos que $\overline{A}$ y $\overline{B}$ sean conjuntos. Si $X = \{x\}$ podemos definir la noción de suma doble de Sylvester para multiconjuntos A y B con p y q en el rango del Teorema 4.2.6, que extiende la noción usual de la suma doble de Sylvester para conjuntos, como enunciamos en la Definición 4.2.3. Podemos entonces demostrar el Teorema 4.2.5.

Demostración del Teorema 4.2.5. Por el Teorema 4.2.6, tenemos que la siguiente igualdad se satisface para conjuntos A y B, cualesquiera subconjuntos $\overline{A} \subset A$ y $\overline{B} \subset B$ y con p y q en el rango del enunciado:

$$\binom{d}{p}\mathrm{Sres}_d(f,g)(x) = (-1)^{p(m-d)}\mathrm{SylM}_{p,q}(A,B)(x).$$

El pasaje de conjuntos a multiconjuntos, como en el caso suma simple, es natural tomando límites de conjuntos a multiconjuntos, como en la demostración del Teorema 4.1.4. □

Observemos que la Definición 4.2.3 es compatible con la Definición 4.1.3 cuando se dan las condiciones de ambas. Esto es, si $n' = 0$, la suma $\mathrm{SylM}_{p,q}(A,B)(x)$ de la Definición 4.2.3 coincide con la suma $\mathrm{SylM}_{d,0}(A,B)(x)$ de la Definición 4.1.3 cuando $p = d$ y $q = 0$. Por esto es que tiene sentido que usemos la misma notación. De hecho se podría encontrar

la expresión general para $\mathrm{SylM}_{p,q}(A,B)(x)$ para todos los valores de p y de q, usando el Teorema 4.1.12, con polinomios de Schur.

Probamos ahora el Lema 4.2.4

Demostración del Lema 4.2.4. Escribimos

$$\begin{aligned}(-1)^{p'q'}\sum_{\substack{C\subset A'\cup B'\\|C|=p}}\sum_{\substack{C'\subset C\\|C'|=p'}}\frac{\mathcal{R}(C',B')}{\mathcal{R}(C',C\backslash C')} &= \sum_{\substack{C\subset A'\cup B'\\|C|=p}}\sum_{\substack{C'\subset C\\|C'|=p'}}\frac{\mathcal{R}(B',C')}{\mathcal{R}(C\backslash C',C')}\\ &= \sum_{\substack{C'\subset A'\\|C'|=p'}}\sum_{\substack{C''\subset (A'\backslash C')\cup B'\\|C''|=m'}}\frac{\mathcal{R}(B',C')}{\mathcal{R}(C'',C')}\\ &= \sum_{\substack{A_1\subset A'\\|A_1|=p'}}\sum_{\substack{C''\subset (A'\backslash A_1)\cup B'\\|C''|=m'}}\frac{\mathcal{R}(B',A_1)}{\mathcal{R}(C'',A_1)},\end{aligned}$$

llamando $A_1 := C'$. Llamemos ahora $A_2 = C''\cap(A'\backslash A_1)$ y $B_1 = C''\cap B'$. Tenemos

$$\frac{\mathcal{R}(B',A_1)}{\mathcal{R}(C'',A_1)} = \frac{\mathcal{R}(B',A_1)}{\mathcal{R}(A_2,A_1)\mathcal{R}(B_1,A_1)} = \frac{\mathcal{R}(B'\backslash B_1,A_1)}{\mathcal{R}(A_2,A_1)}.$$

Llamando $A'' := A_1\cup A_2$ y $B'' := B'\backslash B_1$ podemos escribir toda la expresión como

$$\begin{aligned}&\sum_{\substack{A_1\subset A'\\|A_1|=p'}}\sum_{k\geq 0}\sum_{\substack{A_2\subset (A'\backslash A_1)\\|A_2|=k}}\sum_{\substack{B_1\subset B'\\|B_1|=m'-k}}\frac{\mathcal{R}(B'\backslash B_1,A_1)}{\mathcal{R}(A_2,A_1)}\\ &=\sum_{k\geq 0}\sum_{\substack{A''\subset A'\\|A''|=p'+k}}\sum_{\substack{B''\subset B'\\|B''|=q'+k}}\sum_{\substack{A_2\subset A''\\|A_2|=k}}\frac{\mathcal{R}(B'',A''\backslash A_2)}{\mathcal{R}(A_2,A''\backslash A_2)}.\end{aligned}$$

Del mismo modo podemos obtener una expresión análoga para la suma del miembro derecho de la igualdad del enunciado:

$$\sum_{\substack{C\subset A'\cup B'\\|C|=q}}\sum_{\substack{C'\subset C\\|C'|=q'}}\frac{\mathcal{R}(C',A')}{\mathcal{R}(C',C\backslash C')} = \sum_{k\geq 0}\sum_{\substack{B''\subset B'\\|B''|=q'+k}}\sum_{\substack{A''\subset A'\\|A''|=p'+k}}\sum_{\substack{B_2\subset B''\\|B_2|=k}}\frac{\mathcal{R}(B''\backslash B_2,A'')}{\mathcal{R}(B''\backslash B_2,B_2)}.$$

Pero dado k fijo, tenemos que

$$\sum_{\substack{B_2\subset B''\\|B_2|=k}}\frac{\mathcal{R}(B''\backslash B_2,A'')}{\mathcal{R}(B''\backslash B_2,B_2)} = \sum_{\substack{A_2\subset A''\\|A_2|=k}}\frac{\mathcal{R}(B'',A''\backslash A_2)}{\mathcal{R}(A_2,A''\backslash A_2)},$$

por el Teorema 2.2.2 con $A = B''$, $B = A''$, $d = k$ y $r = 0$. De modo que las dos expresiones del enunciado efectivamente coinciden. □

Damos ahora fórmulas, similares a las que dimos para las sumas simples y dobles, para los polinomios $F_d(f,g)$ y $G_d(f,g)$ de la identidad de Bézout. En el Corolario 4.2.2 los escribimos con un conjunto F auxiliar, de modo que podemos usar el mismo recurso de los Teoremas 4.1.6 y 4.2.6, utilizando un conjunto F apropiado. Lo haremos también solamente para el caso d suficientemente grande; el caso general también se podría hacer usando polinomios de Schur.

Proposición 4.2.7. *Sean K un cuerpo y $f,g \in K[x]$ polinomios mónicos de grados m y n respectivamente, con multiconjuntos de raíces A y B, y conjuntos de raíces distintas $\overline{A}$ y $\overline{B}$ respectivamente. Sean $m' := m - \overline{m}$ y $n' := n - \overline{n}$ y d tal que $m' + n' \leq d \leq \min\{m-1, n-1\}$ y sean $F_d(f,g)$ y $G_d(f,g)$ los polinomios de la identidad de Bézout definidos en la Proposición 1.1.4. Entonces*

$$F_d(f,g) = (-1)^{m-d+n'(m-m'+1)} \sum_{\substack{A' \subset \overline{A} \\ |A'|=n'}} \sum_{\substack{B' \subset \overline{B} \\ |B'|=d+1-n'}} \frac{\mathcal{R}(A\backslash\overline{A}, \overline{B}\backslash B')\mathcal{R}(\overline{A}\backslash A', B\backslash B')\mathcal{R}(x, \overline{B}\backslash B')}{\mathcal{R}(B', \overline{B}\backslash B')\mathcal{R}(A', \overline{A}\backslash A')},$$

$$G_d(f,g) = (-1)^{m-d-1} \sum_{\substack{A' \subset \overline{A} \\ |A'|=n'}} \sum_{\substack{B' \subset \overline{B} \\ |B'|=d+1-n'}} \frac{\mathcal{R}(\overline{A}\backslash A', B\backslash\overline{B})\mathcal{R}(A\backslash A', \overline{B}\backslash B')\mathcal{R}(x, \overline{A}\backslash A')}{\mathcal{R}(\overline{A}\backslash A', A')\mathcal{R}(B', \overline{B}\backslash B')}.$$

Demostración. Hacemos la demostración sólo para $F_d(f,g)$ siendo que la otra es análoga. Por el Corolario 4.2.2, si $F \subset K$ es un conjunto con $|F| \geq m+n-d$, tenemos que

$$F_d(f,g) = (-1)^{m+(n-d)(d+1)+1} \sum_{\substack{F_1 \cup F_2 \cup F_3 = F \\ |F_1|=n-d-1, |F_2|=d+1 \\ |F_3|=|F|-n}} \frac{\mathcal{R}(B, F_3)\mathcal{R}(A \cup x, F_1)}{\mathcal{R}(F_1, F_2)\mathcal{R}(F_1, F_3)\mathcal{R}(F_2, F_3)}.$$

Tomamos entonces $F = \overline{A} \cup \overline{B}$ que tiene tamaño correcto, pues $|F| = \overline{m} + \overline{n} \geq m+n-d$ por hipótesis. Luego,

$$F_d(f,g) = (-1)^{\sigma} \sum_{\substack{F_1 \cup F_2 \cup F_3 = \overline{A} \cup \overline{B} \\ |F_1|=n-d-1, |F_2|=d+1 \\ |F_3|=\overline{m}-n'}} \frac{\mathcal{R}(B, F_3)\mathcal{R}(A \cup x, F_1)}{\mathcal{R}(F_1, F_2)\mathcal{R}(F_1, F_3)\mathcal{R}(F_2, F_3)},$$

con $\sigma = m + (n-d)(d+1) + 1$. Ahora, $\mathcal{R}(B, F_3) = 0$ si $B \cap F_3 \neq \emptyset$ y $\mathcal{R}(A, F_1) = 0$ si $A \cap F_1 \neq \emptyset$. De modo que asumimos $F_3 \subset \overline{A}$ y $F_1 \subset \overline{B}$. Llamemos $A' := \overline{A}\backslash F_3$ y $B' := \overline{B}\backslash F_1$, entonces $F_2 = A' \cup B'$ y podemos reescribir $F_d(f,g)$ como

$$\begin{aligned} F_d(f,g) &= (-1)^{\sigma} \sum_{\substack{A' \subset \overline{A} \\ |A'|=n'}} \sum_{\substack{B' \subset \overline{B} \\ |B'|=d+1-n'}} \frac{\mathcal{R}(B, \overline{A}\backslash A')\mathcal{R}(A \cup x, \overline{B}\backslash B')}{\mathcal{R}(\overline{B}\backslash B', A' \cup B')\mathcal{R}(\overline{B}\backslash B', \overline{A}\backslash A')\mathcal{R}(A' \cup B', \overline{A}\backslash A')} \\ &= (-1)^{\sigma} \sum_{\substack{A' \subset \overline{A} \\ |A'|=n'}} \sum_{\substack{B' \subset \overline{B} \\ |B'|=d+1-n'}} \frac{\mathcal{R}(B, \overline{A}\backslash A')\mathcal{R}(A \cup x, \overline{B}\backslash B')}{\mathcal{R}(\overline{B}\backslash B', \overline{A})\mathcal{R}(\overline{B}\backslash B', B')\mathcal{R}(A', \overline{A}\backslash A')\mathcal{R}(B', \overline{A}\backslash A')} \end{aligned}$$

$$= (-1)^{\sigma+\epsilon} \sum_{\substack{A'\subset\overline{A}\\|A'|=n'}} \sum_{\substack{B'\subset\overline{B}\\|B'|=d+1-n'}} \frac{\mathcal{R}(B\backslash B',\overline{A}\backslash A')\mathcal{R}(A\cup x,\overline{B}\backslash B')}{\mathcal{R}(\overline{A},\overline{B}\backslash B')\mathcal{R}(\overline{B}\backslash B',B')\mathcal{R}(A',\overline{A}\backslash A')}$$

$$= (-1)^{\sigma+\epsilon+\delta} \sum_{\substack{A'\subset\overline{A}\\|A'|=n'}} \sum_{\substack{B'\subset\overline{B}\\|B'|=d+1-n'}} \frac{\mathcal{R}(\overline{A}\backslash A',B\backslash B')\mathcal{R}(A\backslash\overline{A},\overline{B}\backslash B')\mathcal{R}(x,\overline{B}\backslash B')}{\mathcal{R}(B',\overline{B}\backslash B')\mathcal{R}(A',\overline{A}\backslash A')},$$

con $\epsilon := (\overline{n}-(d+1-n'))\overline{m}$ y $\delta := (n-(d+1-n'))(\overline{m}-n')+(\overline{n}-(d+1-n'))(d+1-n')$. Terminamos la demostración observando que $\sigma+\epsilon+\delta = m+(n-d)(d+1)+1+(\overline{n}-(d+1-n'))\overline{m}+(n-(d+1-n'))(\overline{m}-n')+(\overline{n}-(d+1-n'))(d+1-n') \equiv m-d+n'(m-m'+1)$ (mód 2). □

Así como las sumas $\mathrm{SylM}_{d,0}(A,B)(x)$ y $\mathrm{SylM}_{p,q}(A,B)(x)$ extienden respectivamente las definiciones de $\mathrm{Syl}_{d,0}(A,B)(x)$ y de $\mathrm{Syl}_{p,q}(A,B)(x)$ a multiconjuntos, las fórmulas para $F_d(f,g)$ y $G_d(f,g)$ de la Proposición 4.2.7 extienden las fórmulas del Corolario 3.2.6 para multiconjuntos con d en el rango fijado. Efectivamente, cuando A y B son conjuntos, esto es, $m'=n'=0$, se ve que las fórmulas de la Proposición 4.2.7 coinciden con las de dicho corolario.

Observemos por último lo siguiente. Así como la definición de la subresultante es una expresión en los coeficientes de los polinomios y las sumas de Sylvester son expresiones en sus raíces, las fórmulas de las Proposiciones 4.1.1 y 4.1.2, que son expresiones en términos de las raíces para el caso de raíces múltiples, dependiendo de un conjunto arbitrario E, pueden verse también de otra forma. Son también expresiones que dependen de los valores de f y de g precisamente en los puntos del conjunto E. En efecto,

$$a_m^{|E|-m} b_n^{m-d} \sum_{\substack{E_1\cup E_2\cup E_3=E\\|E_1|=d,|E_2|=m-d,|E_3|=|E|-m}} \frac{\mathcal{R}(E_3,A)\mathcal{R}(E_2,B)\mathcal{R}(x,E_1)}{\mathcal{R}(E_2,E_1)\mathcal{R}(E_3,E_1)\mathcal{R}(E_3,E_2)}$$

$$= \sum_{\substack{E_1\cup E_2\cup E_3=E\\|E_1|=d,|E_2|=m-d,|E_3|=n-d}} \frac{(\prod_{\xi\in E_3} f(\xi))(\prod_{\gamma\in E_2} g(\gamma))\mathcal{R}(x,E_1)}{\mathcal{R}(E_2,E_1)\mathcal{R}(E_3,E_1)\mathcal{R}(E_3,E_2)},$$

si a_m y b_n son los respectivos coeficientes principales de f y de g. De hecho, ésta es la notación que usan Apery y Jouanalou en [ApJo2006, Prop.91] en el caso $|E| = m+n-d$. El problema es que el conjunto E es demasiado grande para identificar a f o a g a través de los valores que éstos toman en sus puntos, pues f y g quedan determinados por los valores que toman en $m+1$ y $n+1$ puntos respectivamente. Aquí se necesita más información porque $|E| = m+n-d$. En el Capítulo 5 veremos ejemplos de otras construcciones en donde sí se logra la escritura a través de lo que los polinomios interpolan en una cantidad óptima de puntos.

Notemos que la escritura de la suma doble de la Proposición 4.2.1 puede verse como una expresión dada por los valores que toman f en los puntos de E y g en los puntos de F. Es decir, interpolando a los polinomios en conjuntos diferentes, aunque también

necesitando mayor información que la óptima:

$$a_m^{|E|-m} b_n^{|F|-n} \mathrm{Syl}_{p,q}(A,B)(x)$$
$$= \sum_{\substack{E_1 \cup E_2 \cup E_3 = E \\ |E_1|=p, |E_2|=m-p \\ |E_3|=|E|-m}} \sum_{\substack{F_1 \cup F_2 \cup F_3 = F \\ |F_1|=q, |F_2|=n-q \\ |F_3|=|F|-n}} \frac{(\prod_{\xi \in E_3} f(\xi))(\prod_{\gamma \in F_3} g(\gamma)) \mathcal{R}(E_2,F_2)\mathcal{R}(E_1,F_1)\mathcal{R}(x,E_1)\mathcal{R}(x,F_1)}{\mathcal{R}(E_1,E_2)\mathcal{R}(E_1,E_3)\mathcal{R}(E_2,E_3)\mathcal{R}(F_1,F_2)\mathcal{R}(F_1,F_3)\mathcal{R}(F_2,F_3)}.$$

Capítulo 5

Otras aplicaciones del lema de intercambio

En este capítulo veremos otras aplicaciones del lema de intercambio. Mostraremos algunas aplicaciones más a subresultantes y sumas de Sylvester pero también otras que trascienden dicho campo.

En la Sección 5.1 mostramos un resultado que generaliza el Teorema 1.1.5, que es el que relaciona la subresultante con los restos sucesivos del algoritmo de Euclides. En la Sección 5.2 aplicamos el lema de intercambio para obtener reescrituras de los polinomios que definen las llamadas matrices de Bézout y obtenemos consecuencias inmediatas de estas expresiones. En la Sección 5.3 encontramos reescrituras de los polinomios que conforman una base de Gröbner particular. Finalmente en la Sección 5.4 mostramos cómo puede obtenerse, mediante el recurso de la interpolación simétrica, la conocida escritura en fracciones simples de un cociente de polinomios y la generalizamos a varias variables. Los resultados de este capítulo son originales de esta tesis.

5.1. Subresultantes y el algoritmo de Euclides

En el Capítulo 1 enunciamos el Teorema 1.1.5, llamado el teorema fundamental de los restos polinomiales, en el que se describe la sucesión de subresultantes $\mathrm{Sres}_0(f,g)(x),\ldots,\mathrm{Sres}_d(f,g)(x)$ en función de los sucesivos restos que se obtienen cuando se realiza el algoritmo de Euclides para calcular $\mathrm{mcd}(f,g)$. En esta sección probaremos una generalización de este teorema usando el lema de intercambio. Para esto vamos a usar la misma noción de suma simple multivariada $\mathrm{MSyl}_{0,d}(A,B)(X)$ que introdujimos en la Notación 3.1.1, que nos permitirá inducir una noción de subresultante multivariada calculando su formulación matricial como hicimos en la Proposición 3.1.5.

Definición 5.1.1. Sean $f = a_m x^m + \cdots + a_0$ y $g = b_n x^n + \cdots + b_0$ dos polinomios con coeficientes en un cuerpo K (o eventualemente en un dominio íntegro con cuerpo de fracciones K) de grados exactamente m y n respectivamente, es decir, $a_m \neq 0$ y $b_n \neq 0$, y sea $X_s = (x_1,\ldots,x_s)$ un conjunto ordenado de variables con $1 \leq s \leq m+n-2d$. Definimos la *subresultante multivariada* de orden d entre f y g en X_s para $0 \leq d < \mín\{m,n\}$, o $d = \mín\{m,n\}$ si $m \neq n$, como

$$\mathrm{MSres}_d(f,g)(X_s) :=$$

$$\frac{1}{V(X_s)} \cdot \det \begin{array}{|cccc|c|} \multicolumn{4}{c}{\overbrace{\qquad\qquad\qquad}^{m+n-2d-s}} & \multicolumn{1}{c}{\overbrace{\qquad}^{s}} \\ \hline a_m & \cdots & \cdots & a_{2d+s+1-n} & x_1^{n-d-1}f(x_1) \;\cdots\; x_s^{n-d-1}f(x_s) & \\ & \ddots & & \vdots & \vdots \qquad\qquad \vdots & n-d \\ & & a_m \;\ldots\; a_{d+s} & & f(x_1) \;\cdots\; f(x_s) & \\ \hline b_n & \cdots & \cdots & b_{2d+s+1-m} & x_1^{m-d-1}g(x_1) \;\cdots\; x_s^{m-d-1}g(x_s) & \\ & \ddots & & \vdots & \vdots \qquad\qquad \vdots & m-d \\ & & b_n \;\ldots\; b_{d+s} & & g(x_1) \;\cdots\; g(x_s) & \\ \hline \end{array} .$$

Observemos que en el caso $s = 1$, $\mathrm{MSres}_d(x_1)$ coincide con la definición de la subresultante $\mathrm{Sres}_d(f,g)(x_1)$. Además, si $s = n-d$, $\mathrm{MSres}_d(f,g)(X_{n-d})$ es exactamente la formulación matricial de la suma $\mathrm{MSyl}_{0,d}(A,B)(X)$ que vimos en la Proposición 3.1.5. Y en el caso $s = m+n-2d$, $\mathrm{MSres}_d(f,g)(X_{m+n-2d})$ es la formulación matricial de $\mathrm{MSyl}_{0,d}(A,B)(X')$, que vimos en la demostración alternativa de dicha proposición. Aquí generalizamos a una cantidad arbitraria de variables.

Observemos también que

$$\mathrm{MSres}_d(f,g)(X_s) = (-1)^{(m-d)(n-d)}\mathrm{MSres}_d(g,f)(X_s),$$

del mismo modo que ocurre con la subresultante, como puede verse permutando filas en la matriz de la definición.

Con esta noción probaremos el teorema siguiente, que generaliza el Teorema 1.1.5. En él supondremos sin pérdida de generalidad que $n \geq m$.

Teorema 5.1.2. *Sea K un cuerpo y sean $f, g \in K[x]$ con $\deg(f) = m \leq n = \deg(g)$. Sean $0 \leq d < m$ o $d = m$ si $n > m$, y $X_s = (x_1, \ldots, x_s)$ con $1 \leq s \leq m+n-2d$. Denotamos por $R_0 = g, R_1 = f, \ldots, R_k = c\,\mathrm{mcd}(f,g)$, con $c \in K\backslash\{0\}$, la sucesión de restos en el algoritmo de Euclides entre g y f, y $r_i := \deg(R_i)$. Entonces, se tiene:*

1. *Si $d < r_k$, entonces $\mathrm{MSres}_d(f,g)(X_s) = 0$.*
2. *Si $d \geq r_k$, entonces*

$$\mathrm{MSres}_d(f,g)(X_s) \neq 0 \iff \text{existe } 0 \leq i \leq k \text{ tal que } d \leq r_i \leq d+s.$$

Más aún, si existe $0 \leq j \leq k$ tal que $r_j = d$ o $r_j = d+s$ pero no existe $0 \leq i \leq k$ tal que $d < r_i < d+s$, entonces

1. *Si $d = r_{i_0}$, se tiene $\mathrm{MSres}_d(X_s) = \lambda\, R_{i_0}(x_1) \cdots R_{i_0}(x_s)$ para algún $\lambda \in K\backslash\{0\}$.*
2. *Si $d = r_{i_0-1} - s$, se tiene $\mathrm{MSres}_d(X_s) = \lambda\, R_{i_0}(x_1) \cdots R_{i_0}(x_s)$ para algún $\lambda \in K\backslash\{0\}$.*

Observemos que el Teorema 5.1.2 efectivamente generaliza el Teorema 1.1.5, pues este último es el caso particular $s = 1$ del primero. En efecto, el Teorema 1.1.5 puede leerse como

$$\mathrm{Sres}_d(f,g)(x) \neq 0 \iff \text{existe } 0 \leq i \leq k \text{ tal que } d \leq r_i \leq d+1,$$

y por otro lado, la condición de que no existe $0 \leq i \leq k$ tal que $d < r_i < d+1$ se cumple trivialmente. Finalmente los valores de $\mathrm{Sres}_d(f,g)(x)$ para $d = r_{i_0}$ y $d = r_{i_0-1} - 1$ claramente coinciden con los del Teorema 1.1.5.

Antes de probar el Teorema 5.1.2 vamos a definir la noción de *suma simple multivariada*, con una cantidad arbitraria de variables, que generaliza la suma $\mathrm{MSyl}_{0,d}(A,B)(X)$ de la Notación 3.1.1.

Definición 5.1.3. Sean A y B subconjuntos de un cuerpo K con $|A| = m$ y $|B| = n$. Sean $0 \leq d \leq n$ y X un conjunto finito de variables. Definimos

$$\mathrm{MSyl}_{0,d}(A,B)(X) := \sum_{B' \subset B, |B'|=d} \mathcal{R}(A, B\backslash B') \frac{\mathcal{R}(X,B')}{\mathcal{R}(B', B\backslash B')} = \sum_{\substack{B_1 \cup B_2 = B \\ |B_1|=d, |B_2|=n-d}} \frac{\mathcal{R}(A,B_2)\mathcal{R}(X,B_1)}{\mathcal{R}(B_1,B_2)}.$$

Esta suma coincide, salvo el signo, con la de la Notación 3.1.1 cuando $s = n - d$. No compatibilizamos el signo por comodidad, para lo que haremos a continuación. El siguiente lema es consecuencia inmediata del lema de intercambio.

Lema 5.1.4. *Sean A y B subconjuntos de un cuerpo K con $|A| = m$ y $|B| = n$. Sean $0 \leq d \leq \mín\{m,n\}$ y $X_s := (x_1, \ldots, x_s)$ con $1 \leq s \leq m+n-2d$. Entonces*

$$\mathrm{MSyl}_{0,d}(A,B)(X_s) = \pm \mathrm{MSyl}_{0,d}(B,A)(X_s).$$

Demostración. Queremos ver que

$$\sum_{\substack{B_1 \cup B_2 = B \\ |B_1|=d, |B_2|=n-d}} \frac{\mathcal{R}(A,B_2)\mathcal{R}(X_s,B_1)}{\mathcal{R}(B_1,B_2)} = \pm \sum_{\substack{A_1 \cup A_2 = A \\ |A_1|=d, |A_2|=m-d}} \frac{\mathcal{R}(B,A_2)\mathcal{R}(X_s,A_1)}{\mathcal{R}(A_1,A_2)},$$

y esto es una aplicación directa de la Observación 2.2.4 con $C = X_s$ y cambiando los roles de A y de B. La hipótesis que necesitamos es $m+(n-d) \geq s+d$, que asumimos cierta. □

Relacionaremos ahora los conceptos de las Definiciones 5.1.1 y 5.1.3 de manera análoga a lo hecho en la Proposición 3.1.5, y generalizando además la Proposición 3.1.6.

Proposición 5.1.5. *Sean A y B subconjuntos de un cuerpo K con $|A| = m$ y $|B| = n$, y sean $f = a_m \mathcal{R}(x,A)$ y $g = b_n \mathcal{R}(x,B)$ con $a_m \neq 0$ y $b_n \neq 0$. Sea $X_s = (x_1, \ldots, x_s)$ con $1 \leq s \leq m+n-2d$. Entonces se tiene, para $0 \leq d < \mín\{m,n\}$, o $d = \mín\{m,n\}$ si $m \neq n$,*

$$\mathrm{MSres}_d(f,g)(X_s) = a_m^{n-d} b_n^{m-d} \mathrm{MSyl}_{0,d}(A,B)(X_s).$$

Demostración. Es suficiente probar el enunciado para f y g mónicos debido a la propiedad inmediata $\mathrm{MSres}_d(af,bg)(X_s) = a^{n-d}b^{m-d}\mathrm{MSres}_d(f,g)(X_s)$ para $a, b \in K$.

Asumimos entonces $f = \mathcal{R}(x,A)$ y $g = \mathcal{R}(x,B)$. Si $s = m+n-2d$ la igualdad del enunciado es exactamente la misma que probamos en la demostración alternativa de la Proposición 3.1.5, llamando $X' = X_s$. Supongamos entonces que $1 \leq s < m+n-2d$. Observemos que

$$\mathrm{MSyl}_{0,d}(A,B)(X_s) = \mathrm{coeff}_{x_{s+1}^d \cdots x_{m+n-2d}^d} \left(\mathrm{MSyl}_{0,d}(A,B)(X_{m+n-2d}) \right).$$

Dado que ya sabemos que el enunciado vale en el caso $s = m+n-2d$, se trata de calcular dicho coeficiente en la expresión

$$\frac{1}{V(X_{m+n-2d})} \cdot \det \begin{array}{|ccc|} \multicolumn{3}{c}{\overbrace{}^{m+n-2d}} \\ x_1^{n-d-1}f(x_1) & \dots & x_{m+n-2d}^{n-d-1}f(x_{m+n-2d}) \\ \vdots & & \vdots \\ f(x_1) & \dots & f(x_{m+n-2d}) \\ \hline x_1^{m-d-1}g(x_1) & \dots & x_{m+n-2d}^{m-d-1}g(x_{m+n-2d}) \\ \vdots & & \vdots \\ g(x_1) & \dots & g(x_{m+n-2d}) \end{array} \begin{array}{l} \\ \\ n-d \\ \\ \\ m-d \end{array}$$

$$= \frac{1}{V(x_{m+n-2d},\dots,x_1)} \cdot \det \begin{array}{|ccc|} \multicolumn{3}{c}{\overbrace{}^{m+n-2d}} \\ x_{m+m-2d}^{n-d-1}f(x_{m+n-2d}) & \dots & x_1^{n-d-1}f(x_1) \\ \vdots & & \vdots \\ f(x_{m+n-2d}) & \dots & f(x_1) \\ \hline x_{m+n-2d}^{m-d-1}g(x_{m+n-2d}) & \dots & x_1^{m-d-1}g(x_1) \\ \vdots & & \vdots \\ g(x_{m+n-2d}) & \dots & g(x_1) \end{array} \begin{array}{l} \\ \\ n-d \\ \\ \\ m-d \end{array} . \quad (5.1)$$

Hacemos el cálculo de este coeficiente del mismo modo que lo hicimos en la primera demostración de la Poposición 3.1.5. Notemos $S(X_{m+n-2d})$ al determinante de la matriz de (5.1) y $c_d(X_s) \in K[X_s]$ al coeficiente de $x_{s+1}^d \cdots x_{m+n-2d}^d$ en $\mathrm{MSyl}_{0,d}(A,B)(X_{m+n-2d})$. Tenemos entonces que $\mathrm{MSyl}_{0,d}(A,B)(X_{m+n-2d}) = S(X_{m+n-2d})/V(x_{m+n-2d},\dots,x_1)$. Llamemos $Y_s = (x_{s+1},\dots,x_{m+n-2d})$ y observemos la igualdad

$$V(x_{m+n-2d},\dots,x_1) = V(x_{m+n-2d},\dots,x_{s+1})V(x_s,\dots,x_1)\mathcal{R}(Y_s,X_s).$$

Luego

$$\begin{aligned} &S(X_{m+n-2d}) \\ &= \mathrm{MSyl}_{0,d}(A,B)(X_{m+n-2d})V(x_{m+n-2d},\dots,x_1) \\ &= \mathrm{MSyl}_{0,d}(A,B)(X_{m+n-2d})V(x_{m+n-2d},\dots,x_{s+1})V(x_s,\dots,x_1)\mathcal{R}(Y_s,X_s) \\ &= (c_d(X_s)\, x_{m+n-2d}^d \cdots x_{s+1}^d + \cdots)(x_{m+n-2d}^{m+n-2d-s-1}\, x_{m+n-2d-1}^{m+n-2d-s-2} \cdots x_{s+2} + \cdots) \\ &\qquad \cdot V(x_s,\dots,x_1)\mathcal{R}(Y_s,X_s) \\ &= c_d(X_s)\, x_{m+n-2d}^{m+n-d-1}\, x_{m+n-2d-1}^{m+n-d-2} \cdots x_{s+1}^{d+s} V(x_s,\dots,x_1) + \cdots \end{aligned}$$

Por lo tanto,

$$c_d(X_s)V(x_s,\dots,x_1) = \mathrm{coeff}_{x_{m+n-2d}^{m+n-d-1} x_{m+n-2d-1}^{m+n-d-2} \cdots x_{s+1}^{d+s}}(S(X_{m+n-2d})).$$

Es claro que el coeficiente de $x_{m+n-2d}^{m+n-d-1} x_{m+n-2d-1}^{m+n-d-2} \cdots x_{s+1}^{d+s}$ en el determinante se obtiene, por multilinealidad, a partir del coeficiente del determinante de la matriz en donde la columna de x_{m+n-2d} tiene todos sus exponentes iguales a $m+n-d-1$, la columna de

$x_{m+n-2d-1}$ tiene todos sus exponentes iguales a $m+n-d-2$, y así sucesivamente hasta la columna de x_{s+1}, con exponentes iguales a $d+s$. Esto es,
$\operatorname{coeff}_{x_{m+n-2d}^{m+n-d-1} x_{m+n-2d-1}^{m+n-d-2} \cdots x_{s+1}^{d+s}}(S(X_{m+n-2d}))$ es igual a

$$\det \begin{array}{|ccccc|ccc|l}
\multicolumn{5}{c|}{\overbrace{}^{m+n-2d-s}} & \multicolumn{3}{c|}{\overbrace{}^{s}} & \\
a_m & \cdots & & \cdots & a_{2d+s+1-n} & x_s^{n-d-1}f(x_s) & \cdots & x_1^{n-d-1}f(x_1) & \\
 & \ddots & & & \vdots & \vdots & & \vdots & n-d \\
 & & a_m & \cdots & a_{d+s} & f(x_s) & \cdots & f(x_1) & \\
\hline
b_n & \cdots & & \cdots & b_{2d+s+1-m} & x_s^{m-d-1}g(x_s) & \cdots & x_1^{m-d-1}g(x_1) & \\
 & \ddots & & & \vdots & \vdots & & \vdots & m-d \\
 & & b_n & \cdots & b_{d+s} & g(x_s) & \cdots & g(x_1) &
\end{array}.$$

Luego,

$$c_d(X_s) = \frac{1}{V(x_s,\ldots,x_1)} \cdot$$

$$\det \begin{array}{|ccccc|ccc|l}
\multicolumn{5}{c|}{\overbrace{}^{m+n-2d-s}} & \multicolumn{3}{c|}{\overbrace{}^{s}} & \\
a_m & \cdots & & \cdots & a_{2d+s+1-n} & x_s^{n-d-1}f(x_s) & \cdots & x_1^{n-d-1}f(x_1) & \\
 & \ddots & & & \vdots & \vdots & & \vdots & n-d \\
 & & a_m & \cdots & a_{d+s} & f(x_s) & \cdots & f(x_1) & \\
\hline
b_n & \cdots & & \cdots & b_{2d+s+1-m} & x_s^{m-d-1}g(x_s) & \cdots & x_1^{m-d-1}g(x_1) & \\
 & \ddots & & & \vdots & \vdots & & \vdots & m-d \\
 & & b_n & \cdots & b_{d+s} & g(x_s) & \cdots & g(x_1) &
\end{array},$$

y esto es exactamente $\operatorname{MSres}_d(f,g)(X_s)$, dado que el signo al reordenar las columnas de las variables se compensa con el signo en el que difieren $V(X_s)$ y $V(x_s,\ldots,x_1)$. □

Para probar el Teorema 5.1.2 usaremos el siguiente lema.

Lema 5.1.6. *Sea K un cuerpo y sean $f,g \in K[x]$ con $\deg(f) = m \le n = \deg(g)$. Sean $0 \le d < m$ o $d = m$ si $n > m$, y $X_s = (x_1,\ldots,x_s)$, con $1 \le s \le m+n-2d$. Denotamos por $R_0 = g, R_1 = f, \ldots, R_k = c\,\operatorname{mcd}(f,g)$, con $c \in K\backslash\{0\}$, la sucesión de restos en el algoritmo de Euclides entre f y g, y $r_i = \deg(R_i)$. Sea $1 \le i < k$ tal que $r_{i-1} + r_i \ge 2d+s$ y $r_i \ge d$, y supongamos que R_{i-1}, R_i y R_{i+1} tienen raíces simples. Entonces existe $\lambda \in K\backslash\{0\}$ tal que*

$$\operatorname{MSyl}_{0,d}(C_i, C_{i-1})(X_s) = \lambda \operatorname{MSyl}_{0,d}(C_{i+1}, C_i)(X_s),$$

donde C_j es el conjunto de raíces de R_j, para cada $j \in \{i-1, i, i+1\}$.

Si además $d \le r_{i+1}$, entonces existe $\mu \in K\backslash\{0\}$ tal que

$$\operatorname{MSres}_d(R_i, R_{i-1})(X_s) = \mu \operatorname{MSres}_d(R_{i+1}, R_i)(X_s).$$

Demostración. Una vez probada la primera parte, la igualdad

$$\operatorname{MSres}_d(R_i, R_{i-1})(X_s) = \mu \operatorname{MSres}_d(R_{i+1}, R_i)(X_s),$$

para el caso $d \leq r_{i+1} < r_i$ es inmediata a partir de la Proposición 5.1.5 ya que están definidas tanto $\mathrm{MSres}_d(R_i, R_{i-1})(X_s)$ como $\mathrm{MSres}_d(R_{i+1}, R_i)(X_s)$.
Probamos ahora la primera parte del enunciado. Por el Lema 5.1.4, dado que $d \leq r_i < r_{i-1}$ y $r_{i-1} + r_i \geq 2d + s$, tenemos

$$\mathrm{MSyl}_{0,d}(C_i, C_{i-1})(X_s) = \pm\mathrm{MSyl}_{0,d}(C_{i-1}, C_i)(X_s) = \pm \sum_{\substack{C' \cup C'' = C_i \\ |C'|=d, |C''|=r_i-d}} \frac{\mathcal{R}(C_{i-1}, C'')\mathcal{R}(X_s, C')}{\mathcal{R}(C', C'')}.$$

Ahora, por la relación $R_{i-1} = q_i \cdot R_i + R_{i+1}$, si $C'' = \{\gamma_1, \ldots, \gamma_{r_i-d}\}$, tenemos

$$\begin{aligned}\mathcal{R}(C_{i-1}, C'') = \pm\frac{1}{\mu^{r_i-d}} R_{i-1}(\gamma_1) \cdots R_{i-1}(\gamma_{r_i-d}) &= \pm\frac{1}{\mu^{r_i-d}} R_{i+1}(\gamma_1) \cdots R_{i+1}(\gamma_{r_i-d}) \\ &= \pm \left(\frac{\eta}{\mu}\right)^{r_i-d} \mathcal{R}(C_{i+1}, C''),\end{aligned}$$

donde μ y η son los respectivos coeficientes principales de R_i y R_{i+1}. De este modo resulta

$$\begin{aligned}\sum_{\substack{C' \cup C'' = C_i \\ |C'|=d, |C''|=r_i-d}} \frac{\mathcal{R}(C_{i-1}, C'')\mathcal{R}(X_s, C')}{\mathcal{R}(C', C'')} &= \pm \left(\frac{\eta}{\mu}\right)^{r_i-d} \sum_{\substack{C' \cup C'' = C_i \\ |C'|=d, |C''|=r_i-d}} \frac{\mathcal{R}(C_{i+1}, C'')\mathcal{R}(X_s, C')}{\mathcal{R}(C', C'')} \\ &= \pm \left(\frac{\eta}{\mu}\right)^{r_i-d} \mathrm{MSyl}_{0,d}(C_{i+1}, C_i),\end{aligned}$$

que prueba lo que queremos ver. □

Ahora podemos probar el Teorema 5.1.2.

Demostración del Teorema 5.1.2. Probemos primero que si $d < r_k$, entonces

$$\mathrm{MSres}_d(f, g)(X_s) = 0.$$

Supongamos primero que f y g tienen raíces simples y llamemos A y B a sus respectivos conjuntos de raíces. Por la Proposición 5.1.5 tenemos

$$\mathrm{MSres}_d(f, g)(X_s) = \lambda\mathrm{MSyl}_{0,d}(A, B)(X_s) = \lambda \sum_{\substack{B_1 \cup B_2 = B \\ |B_1|=d, |B_2|=n-d}} \frac{\mathcal{R}(A, B_2)\mathcal{R}(X_s, B_1)}{\mathcal{R}(B_1, B_2)},$$

donde $\lambda = a_m^{n-d} b_n^{m-d} \in K\backslash\{0\}$. Pero aquí, para cada sumando, $|B_2| = n - d > n - r_k = |B\backslash(A \cap B)|$ y por lo tanto $A \cap B_2 \neq \emptyset$, con lo cual se tiene $\mathcal{R}(A, B_2) = 0$, o sea $\mathrm{MSres}_d(f, g)(X_s) = 0$.

Para el caso general hacemos un proceso de pasaje de conjuntos a multiconjuntos parecido al que hicimos, por ejemplo, en la demostración del Teorema 4.1.4. Supongamos que A y B son multiconjuntos. Digamos $A = (\alpha_1, \ldots, \alpha_{m-r_k}, \gamma_1, \ldots, \gamma_{r_k})$ y $B = (\beta_1, \ldots, \beta_{n-r_k}, \gamma_1, \ldots, \gamma_{r_k})$, con posibles repeticiones entre los α_j, entre los β_j o entre los γ_j.

El multiconjunto de los γ_j es el de las raíces de $R_k = c\,\mathrm{mcd}(f,g)$. Sean $Y = (y_1,\dots,y_{m-r_k})$, $Z = (z_1,\dots,z_{n-r_k})$ y $W = (w_1,\dots,w_{r_k})$ conjuntos de variables y sean

$$F = a_m \prod_{i=1}^{m-r_k}(x-y_i)\prod_{i=1}^{r_k}(x-w_i) \quad \text{y} \quad G = b_n \prod_{i=1}^{n-r_k}(x-z_i)\prod_{i=1}^{r_k}(x-w_i),$$

con a_m y b_n los respectivos coeficientes principales de f y g. Entonces, como F y G tienen raíces simples, por lo que hicimos antes, tenemos que $\mathrm{MSres}_d(F,G)(X_s) = 0$. Pero evaluando las variables y_i en los α_i, las z_i en los β_i y las w_i en los γ_i, obtenemos f y g a partir de F y G, con lo cual resulta $\mathrm{MSres}_d(f,g)(X_s) = 0$.

Nos concentramos ahora en el caso $d \geq r_k$. Vamos a suponer primero que cada R_j tiene raíces simples.

(1) Probemos primero que si existe i, $1 \leq i \leq k$, tal que $d \leq r_i \leq d+s$, entonces $\mathrm{MSres}_d(f,g)(X_s) \neq 0$. Sea i_0 el mínimo índice tal que $d \leq r_i \leq d+s$. Supongamos primero que $i_0 \geq 1$. Tenemos entonces que

$$d \leq r_{i_0} \leq d+s < r_{i_0-1},$$

dado que $r_{i_0-1} > r_{i_0} \geq d$ no satisface $r_{i_0-1} \leq d+s$ por ser i_0 mínimo. Luego, para cada $1 \leq j \leq i_0$ tenemos

$$r_{j-1} + r_j \geq r_{i_0-1} + r_{i_0} > (d+s) + d = 2d+s.$$

Esta condición, junto con $r_j \geq r_{i_0} \geq d$, nos permite aplicar el Lema 5.1.6 al índice $j=1$, luego al índice $j=2$ y así sucesivamente hasta $j = i_0$. De este modo resulta

$$\begin{aligned}
\mathrm{MSres}_d(f,g)(X_s) &= \lambda \mathrm{MSyl}_{0,d}(A,B)(X_s) \\
&= \lambda' \mathrm{MSyl}_{0,d}(C_{i_0+1}, C_{i_0})(X_s) \\
&= \lambda' \sum_{\substack{C'\cup C'' = C_{i_0} \\ |C'|=d, |C''| = r_{i_0}-d}} \frac{\mathcal{R}(C_{i_0+1}, C'')\mathcal{R}(X_s, C')}{\mathcal{R}(C', C'')}, \qquad (5.2)
\end{aligned}$$

con $\lambda' \in K\backslash\{0\}$. Notemos que incluso si $i_0 = 0$ la igualdad (5.2) también vale trivialmente, pues en ese caso $C_{i_0} = B$ y $C_{i_0+1} = A$, de modo que podemos dejar de suponer $i_0 \geq 1$. Ahora,

$$|C_{i_0} \cap C_{i_0+1}| = \deg(\mathrm{mcd}(R_{i_0}, R_{i_0+1})) = \deg(\mathrm{mcd}(f,g)) = r_k,$$

por lo que $|C_{i_0}\backslash C_{i_0+1}| = r_{i_0} - r_k \geq r_{i_0} - d$. Existe entonces $\widetilde{C} \subset C_{i_0}\backslash C_{i_0+1}$ tal que $|\widetilde{C}| = r_{i_0} - d$. Por otro lado, como $s > r_{i_0} - d$, en (5.2) podemos evaluar las primeras $r_{i_0} - d$ variables de X_s en los elementos del conjunto $\widetilde{C}$, poniendo $X_s = \widetilde{C} \cup Y$, donde Y es un conjunto de variables con $|Y| = s - (r_{i_0} - d)$. Nos queda, dada la elección de $\widetilde{C}$,

$$\begin{aligned}
\lambda' \sum_{\substack{C'\cup C'' = C_{i_0} \\ |C'|=d, |C''| = r_{i_0}-d}} \frac{\mathcal{R}(C_{i_0+1}, C'')\mathcal{R}(\widetilde{C}\cup Y, C')}{\mathcal{R}(C', C'')} &= \lambda' \frac{\mathcal{R}(C_{i_0+1}, \widetilde{C})\mathcal{R}(\widetilde{C}\cup Y, C_{i_0}\backslash\widetilde{C})}{\mathcal{R}(C_{i_0}\backslash\widetilde{C}, \widetilde{C})} \\
&= \lambda' \mathcal{R}(C_{i_0+1}, \widetilde{C})\mathcal{R}(Y, C_{i_0}\backslash\widetilde{C}) \;\neq\; 0.
\end{aligned}$$

(2) Probemos ahora que si para todo i, $1 \leq i \leq k$, se tiene $d > r_i$ o $r_i > d + s$, entonces $\mathrm{MSres}_d(f,g)(X_s) = 0$. Sea i_0, $0 \leq i_0 \leq k$ tal que $r_{i_0+1} < d < d+s < r_{i_0}$. Razonando como en (1), pues de nuevo tenemos $r_{i_0-1} + r_{i_0} \geq 2d + s$ y $r_{i_0} \geq d$, en el caso $i_0 \geq 1$, resulta

$$\begin{aligned}\mathrm{MSres}_d(f,g)(X_s) &= \lambda \mathrm{MSyl}_{0,d}(A,B)(X_s)\\ &= \lambda' \mathrm{MSyl}_{0,d}(C_{i_0+1}, C_{i_0})(X_s)\\ &= \pm\lambda' \sum_{\substack{C'\cup C''=C_{i_0}\\ |C'|=d, |C''|=r_{i_0}-d}} \frac{\mathcal{R}(C_{i_0+1}, C'')\mathcal{R}(X_s, C')}{\mathcal{R}(C', C'')},\end{aligned}$$

que se cumple incluso si $i_0 = 0$. Aplicamos ahora la Observación 2.2.4 con $A = C_{i_0}$, $B = C_{i_0+1}$ y $C = X_s$ y con $p = r_{i_0} - d$ y $q = d$.

- Si $r_{i_0+1} + r_{i_0} - d \geq s + d$, i.e. $r_{i_0+1} + r_{i_0} \geq s + 2d$, aplicamos la primera igualdad en dicha observación y resulta

$$\begin{aligned}\sum_{\substack{C'\cup C''=C_{i_0}\\ |C'|=d, |C''|=r_{i_0}-d}} \frac{\mathcal{R}(C_{i_0+1}, C'')\mathcal{R}(X_s, C')}{\mathcal{R}(C', C'')} &= \pm \sum_{\substack{C^{(3)}\cup C^{(4)}=C_{i_0+1}\\ |C^{(3)}|=r_{i_0+1}-d, |C^{(4)}|=d}} \frac{\mathcal{R}(C^{(3)}, C_{i_0})\mathcal{R}(C^{(4)}, X_s)}{\mathcal{R}(C^{(3)}, C^{(4)})}\\ &= 0,\end{aligned}$$

  ya que $C^{(3)}$ tiene cardinal negativo por ser $r_{i_0+1} < d$.

- Si por el contrario $r_{i_0+1} + r_{i_0} - d \leq s + d$, i.e. $r_{i_0+1} + r_{i_0} \leq s + 2d$, aplicamos la segunda igualdad en la Observación 2.2.4 y tenemos

$$\begin{aligned}\sum_{\substack{C'\cup C''=C_{i_0}\\ |C'|=d, |C''|=r_{i_0}-d}} \frac{\mathcal{R}(C_{i_0+1}, C'')\mathcal{R}(X_s, C')}{\mathcal{R}(C', C'')} &= \pm \sum_{\substack{X'\cup X''=X_s\\ |X'|=s-(r_{i_0}-d)\\ |X''|=r_{i_0}-d}} \frac{\mathcal{R}(X', C_{i_0+1})\mathcal{R}(X'', C_{i_0})}{\mathcal{R}(X', X'')}\\ &= 0,\end{aligned}$$

  por tener X' cardinal negativo, pues $r_{i_0} - d > s$.

Esto prueba la primera afirmación del teorema.

Para probar la segunda afirmacion, supongamos primero que $d = r_{i_0}$ pero $r_{i_0-1} \geq d+s$, asumiendo por ahora que $i_0 \geq 1$. En este caso tenemos las mismas hipótesis que en (1), de modo que también llegamos a (5.2), que incluso vale si $i_0 = 0$. Pero ahora, como $d = r_{i_0}$, en (5.2) queda

$$\lambda' \mathcal{R}(X_s, C_{i_0}) = \lambda'' R_{i_0}(x_1) \cdots R_{i_0}(x_s),$$

como queríamos probar.

Supongamos por último que $d = r_{i_0-1} - s$, i.e. $r_{i_0-1} = s + d$ pero $r_{i_0} \leq d$. Aquí se vuelven a cumplir las hipótesis de (1), pero para $i_0 - 1$. Llegamos entonces a

$$\mathrm{MSres}_d(f,g)(X_s) = \lambda' \sum_{\substack{C'\cup C''=C_{i_0-1}\\ |C'|=d, |C''|=r_{i_0-1}-d}} \frac{\mathcal{R}(C_{i_0}, C'')\mathcal{R}(X_s, C')}{\mathcal{R}(C', C'')}.$$

Volvamos a aplicar la Observación 2.2.4, ahora para $A = C_{i_0-1}$, $B = C_{i_0}$, $C = X_s$, $p = r_{i_0-1} - d$ y $q = d$. En este caso

$$s + d = r_{i_0-1} \geq r_{i_0-1} + r_{i_0} - d,$$

por lo que usamos la segunda igualdad en dicha observación y nos queda

$$\sum_{\substack{C' \cup C'' = C_{i_0-1} \\ |C'|=d, |C''|=r_{i_0-1}-d}} \frac{\mathcal{R}(C_{i_0}, C'')\mathcal{R}(X_s, C')}{\mathcal{R}(C', C'')} = \pm \sum_{\substack{X' \cup X'' = X_s \\ |X'|=s-(r_{i_0-1}-d) \\ |X''|=r_{i_0-1}-d}} \frac{\mathcal{R}(X', C_{i_0-1})\mathcal{R}(X'', C_{i_0})}{\mathcal{R}(X', X'')},$$

que en este caso, dado que $s = r_{i_0-1} - d$, es igual a $\pm\mathcal{R}(X_s, C_{i_0}) = \pm\lambda'' R_{i_0}(x_1) \cdots R_{i_0}(x_s)$, como queríamos probar.

Sólo resta observar que se puede deducir el caso general del caso en que todos los polinomios R_i tienen raíces simples, de manera similar a como lo hicimos al principio de esta demostración para el caso $r_k < d$. □

El Teorema 5.1.2 nos dice que el polinomio $\mathrm{MSres}_d(f, g)(X_s)$ tiene más información que el polinomio subresultante, no sólo porque este teorema generaliza el Teorema 1.1.5, sino además porque la subresultante es un coeficiente de $\mathrm{MSres}_d(f, g)(X_s)$:

$$\mathrm{Sres}_d(f, g)(x_1) = \mathrm{coeff}_{x_2^d \cdots x_s^d} \left(\mathrm{MSres}_d(f, g)(X_s)\right).$$

Esto puede calcularse directamente de la definición, o más fácilmente, usando la Proposición 5.1.5 y la identidad

$$\mathrm{Syl}_{0,d}(A, B)(x_1) = \mathrm{coeff}_{x_2^d \cdots x_s^d} \left(\mathrm{MSyl}_{0,d}(A, B)(X_s)\right).$$

5.2. Matrices de Bézout

En esta sección obtendremos diferentes escrituras de los polinomios que definen las matrices de Bézout o Bezoutianos, que están muy ligadas a la resultantes y a las subresultantes. Daremos primero una breve introducción teórica.

5.2.1. Preliminares

Para esta parte necesitamos introducir la siguiente notación para matrices de Vandermonde.

Notación 5.2.1. Sea $X = (x_1, \ldots, x_k)$ una k-upla de indeterminadas o de elementos distintos y $\ell \in \mathbb{N}$. Denotamos

$$\mathcal{V}'_\ell(X) := \overset{k}{\boxed{\begin{array}{ccc} 1 & \cdots & 1 \\ \vdots & & \vdots \\ x_1^{\ell-1} & \cdots & x_k^{\ell-1} \end{array}}}\ \ell\ .$$

Cuando $\ell = k$ escribimos simplemente $\mathcal{V}'(X)$.

Usamos la notación $\mathcal{V}'$ para diferenciarla de la matriz de Vandermonde rectangular de la Notación 4.1.7, dado que aquí tomamos los exponentes de las filas en orden creciente.

Las matrices de Bézout son matrices cuadradas asociadas a dos polinomios univariados y fueron introducidas por él en 1764 ([Bez1764]). La notación actual y la denominación de *Bezoutianos* se debe a Sylvester ([Syl1853]). Aquí la definición precisa:

Definición 5.2.2. Sea K un cuerpo. Sean $f, g \in K[x]$ y sea $r \geq \text{máx}\{\deg(f), \deg(g)\}$. La *matriz de Bézout* de orden r asociada a f y a g se define como

$$B_r(f,g) := (c_{ij})_{1\leq,i,j\leq r} \in K^{r\times r},$$

donde los c_{ij} están caracterizados por la identidad

$$\Phi(x,y) := \frac{f(x)g(y) - f(y)g(x)}{x-y} = \sum_{1\leq i,j\leq r} c_{ij}x^{i-1}y^{j-1}.$$

Observemos que los c_{ij} están bien definidos ya que es claro que el cociente $\Phi(x,y)$ es realmente un polinomio en $K[x,y]$. En efecto, $x-y$ divide al numerador, pues éste se anula cuando $y = x$. Además los grados de este polinomio en x y en y son en efecto menores o iguales que $r-1$.

Uno puede explicitar los c_{ij} en términos de los coeficientes de f y de g según la siguiente observación.

Observación 5.2.3. ([ApJo2006, Ch. 5, Def. 5.1]) Si $f = \sum_{i=0}^{r} a_i x^i$ y $g = \sum_{j=0}^{r} b_j x^j$, los coeficientes c_{ij} de $B_r(f,g)$ satisfacen

$$c_{ij} = \sum_{s} a_{2r-(i+j)+1-s}b_s - a_s b_{2r-(i+j)+1-s},$$

donde la suma recorre los valores de s tales que $r-\text{mín}\{i,j\}+1 \leq s \leq \text{mín}\{r, 2r-(i+j)+1\}$.

La siguiente observación es trivial a partir de las definiciones anteriores.

Observación 5.2.4. Dados $x, y \in K$, se tiene

$$\Phi(x,y) = \mathcal{V}'_r(x)^T B_r(f,g)\mathcal{V}'_r(y),$$

donde la T denota la operación transponer.

Otras observaciones inmediatas que son consecuencias de propiedades de $\Phi(x,y)$:

1. $B_r(f,g)$ es una matriz simétrica.
2. $B_r(f,g) = -B_r(g,f)$.
3. $B_r(f,f) = 0$.

4. Queda inducida una aplicación

$$\begin{array}{rccc} B_r: & K[x]_{\leq r} \times K[x]_{\leq r} & \to & K^{r\times r} \\ & (f,g) & \mapsto & B_r(f,g), \end{array}$$

que resulta ser bilineal.

La matriz de Bézout proporciona otra forma de calcular la resultante, según la siguiente proposición, que se encuentra en [ApJo2006, Ch. 5, Prop. 17].

Proposición 5.2.5. *Sea K un cuerpo. Sean $f, g \in K[x]$ con $\deg(f) = m$ y $\deg(g) = n$ y supongamos $m \geq n$. Entonces*

$$\det(B_m(f,g)) = (-1)^{\frac{m(m-1)}{2}} a_m^{m-n} \mathrm{Res}(f,g),$$

donde a_m es el coeficiente principal de f.

Aquí hemos hecho, sin perder generalidad, la suposición $\deg(f) \geq \deg(g)$ y la haremos en el resto de la sección. Ésta es la suposición contraria a la que hicimos en los Capítulos 1 y 3 y en la Sección 5.1, pero aquí nos conviene hacerlo así para que sea más sencillo trabajar con el signo.

Más generalmente, pueden calcularse las subresultantes a través de matrices de Bézout. La siguiente proposición se encuentra en [ApJo2006, Ch. 9, Prop. 93].

Proposición 5.2.6. *Sea K un cuerpo. Sean $f, g \in K[x]$ con $\deg(f) = m$ y $\deg(g) = n$ y supongamos $m \geq n$. Sea $0 \leq d < \deg(g)$. Entonces*

$$\mathrm{Sres}_d(f,g)(x) = (-1)^{\frac{(m-d)(m-d-1)}{2}} \det \begin{pmatrix} h_{d+1}(x) & h_{d+2}(x) & \cdots & h_m(x) \\ c_{d+2,d+1} & c_{d+2,d+2} & \cdots & c_{d+2,m} \\ \vdots & \vdots & & \vdots \\ c_{m,d+1} & c_{m,d+2} & \cdots & c_{m,m} \end{pmatrix},$$

donde, para cada $1 \leq i \leq m$, se define

$$h_i(x) = \sum_{j=1}^{m} c_{ij} x^{j-1}.$$

Es claro que la Proposición 5.2.5 es el caso $d = 0$ de la Proposición 5.2.6.

El cálculo de subresultantes vía matrices de Bézout tiene la ventaja de que la matriz involucrada es de menor tamaño, sin embargo sus coeficientes son expresiones más complicadas que los coeficientes que aparecen en la matriz de Sylvester.

La Proposición 5.2.5 dice, en particular, que $\det(B_m(f,g)) = 0$ si, y sólo si, f y g tienen raíces en común. Esta propiedad es más general y lo muestra el siguiente teorema, que fue probado de manera independiente por Jacobi en [Jac1836] y por G. Darboux en [Dar1876].

Teorema 5.2.7. *[Teorema de Jacobi-Darboux] Sea K un cuerpo. Sean $f, g \in K[x]$ con $\deg(f) = m$ y $\deg(g) = n$ y supongamos $m \geq n$. Entonces $\mathrm{rk}(B_m(f,g)) = m - \deg(\mathrm{mcd}(f,g))$, donde* rk *denota el rango de la matriz.*

5.2.2. Matrices de Bézout y el lema de intercambio

Veremos ahora cómo podemos hacer algunas observaciones sencillas con el lema de intercambio aplicado a la construcción de las matrices de Bézout. Con el siguiente lema podemos escribir los polinomios $\Phi(x,y)$ en términos de las raíces de f o de g en el caso de raíces simples.

Lema 5.2.8. *Sea K un cuerpo y sean $f,g \in K[x]$ con $\deg(f)=m$ y $\deg(g)=n$. Supongamos que $m \geq n$ y que $f(x)=a_m\mathcal{R}(x,A)$ tiene raíces simples. Entonces*

$$\Phi(x,y) = a_m \sum_{\alpha\in A} \frac{g(\alpha)\mathcal{R}(\{x,y\},A\backslash\alpha)}{\mathcal{R}(\alpha,A\backslash\alpha)}.$$

Demostración. Si b_n es el coeficiente principal de g y B es el multiconjunto de raíces de g, o sea $g(x)=b_n\mathcal{R}(x,B)$, tenemos, por la Definición 5.2.2,

$$\begin{aligned}
\Phi(x,y) &= \frac{f(x)g(y)-f(y)g(x)}{x-y} = \frac{f(x)g(y)}{x-y} + \frac{f(y)g(x)}{y-x} \\
&= a_m b_n \left(\frac{\mathcal{R}(x,A)\mathcal{R}(y,B)}{\mathcal{R}(x,y)} + \frac{\mathcal{R}(y,A)\mathcal{R}(x,B)}{\mathcal{R}(y,x)} \right) \\
&= a_m b_n \sum_{\substack{T_1\cup T_2=\{x,y\}\\ |T_1|=|T_2|=1}} \frac{\mathcal{R}(T_2,A)\mathcal{R}(T_1,B)}{\mathcal{R}(T_2,T_1)} \\
&= (-1)^n a_m b_n \sum_{\substack{T_1\cup T_2=\{x,y\}\\ |T_1|=|T_2|=1}} \frac{\mathcal{R}(T_2,A)\mathcal{R}(B,T_1)}{\mathcal{R}(T_2,T_1)} \\
&= (-1)^n a_m b_n \sum_{\substack{A_1\cup A_2=A\\ |A_1|=1,\,|A_2|=m-1}} \frac{\mathcal{R}(\{x,y\},A_2)\mathcal{R}(B,A_1)}{\mathcal{R}(A_1,A_2)} \qquad (5.3) \\
&= a_m \sum_{\alpha\in A} \frac{\mathcal{R}(\{x,y\},A\backslash\alpha)g(\alpha)}{\mathcal{R}(\alpha,A\backslash\alpha)}, \qquad (5.4)
\end{aligned}$$

usando en (5.3) el Teorema 2.2.2 para $A=\{x,y\}$, $B=A$ y $X=B$, y llamando $\{\alpha\}=A_1$ en (5.4). □

Con esta reescritura es inmediata la siguiente observación.

Observación 5.2.9. Sea K un cuerpo y sean $f,g \in K[x]$ con $\deg(f)=m$ y $\deg(g)=n$. Supongamos que $m \geq n$, que $f=a_m\mathcal{R}(x,A)$ tiene raíces simples y $g=b_n\mathcal{R}(x,B)$ donde B es un multiconjunto. Entonces,

$$\mathrm{coeff}_{y^{m-1}}(\Phi(x,y)) = (-1)^{m-1}a_m b_n \mathrm{Syl}_{m-1,0}(A,B)(x) = a_m b_n \mathrm{Sres}_{m-1}(f,g)(x).$$

En particular esto muestra que la última fila (o columna) de la matriz $B_m(f,g)$ contiene exactamente los coeficientes del polinomio $\mathrm{Sres}_{m-1}(f,g)(x)$, salvo el coeficiente a_m.

Como consecuencia también podemos obtener expresiones alternativas para los coeficientes c_{ij} de la matriz $B_m(f,g)$:

Corolario 5.2.10. *Sea K un cuerpo y sean $f, g \in K[x]$ con $\deg(f) = m$ y $\deg(g) = n$. Supongamos que $m \geq n$ y que $f(x) = a_m \mathcal{R}(x, A)$ tiene raíces simples. Sea $B_m(f, g) = (c_{ij})_{1 \leq i,j \leq m}$ la matriz de Bézout asociada a f y g. Entonces se tiene, para $1 \leq i, j \leq m$,*

$$c_{ij} = (-1)^{i+j} a_m \sum_{\alpha \in A} \frac{g(\alpha) e_{m-i}(A \backslash \alpha) e_{m-j}(A \backslash \alpha)}{\mathcal{R}(\alpha, A \backslash \alpha)},$$

recordando que e_k es el k-ésimo polinomio simétrico elemental que usamos en el Capítulo 2 y que definimos como

$$e_k(Z) := \sum_{1 \leq i_1 < \cdots < i_\ell \leq r} z_{i_1} \cdots z_{i_\ell},$$

para un conjunto $Z = \{z_1, \ldots, z_\ell\}$ y $0 \leq k \leq \ell - 1$, y con $e_0(Z) := 1$.

Demostración. Por definición, $c_{ij} = \operatorname{coeff}_{x^{i-1} y^{j-1}}(\Phi(x, y))$. Luego, por el Lema 5.2.8, tenemos

$$c_{ij} = a_m \sum_{\alpha \in A} \frac{g(\alpha)}{\mathcal{R}(\alpha, A \backslash \alpha)} \operatorname{coeff}_{x^{i-1} y^{j-1}}(\mathcal{R}(\{x, y\}, A \backslash \alpha)).$$

Basta entonces recordar la conocida relación entre coeficientes y raíces de un polinomio:

$$\operatorname{coeff}_{x^k}(\mathcal{R}(x, Z)) = (-1)^{r-l} e_{r-\ell}(Z),$$

si $|Z| = \ell$. □

Con esta escritura es fácil ver una desigualdad en el Teorema 5.2.7 en el caso en que f tiene raíces simples. Después mostraremos cómo probar la igualdad del teorema, bajo la misma suposición para f, pero es interesante ver cómo sale de manera sencilla una de las desigualdades gracias al Lema 5.2.8.

Lema 5.2.11. *Sea K un cuerpo y sean $f, g \in K[x]$ con $\deg(f) = m$ y $\deg(g) = n$. Supongamos que $m \geq n$, que $f = a_m \mathcal{R}(x, A)$ tiene raíces simples y $g = b_n \mathcal{R}(x, B)$ donde B es un multiconjunto. Sea $\gamma \in A \cap B$. Entonces, $B_m(f, g) \mathcal{V}'_m(\gamma) = 0$.*

Demostración. Queremos ver que $\sum_{j=1}^m c_{ij} \gamma^{j-1} = 0$ para todo $1 \leq i \leq m$. Dado un tal i fijo, por el Corolario 5.2.10, tenemos

$$\begin{aligned}
\sum_{j=1}^m c_{ij} \gamma^{j-1} &= \sum_{j=1}^m ((-1)^{i+j} a_m \sum_{\alpha \in A} \frac{g(\alpha) e_{m-i}(A \backslash \alpha) e_{m-j}(A \backslash \alpha)}{\mathcal{R}(\alpha, A \backslash \alpha)}) \gamma^{j-1} \\
&= (-1)^{m-i} a_m \sum_{\alpha \in A} \frac{g(\alpha) e_{m-i}(A \backslash \alpha)}{\mathcal{R}(\alpha, A \backslash \alpha)} \sum_{j=1}^m (-1)^{m-j} e_{m-j}(A \backslash \alpha) \gamma^{j-1} \\
&= (-1)^{m-i} a_m \sum_{\alpha \in A} \frac{g(\alpha) e_{m-i}(A \backslash \alpha)}{\mathcal{R}(\alpha, A \backslash \alpha)} \sum_{j=0}^{m-1} (-1)^{(m-1)-j} e_{(m-1)-j}(A \backslash \alpha) \gamma^j \\
&= (-1)^{m-i} a_m \sum_{\alpha \in A} \frac{g(\alpha) e_{m-i}(A \backslash \alpha)}{\mathcal{R}(\alpha, A \backslash \alpha)} \mathcal{R}(\gamma, A \backslash \alpha) \\
&= (-1)^{m-i} a_m g(\gamma) e_{m-i}(A \backslash \alpha_0) = 0,
\end{aligned}$$

usando en la última igualdad que $\gamma \in B$. □

Corolario 5.2.12. *Sea K un cuerpo y sean $f, g \in K[x]$ con $\deg(f) = m$ y $\deg(g) = n$. Supongamos que $m \geq n$ y que f tiene raíces simples. Sea $B_m(f,g)$ la matriz de Bézout asociada a f y g. Entonces,* $\mathrm{rk}(B_m(f,g)) \leq m - \deg(\mathrm{mcd}(f,g))$.

Demostración. Llamemos $A \cap B = \{\gamma_1, \ldots, \gamma_s\}$, notando, en particular, $s = \deg(\mathrm{mcd}(f,g))$. Por el Lema 5.2.11 tenemos que $\langle \mathcal{V}'_m(\gamma_1), \ldots, \mathcal{V}'_m(\gamma_s) \rangle \subset \mathrm{Ker}(B_m(f,g))$. Además, como los γ_i son distintos, $\{\mathcal{V}'_m(\gamma_1), \ldots, \mathcal{V}'_m(\gamma_s)\}$ es un conjunto de vectores linealmente independiente. Esto implica entonces que

$$s \leq \dim_K(\mathrm{Ker}(B_m(f,g))) = m - r_k(B_m(f,g)),$$

como queríamos ver. □

Veremos ahora que tanto este resultado, y más en general el Teorema 5.2.7 en el caso de raíces simples, como la Proposición 5.2.5, pueden derivarse como consecuencia de una escritura de la matriz $B_m(f,g)$ en otra base. Precisamente, la escritura del Lema 5.2.8 sugiere que sería más fácil trabajar con los coeficientes de $\Phi(x,y)$ en otra base. Llamemos $A = \{\alpha_1, \ldots, \alpha_m\}$ y consideremos el conjunto

$$\left\{ q_{ij}(x,y) := \frac{\mathcal{R}(x, A\backslash\alpha_i)}{\mathcal{R}(\alpha_i, A\backslash\alpha_i)} \frac{\mathcal{R}(y, A\backslash\alpha_j)}{\mathcal{R}(\alpha_j, A\backslash\alpha_j)};\ 1 \leq i, j \leq m \right\}.$$

Es fácil ver que este conjunto es una base del espacio vectorial de polinomios en $K[x,y]$ con grados en x y en y acotados por $m-1$ y, por lo tanto, existen únicos $a_{ij} \in K$, con $1 \leq i, j \leq m$, tales que

$$\Phi(x,y) = \sum_{1 \leq i,j \leq m} a_{ij}\, q_{ij}(x,y).$$

Esta base es más compatible con la escritura del Lema 5.2.5 ya que se ve fácilmente que

$$\begin{aligned} a_{ij} = \mathrm{coeff}_{q_{ij}(x,y)}(\Phi(x,y)) &= a_m \sum_{\alpha \in A} g(\alpha) \mathrm{coeff}_{q_{ij}(x,y)} \left(\frac{\mathcal{R}(\{x,y\}, A\backslash\alpha)}{\mathcal{R}(\alpha, A\backslash\alpha)} \right) \\ &= \begin{cases} a_m g(\alpha_i) \mathcal{R}(\alpha_i, A\backslash\alpha_i) & \text{si } i = j \\ 0 & \text{si } i \neq j \end{cases} \\ &= \begin{cases} g(\alpha_i) f'(\alpha_i) & \text{si } i = j \\ 0 & \text{si } i \neq j. \end{cases} \end{aligned} \tag{5.5}$$

Luego, si consideramos la matriz $(a_{ij})_{1 \leq i,j \leq m}$, ésta resulta diagonal y se simplifican varios resultados. En la siguiente proposición relacionamos la matriz de Bézout con esta matriz diagonal de manera precisa.

Proposición 5.2.13. *Sea K un cuerpo y sean $f, g \in K[x]$ con $\deg(f) = m$ y $\deg(g) = n$. Supongamos que $m \geq n$ y que $f = a_m \mathcal{R}(x, A)$ tiene raíces simples, con $A = \{\alpha_1, \ldots, \alpha_m\}$. Sea $B_m(f,g)$ la matriz de Bézout asociada a f y g. Entonces,*

$$\mathcal{V}'(A)^T B_m(f,g) \mathcal{V}'(A) = \mathrm{Diag}(g(\alpha_1)f'(\alpha_1), \ldots, g(\alpha_m)f'(\alpha_m)).$$

Demostración. Definamos

$$\mathcal{L}_m(x) := \begin{pmatrix} \frac{\mathcal{R}(x,A\backslash\alpha_1)}{\mathcal{R}(\alpha_1,A\backslash\alpha_1)} \\ \vdots \\ \frac{\mathcal{R}(x,A\backslash\alpha_m)}{\mathcal{R}(\alpha_m,A\backslash\alpha_m)} \end{pmatrix}.$$

Veamos que $\mathcal{V}'(A)\mathcal{L}_m(x) = \mathcal{V}'_m(x)$. Esto es, veamos que para todo $1 \leq i \leq m$, se tiene

$$\sum_{j=1}^{m} \alpha_j^{i-1} \frac{\mathcal{R}(x, A\backslash\alpha_j)}{\mathcal{R}(\alpha_j, A\backslash\alpha_j)} = x^{i-1}.$$

Pero esto es cierto por la interpolación de Lagrange (Proposición 2.1.1). Luego, tenemos

$$\begin{aligned} \Phi(x,y) = \mathcal{V}'_m(x)^T B_m(f,g)\mathcal{V}'_m(y) &= (\mathcal{V}'(A)\mathcal{L}_m(x))^T B_m(f,g)(\mathcal{V}'(A)\mathcal{L}_m(y)) \\ &= \mathcal{L}_m(x)^T(\mathcal{V}'(A)^T B_m(f,g)\mathcal{V}'(A))\mathcal{L}_m(y). \end{aligned}$$

Pero por otro lado, por (5.5),

$$\begin{aligned} \Phi(x,y) &= \sum_{1\leq i,j\leq m} a_{ij}\, q_{ij}(x,y) \\ &= \sum_{1\leq i\leq m} g(\alpha_i)f'(\alpha_i)q_{ii}(x,y) \\ &= \sum_{1\leq i\leq m} \frac{\mathcal{R}(x,A\backslash\alpha_i)}{\mathcal{R}(\alpha_i,A\backslash\alpha_i)} g(\alpha_i)f'(\alpha_i) \frac{\mathcal{R}(y,A\backslash\alpha_i)}{\mathcal{R}(\alpha_i,A\backslash\alpha_i)} \\ &= \mathcal{L}_m(x)^T \mathrm{Diag}(g(\alpha_1)f'(\alpha_1),\ldots,g(\alpha_m)f'(\alpha_m))\mathcal{L}_m(y). \end{aligned}$$

Como estas identidades valen para todo x e y, queda probado el enunciado. □

Con esta diagonalización de la matriz de Bézout pueden deducirse fácilmente la Proposición 5.2.5 y el Teorema 5.2.7.

Corolario 5.2.14. *Sea K un cuerpo y sean $f, g \in K[x]$ con $\deg(f) = m$ y $\deg(g) = n$. Supongamos que $m \geq n$ y que $f = a_m\mathcal{R}(x, A)$ tiene raíces simples. Sea $B_m(f,g)$ la matriz de Bézout asociada a f y g. Entonces,*

1. $\det(B_m(f,g)) = (-1)^{\frac{m(m-1)}{2}} a_m^{m-n}\mathrm{Res}(f,g)$.
2. $\mathrm{rk}(B_m(f,g)) = m - \deg(\mathrm{mcd}(f,g))$.

Demostración. Tomando determinante a ambos lados en la igualdad de la Proposición 5.2.13 tenemos

$$(\det(\mathcal{V}'(A)))^2 \det(B_m(f,g)) = \prod_{i=1}^{m} g(\alpha_i)f'(\alpha_i) = a_m^{-n}\mathrm{Res}(f,g)\prod_{i=1}^{m} f'(\alpha_i),$$

pues, por la fórmula de Poisson, se tiene $\mathrm{Res}(f,g) = a_m^n \prod_{i=1}^m g(\alpha_i)$.

Por otro lado, como $f = a_m \mathcal{R}(x, A) = a_m \prod_{a \in A} (x - a)$:

$$f' = a_m \sum_{a \in A} \prod_{a' \in A \setminus a} (x - a').$$

Con lo cual

$$f'(\alpha_i) = a_m \prod_{a' \in A \setminus \alpha_i} (\alpha_i - a') = a_m \mathcal{R}(\alpha_i, A \setminus \alpha_i). \tag{5.6}$$

Pero

$$\prod_{i=1}^{m} a_m \mathcal{R}(\alpha_i, A \setminus \alpha_i) = a_m^m \prod_{i<j} (\alpha_i - \alpha_j)(\alpha_j - \alpha_i) = (-1)^{\frac{m(m-1)}{2}} a_m^m \prod_{i<j} (\alpha_i - \alpha_j)^2$$
$$= (-1)^{\frac{m(m-1)}{2}} \det(\mathcal{V}'(A))^2,$$

lo cual prueba (1), dado que $\mathcal{V}'(A) \neq 0$.

Para probar (2) notemos que $\mathrm{rk}(B_m(f, g))) = \mathrm{rk}(\widetilde{B}_m(f, g))$, donde $\widetilde{B}_m(f, g) = \mathrm{Diag}(g(\alpha_1)f'(\alpha_1), \ldots, g(\alpha_m)f'(\alpha_m))$. Esto es simplemente porque $\mathcal{V}'(A)$ es una matriz inversible. Pero es claro que $\mathrm{rk}(\widetilde{B}_m(f, g))$ es igual a $m - s$, siendo s la cantidad de α_i que pertenecen a B. Esto es, $s = |A \cap B| = \deg(\mathrm{mcd}(f, g))$, como queríamos probar. □

Otra consecuencia de esta diagonalización es el cálculo de la matriz inversa de $B_m(f, g)$ cuando f y g no tienen raíces en común. Esto se puede encontrar en [KST2006] con una técnica similar a la que desarrollamos aquí.

Finalmente usaremos el lema de intercambio para obtener otra reescritura de los polinomios $\Phi(x, y)$. La escritura del Lema 5.2.8 necesita que f tenga raíces simples. Usando la Observación 2.2.7 lograremos una escritura para el caso general.

Lema 5.2.15. *Sea K un cuerpo y sean $f, g \in K[x]$ con $\deg(f) = m$ y $\deg(g) = n$ y supongamos que $m \geq n$. Sean A y B los respectivos multiconjuntos de raíces de f y de g, y a_m, b_n sus coeficientes principales. Sea $E \subset K$ un conjunto finito tal que $|E| \geq m + 1$. Entonces*

$$\Phi(x, y) = a_m b_n \sum_{\substack{E_1 \cup E_2 \cup E_3 = E \\ |E_1|=1, |E_2|=m-1, |E_3|=|E|-m}} \frac{\mathcal{R}(E_3, A)\mathcal{R}(E_1, B)\mathcal{R}(\{x, y\}, E_2)}{\mathcal{R}(E_3, E_1)\mathcal{R}(E_3, E_2)\mathcal{R}(E_1, E_2)}.$$

En particular, si $|E| = m + 1$,

$$\Phi(x, y) = \sum_{\{\gamma, \epsilon\} \subset E} \frac{f(\epsilon)g(\gamma)\mathcal{R}(\{x, y\}, E \setminus \{\gamma, \epsilon\})}{(\epsilon - \gamma)\mathcal{R}(\{\gamma, \epsilon\}, E \setminus \{\gamma, \epsilon\})}.$$

Demostración.

$$\begin{aligned}
\Phi(x,y) &= a_m b_n \sum_{\substack{A_1\cup A_2=A\\ |A_1|=1,\,|A_2|=m-1}} \frac{\mathcal{R}(\{x,y\},A_2)\mathcal{R}(A_1,B)}{\mathcal{R}(A_1,A_2)} \\
&= (-1)^n a_m b_n \sum_{\substack{A_1\cup A_2=A\\ |A_1|=1,\,|A_2|=m-1}} \frac{\mathcal{R}(\{x,y\},A_2)\mathcal{R}(B,A_1)}{\mathcal{R}(A_1,A_2)} \\
&= (-1)^n a_m b_n \sum_{\substack{E_1\cup E_2\cup E_3=E\\ |E_1|=1,|E_2|=m-1,|E_3|=|E|-m}} \frac{\mathcal{R}(E_3,A)\mathcal{R}(\{x,y\},E_2)\mathcal{R}(B,E_1)}{\mathcal{R}(E_3,E_1)\mathcal{R}(E_3,E_2)\mathcal{R}(E_1,E_2)} \qquad (5.7)\\
&= a_m b_n \sum_{\substack{E_1\cup E_2\cup E_3=E\\ |E_1|=1,|E_2|=m-1,|E_3|=|E|-m}} \frac{\mathcal{R}(E_3,A)\mathcal{R}(E_1,B)\mathcal{R}(\{x,y\},E_2)}{\mathcal{R}(E_3,E_1)\mathcal{R}(E_3,E_2)\mathcal{R}(E_1,E_2)},
\end{aligned}$$

aplicando en (5.7) la Observación 2.2.7 (2) para $B = A$, $X = B$ y $Y = \{x, y\}$. En efecto, $|E| \geq m + 1 \geq \text{máx}\{|B| + 1, |\{x, y\}| + (m - 1), |A|\}$. □

Corolario 5.2.16. *Sea K un cuerpo y sean $f, g \in K[x]$ con $\deg(f) = m$ y $\deg(g) = n$ y supongamos que $m \geq n$. Sean A y B los respectivos multiconjuntos de raíces de f y de g, y a_m, b_n sus coeficientes principales. Sea $E \subset K$ un conjunto finito tal que $|E| \geq m + 1$. Sea $B_m(f, g) = (c_{ij})_{1\leq i,j\leq m}$ la matriz de Bézout asociada a f y g. Entonces se tiene para cada $1 \leq i, j \leq m$,*

$$c_{ij} = (-1)^{i+j} a_m b_n \sum_{\substack{E_1\cup E_2\cup E_3=E\\ |E_1|=1,|E_2|=m-1,|E_3|=|E|-m}} \frac{\mathcal{R}(E_3,A)\mathcal{R}(E_1,B)e_{m-i}(E_2)e_{m-j}(E_2)}{\mathcal{R}(E_3,E_1)\mathcal{R}(E_3,E_2)\mathcal{R}(E_1,E_2)}.$$

En particular, si $|E| = m + 1$,

$$c_{ij} = (-1)^{i+j} \sum_{\{\gamma,\epsilon\}\subset E} \frac{f(\epsilon)g(\gamma)e_{m-i}(E\backslash\{\gamma,\epsilon\})e_{m-j}(E\backslash\{\gamma,\epsilon\})}{(\epsilon-\gamma)\mathcal{R}(\{\gamma,\epsilon\},E\backslash\{\gamma,\epsilon\})}.$$

Demostración. La demostración es análoga a la demostración del Corolario 5.2.10. □

Observemos que en el caso particular $|E| = m+1$, el Lema 5.2.15 y el Corolario 5.2.16 nos dan fórmulas en términos de los valores que toman f y g en E. El tamaño de E es óptimo para f, pues f queda definido por su interpolación en $m + 1$ puntos. En el caso que $n = m$ el conjunto E será óptimo para ambos. Notamos a posteriori que un desarrollo similar para obtener una fórmula parecida puede encontrarse en [Sha2004].

Podemos obtener también una fórmula del estilo de la que obtuvimos para la suma doble de Sylvester en la Proposición 4.2.1, logrando que f y g interpolen en distintos conjuntos de puntos.

Lema 5.2.17. *Sea K un cuerpo y sean $f, g \in K[x]$ con $\deg(f) = m$ y $\deg(g) = n$, con $m \geq n$. Sean A y B los respectivos multiconjuntos de raíces de f y de g, y a_m, b_n sus*

coeficientes principales. Sean $0 \leq p, q \leq m$ *tales que* $p+q = m-1$. *Sean* E *y* F *conjuntos tales que* $|E| \geq m+1$ *y* $|F| \geq m+1$. *Entonces*

$$\binom{m-1}{p}\Phi(x,y) \;=\; (-1)^{p(m-d)+(m-n)(|F|-m)}a_m b_n \sum_{\substack{E_1\cup E_2\cup E_3=E\\ |E_1|=p,|E_2|=m-p\\ |E_3|=|E|-m}} \sum_{\substack{F_1\cup F_2\cup F_3=F\\ |F_1|=q,|F_2|=m-q\\ |F_3|=|F|-m}}$$

$$\frac{\mathcal{R}(A,E_3)\mathcal{R}(B,F_3)\mathcal{R}(E_2,F_2)\mathcal{R}(E_1,F_1)\mathcal{R}(\{x,y\},E_1)\mathcal{R}(\{x,y\},F_1)(e_{|F|-m-1}(F_3))^{m-n}}{\mathcal{R}(E_1,E_2)\mathcal{R}(E_1,E_3)\mathcal{R}(E_2,E_3)\mathcal{R}(F_1,F_2)\mathcal{R}(F_1,F_3)\mathcal{R}(F_2,F_3)}.$$

En particular, si $|E| = |F| = m+1$,

$$\binom{m-1}{p}\Phi(x,y) \;=\; (-1)^{p(m-d)+(m-n)}$$

$$\cdot \sum_{\substack{E_1\cup E_2\cup\{\gamma\}=E\\ |E_1|=p,|E_2|=m-p}} \sum_{\substack{F_1\cup F_2\cup\{\epsilon\}=F\\ |F_1|=q,|F_2|=m-q}} \frac{f(\gamma)g(\epsilon)\mathcal{R}(E_2,F_2)\mathcal{R}(E_1,F_1)\mathcal{R}(\{x,y\},E_1)\mathcal{R}(\{x,y\},F_1)}{\mathcal{R}(E_1,E_2)\mathcal{R}(E_1,E_3)\mathcal{R}(E_2,E_3)\mathcal{R}(F_1,F_2)\mathcal{R}(F_1,F_3)\mathcal{R}(F_2,F_3)}.$$

Demostración. Supongamos primero que $n = m$. Tenemos

$$\begin{aligned}
&\binom{m-1}{p}\Phi(x,y)\\
&= a_m b_m \binom{m-1}{p} \sum_{\substack{A_1\cup A_2=A\\ |A_1|=1,\,|A_2|=m-1}} \frac{\mathcal{R}(\{x,y\},A_2)\mathcal{R}(A_1,B)}{\mathcal{R}(A_1,A_2)} \qquad (5.8)\\
&= (-1)^{p(m-d)}a_m b_m \sum_{\substack{A'\cup A''=A\\ |A'|=p\\ |A''|=m-p}} \sum_{\substack{B'\cup B''=B\\ |B'|=q\\ |B''|=m-q}} \frac{\mathcal{R}(A',B')\mathcal{R}(A'',B'')\mathcal{R}(\{x,y\},A')\mathcal{R}(\{x,y\},B')}{\mathcal{R}(A',A'')\mathcal{R}(B',B'')},
\end{aligned}$$

usando la Proposición 2.2.9 con $X' = X'' = \{x,y\}$ y $d = m-1$. En efecto,

$$|\{x,y\}| = 2 = m+m-2(m-1) = |A|+|B|-2(m-1).$$

Por otro lado

$$\sum_{\substack{A'\cup A''=A\\ |A'|=p,|A''|=m-p}} \sum_{\substack{B'\cup B''=B\\ |B'|=q,\,|B''|=m-q}} \frac{\mathcal{R}(A',B')\mathcal{R}(A'',B'')\mathcal{R}(\{x,y\},A')\mathcal{R}(\{x,y\},B')}{\mathcal{R}(A',A'')\mathcal{R}(B',B'')}$$

$$= \sum_{\substack{E_1\cup E_2\cup E_3=E\\ |E_1|=p,|E_2|=m-p,|E_3|=|E|-m}} \sum_{\substack{F_1\cup F_2\cup F_3=F\\ |F_1|=q,|F_2|=m-q,|F_3|=|F|-m}} \frac{\mathcal{R}(A,E_3)\mathcal{R}(B,F_3)\mathcal{R}(E_2,F_2)\mathcal{R}(E_1,F_1)\mathcal{R}(\{x,y\},E_1)\mathcal{R}(\{x,y\},F_1)}{\mathcal{R}(E_1,E_2)\mathcal{R}(E_1,E_3)\mathcal{R}(E_2,E_3)\mathcal{R}(F_1,F_2)\mathcal{R}(F_1,F_3)\mathcal{R}(F_2,F_3)},$$

debido a la Proposición 4.2.1. En efecto, $\max\{|\{x,y\}|+(m-1), m+m-(m-1), m\} = m+1 \leq |E|, |F|$. Esto prueba el caso $n = m$.

Para el caso general el truco será una vez más agrandar el conjunto B para llevarlo al caso que probamos. Supongamos entonces $n < m$ y sea $Y = (y_1, \ldots, y_{m-n})$.

Tenemos

$$\Phi(x,y) = a_m b_n \sum_{\substack{A_1\cup A_2 = A \\ |A_1|=1,\, |A_2|=m-1}} \frac{\mathcal{R}(\{x,y\},A_2)\mathcal{R}(A_1,B)}{\mathcal{R}(A_1,A_2)}$$

$$= (-1)^{m-n} a_m b_n \mathrm{coeff}_{y_1\cdots y_{m-n}} \left(\sum_{\substack{A_1\cup A_2 = A \\ |A_1|=1,\, |A_2|=m-1}} \frac{\mathcal{R}(\{x,y\},A_2)\mathcal{R}(A_1,B\cup Y)}{\mathcal{R}(A_1,A_2)} \right).$$

Ahora, considerando $B\cup Y$ en lugar de B, estamos en el caso anterior, pues $|B\cup Y| = m$. Luego

$$(-1)^{p(m-d)}\binom{m-1}{p} \sum_{\substack{A_1\cup A_2 = A \\ |A_1|=1,\, |A_2|=m-1}} \frac{\mathcal{R}(\{x,y\},A_2)\mathcal{R}(A_1,B\cup Y)}{\mathcal{R}(A_1,A_2)}$$

$$= \sum_{\substack{E_1\cup E_2\cup E_3 = E \\ |E_1|=p \\ |E_2|=m-p \\ |E_3|=|E|-m}} \sum_{\substack{F_1\cup F_2\cup F_3 = F \\ |F_1|=q \\ |F_2|=m-q \\ |F_3|=|F|-m}} \frac{\mathcal{R}(A,E_3)\mathcal{R}(B\cup Y,F_3)\mathcal{R}(E_2,F_2)\mathcal{R}(E_1,F_1)\mathcal{R}(\{x,y\},E_1)\mathcal{R}(\{x,y\},F_1)}{\mathcal{R}(E_1,E_2)\mathcal{R}(E_1,E_3)\mathcal{R}(E_2,E_3)\mathcal{R}(F_1,F_2)\mathcal{R}(F_1,F_3)\mathcal{R}(F_2,F_3)}.$$

El coeficiente de $y_1\cdots y_{m-n}$ en esta última suma resulta ser

$$(-1)^{(|F|-m-1)(m-n)} \sum_{\substack{E_1\cup E_2\cup E_3 = E \\ |E_1|=p,|E_2|=m-p,|E_3|=|E|-m}} \sum_{\substack{F_1\cup F_2\cup F_3 = F \\ |F_1|=q,|F_2|=m-q,|F_3|=|F|-m}}$$
$$\frac{\mathcal{R}(A,E_3)\mathcal{R}(B,F_3)(e_{|F|-m-1}(F_3))^{m-n}\mathcal{R}(E_2,F_2)\mathcal{R}(E_1,F_1)\mathcal{R}(\{x,y\},E_1)\mathcal{R}(\{x,y\},F_1)}{\mathcal{R}(E_1,E_2)\mathcal{R}(E_1,E_3)\mathcal{R}(E_2,E_3)\mathcal{R}(F_1,F_2)\mathcal{R}(F_1,F_3)\mathcal{R}(F_2,F_3)},$$

lo cual concluye la demostración. □

Obviamente tenemos un corolario similar con análoga demostración.

Corolario 5.2.18. *Sea K un cuerpo y sean $f,g\in K[x]$ con $\deg(f)=m$ y $\deg(g)=n$, con $m\geq n$. Sean A y B los respectivos multiconjuntos de raíces de f y de g, y a_m, b_n sus coeficientes principales. Sean $0\leq p,q\leq m$ tales que $p+q=m-1$. Sean E y F conjuntos tales que $|E|\geq m+1$ y $|F|\geq m+1$. Sea $B_m(f,g)=(c_{ij})_{1\leq i,j\leq m}$ la matriz de Bézout asociada a f y g. Entonces se tiene, para $1\leq i,j\leq m$,*

$$\binom{m-1}{p} c_{ij} = (-1)^{p(m-d)+(m-n)(|F|-m)+i+j} a_m b_n \cdot$$
$$\sum_{\substack{E_1\cup E_2\cup E_3 = E \\ |E_1|=p,|E_2|=m-p,|E_3|=|E|-m}} \sum_{\substack{F_1\cup F_2\cup F_3 = F \\ |F_1|=q,|F_2|=m-q,|F_3|=|F|-m}}$$
$$\frac{\mathcal{R}(A,E_3)\mathcal{R}(B,F_3)\mathcal{R}(E_2,F_2)\mathcal{R}(E_1,F_1)e_{m-i}(E_1\cup F_1)e_{m-j}(E_1\cup F_1)(e_{|F|-m-1}(F_3))^{m-n}}{\mathcal{R}(E_1,E_2)\mathcal{R}(E_1,E_3)\mathcal{R}(E_2,E_3)\mathcal{R}(F_1,F_2)\mathcal{R}(F_1,F_3)\mathcal{R}(F_2,F_3)}.$$

En particular, si $|E|=|F|=m+1$,

$$\binom{m-1}{p} c_{ij} = (-1)^{p(m-d)+(m-n)+i+j}\cdot$$
$$\sum_{\substack{E_1\cup E_2\cup\{\gamma\}=E\\ |E_1|=p\\ |E_2|=m-p}} \sum_{\substack{F_1\cup F_2\cup\{\epsilon\}=F\\ |F_1|=q\\ |F_2|=m-q}} \frac{f(\gamma)g(\epsilon)\mathcal{R}(E_2,F_2)\mathcal{R}(E_1,F_1)e_{m-i}(E_1\cup F_1)e_{m-j}(E_1\cup F_1)}{\mathcal{R}(E_1,E_2)\mathcal{R}(E_1,E_3)\mathcal{R}(E_2,E_3)\mathcal{R}(F_1,F_2)\mathcal{R}(F_1,F_3)\mathcal{R}(F_2,F_3)}.$$

5.3. Aplicación a una base de Gröbner

Fijemos A y B, dos subconjuntos de un cuerpo K, con $|A| = m$ y $B = \{\beta_1, \ldots, \beta_n\}$, y sean $f(x) = \mathcal{R}(x, A)$ y $g = \mathcal{R}(x, B)$. En el Capítulo 3 dimos una demostración de la Proposición 3.1.6, que muestra la igualdad entre la suma simple de Sylvester y la subresultante, usando de manera auxiliar el polinomio $\mathrm{MSyl}_{0,d}(A,B)(X)$ de la Notación 3.1.1. Volvamos a considerar ese polinomio pero olvidándonos del signo. Sea $X = (x_1, \ldots, x_{n-d})$ y llamemos

$$\begin{aligned}\mathcal{H}_d(X) :&= \sum_{B'\subset B, |B'|=d} \mathcal{R}(B\backslash B', A)\frac{\mathcal{R}(X,B')}{\mathcal{R}(B\backslash B', B')}\\ &= \sum_{B'\subset B, |B'|=d} \left(\prod_{\beta\in B\backslash B'} f(\beta)\right)\frac{\mathcal{R}(X,B')}{\mathcal{R}(B\backslash B', B')}.\end{aligned}$$

Como vimos en la Observación 3.1.2, $\mathcal{H}_d(X) \in S_{(n-d,d)}$ es el único polinomio de $S_{(n-d,d)}$ que satisface las $\binom{n}{d}$ condiciones

$$\mathcal{H}_d(B\backslash B') = \mathcal{R}(B\backslash B', A) \text{ para todo } B'\subset B, |B'| = d.$$

Y en particular,

$$\mathcal{H}_d(X) = f(x_1)\cdots f(x_{n-d}), \quad \text{si } m \le d. \tag{5.9}$$

Supongamos que no tenemos la hipótesis $m \le d$. Si bien no es cierto que $\mathcal{H}_d(X) = f(x_1)\cdots f(x_{n-d})$, ambos polinomios interpolan lo mismo en $B\backslash B'$, para todo B'. Es decir, dichos polinomios difieren en un polinomio que se anula en cada $B\backslash B'$. Esto nos motiva a considerar el ideal que forman tales polinomios. Consideramos el conjunto

$$\mathcal{L}_d(B) := \left\{\left(\beta_{i_1}, \ldots, \beta_{i_{n-d}}\right) : 1 \le i_k \ne i_l \le n\right\},$$

y el ideal $I(\mathcal{L}_d(B))$ de los polinomios que se anulan en $\mathcal{L}_d(B)$. Así, en el caso general, los polinomios de (5.9) diferirán en un elemento de $I(\mathcal{L}_d(B))$. De este modo, conocer este ideal puede brindarnos información del polinomio $\mathcal{H}_d$. Precisamente puede verse que $\mathcal{H}_d$ resulta ser la reducción, módulo cierta base de Gröbner de $I(\mathcal{L}_d(B))$, del polinomio $f(x_1)\cdots f(x_{n-d})$. Estas observaciones nos fueron comunicadas por Agnes Szanto.

En esta sección vamos a trabajar con dicha base de Gröbner obteniendo reescrituras de los polinomios que la componen. Escribamos $g = x^n + b_{n-1}x^{n-1} + \cdots + b_0$. Para

$i = 1, \ldots, n-d$ y $j \geq 0$ recordemos la definición de los *polinomios simétricos homogéneos completos*:

$$h_j^{(i)} := \sum_{|\mathbf{k}|=j} x_1^{k_1} \cdots x_i^{k_i},$$

donde la suma es sobre todos los $\mathbf{k} = (k_1, \ldots, k_i)$ tales que $|\mathbf{k}| := k_1 + \cdots + k_i = j$. Es decir, la suma de todos los monomios de grado total j en $(x_1, \ldots, x_i)$. Si $i = n-d$ notamos simplemente $h_j := h_j^{(n-d)}$.
La siguiente proposición se puede encontrar, por ejemplo, en [CLO2007, Ch. 7, Prop. 5].

Proposición 5.3.1. *El conjunto*

$$\begin{aligned} G_d(g) \;:=\; \Big\{ & p_1(x_1) := g(x_1) = h_n^{(1)} + b_{n-1} h_{n-1}^{(1)} + \cdots + b_1 h_1^{(1)} + b_0, \\ & p_2(x_1, x_2) := h_{n-1}^{(2)} + b_{n-1} h_{n-2}^{(2)} + \cdots + b_2 h_1^{(2)} + b_1, \ldots, \\ & p_{n-d}(x_1, \ldots, x_{n-d}) := h_{d+1}^{(n-d)} + b_{n-1} h_d^{(n-d)} + \cdots + b_{d+1} \Big\}, \end{aligned}$$

es una base de Gröbner de $I(\mathcal{L}_d(B))$ con respecto al orden lexicográfico $\prec$ de $K[X]$ con $x_1 < x_2 < \cdots < x_{n-d}$.

Aplicando el lema de intercambio obtendremos reescrituras muy cómodas de los polinomios de la base $G_d(g)$ de la Proposición 5.3.1. Para ello usaremos la siguiente recurrencia que satisfacen dichos polinomios, que puede verificarse fácilmente por inducción:

$$p_i(x_1, \ldots, x_i) = \frac{p_{i-1}(x_1, \ldots, x_{i-1}) - p_{i-1}(x_i, x_2, \ldots, x_{i-1})}{x_1 - x_i}, \tag{5.10}$$

para $2 \leq i \leq n-d$. Observemos que en particular

$$p_2(x_1, x_2) = \frac{g(x_1) - g(x_2)}{x_1 - x_2},$$

que es un cociente incremental de g y que coincide con el polinomio $\Phi(x_1, x_2)$ de la Definición 5.2.2 con $f = g$ y $g = 1$. En el siguiente lema reescribimos los polinomios p_i en términos del conjunto B.

Lema 5.3.2. *Sea $p_i(x_1, \ldots, x_i)$ el i-ésimo polinomio de la base $G_d(g)$ de la Proposición 5.3.1, con $1 \leq i \leq n-d$. Entonces*

$$p_i(x_1, \ldots, x_i) = \sum_{B' \subset B,\, |B'|=i-1} \frac{\mathcal{R}(\{x_1, \ldots, x_i\}, B \backslash B')}{\mathcal{R}(B', B \backslash B')} = \sum_{1 \leq j \leq i} \frac{g(x_j)}{\prod_{k \neq j}(x_j - x_k)}.$$

Demostración. Probamos primero la primera igualdad por inducción. Si $i = 1$ es obvio por definición. Supongamos que $2 \leq i \leq n-d$. Por la igualdad (5.10) se tiene

$$\begin{aligned} p_i(x_1, \ldots, x_i) &= \frac{p_{i-1}(x_1, \ldots, x_{i-1}) - p_{i-1}(x_i, x_2, \ldots, x_{i-1})}{x_1 - x_i} \\ &= \frac{1}{x_1 - x_i} \left(\sum_{\substack{B' \subset B \\ |B'|=i-2}} \frac{\mathcal{R}(\{x_1, \ldots, x_{i-1}\}, B \backslash B')}{\mathcal{R}(B', B \backslash B')} - \sum_{\substack{B' \subset B \\ |B'|=i-2}} \frac{\mathcal{R}(\{x_i, x_2, \ldots, x_{i-2}\}, B \backslash B')}{\mathcal{R}(B', B \backslash B')} \right) \qquad (5.11) \\ &= \sum_{B' \subset B,\, |B'|=i-2} \frac{\mathcal{R}(\{x_2, \ldots, x_{i-1}\}, B \backslash B')}{\mathcal{R}(B', B \backslash B')} \left(\frac{\mathcal{R}(x_1, B \backslash B') - \mathcal{R}(x_i, B \backslash B')}{x_1 - x_i} \right), \end{aligned}$$

usando la hipótesis inductiva en (5.11). Ahora, dado B' fijo, llamemos $h(x) = \mathcal{R}(x, B\backslash B')$. Entonces

$$\frac{\mathcal{R}(x_1, B\backslash B') - \mathcal{R}(x_i, B\backslash B')}{x_1 - x_i} = \frac{h(x_1) - h(x_i)}{x_1 - x_i} = \sum_{\beta \in B\backslash B'} \frac{\mathcal{R}(\{x_1, x_i\}, (B\backslash B')\backslash\beta)}{\mathcal{R}(\beta, (B\backslash B')\backslash\beta)},$$

por el Lema 5.2.8. Llamando $B'' = B' \cup \{\beta\}$ podemos reescribir toda la expresión como

$$\sum_{B''\subset B,\, |B''|=i-1} \frac{\mathcal{R}(\{x_1, \ldots, x_i\}, B\backslash B'')}{\mathcal{R}(B'', B\backslash B'')} \sum_{\beta \in B''} \frac{\mathcal{R}(\{x_2, \ldots, x_{i-1}\}, \beta)}{\mathcal{R}(B''\backslash\beta, \beta)}.$$

Pero

$$\sum_{\beta \in B''} \frac{\mathcal{R}(\{x_2, \ldots, x_{i-1}\}, \beta)}{\mathcal{R}(B''\backslash\beta, \beta)} = 1,$$

por la Proposición 2.1.4, dado que es el único polinomio $H \in S_{(i-2,1)}$ que satisface las $i-1$ condiciones $H(B''\backslash\beta) = 1$, para todo $\beta \in B''$. Esto prueba la primera igualdad del enunciado. Ahora veremos que la segunda expresión coincide con la tercera:

$$\begin{aligned}
\sum_{B'\subset B, |B'|=i-1} \frac{\mathcal{R}(\{x_1, \ldots, x_i\}, B\backslash B')}{\mathcal{R}(B', B\backslash B')} &= (-1)^{n-i+1} \sum_{B'\subset B, |B'|=i-1} \frac{\mathcal{R}(B\backslash B', \{x_1, \ldots, x_i\})}{\mathcal{R}(B\backslash B', B')} \\
&= (-1)^{n-i+1} \sum_{\substack{X'\cup X''=\{x_1,\ldots,x_i\} \\ |X'|=i-1,\, |X''|=1}} \frac{\mathcal{R}(B, X'')}{\mathcal{R}(X', X'')} \qquad (5.12) \\
&= \sum_{1\le j\le i} \frac{g(x_j)}{\prod_{k\neq j}(x_j - x_k)},
\end{aligned}$$

usando en (5.12) el Teorema 2.2.2 con $A = B$, $B = \{x_1, \ldots, x_i\}$ y $X = \emptyset$. □

Con esta reescritura es sencillo ver que efectivamente $G_d(g)$ es una base de Gröbner, lo que prueba la Proposición 5.3.1. De hecho, es inmediato verificar que los polinomios p_i se anulan en los puntos de $\mathcal{L}_d(B)$, lo cual no es evidente a partir de su definición inicial. Por otro lado, si llamamos $F(x) = (x - x_1)\cdots(x - x_i)$ y $A = \{x_1, \ldots, x_i\}$, observamos que p_i resulta ser el coeficiente principal de $\mathrm{Syl}_{0,i-1}(A, B)(x) = \mathrm{Sres}_{i-1}(F, g)(x)$. Esto es, $p_i = \mathrm{PSres}_{i-1}(F, g)(x)$.

Finalmente, daremos ahora otra reescritura más de los polinomios p_i. En el Lema 5.3.2 los escribimos en términos del conjunto B, que son las raíces de g. Ahora utilizaremos una vez más la Observación 2.2.7 para obtener una escritura que se aplique incluso al caso que B sea un multiconjunto.

Lema 5.3.3. *Sea $p_i(x_1, \ldots, x_i)$ el i-ésimo polinomio de la base $G_d(g)$ de la Proposición 5.3.1, con $1 \le i \le n - d$. Si E es un conjunto tal que $|E| \ge n + 1$ entonces*

$$p_i(x_1, \ldots, x_i) = \sum_{\substack{E_1\cup E_2\cup E_3=E \\ |E_1|=n-i+1, |E_2|=i-1, |E_3|=|E|-n}} \frac{\mathcal{R}(E_3, B)\mathcal{R}(\{x_1, \ldots, x_i\}, E_2)}{\mathcal{R}(E_3, E_1)\mathcal{R}(E_3, E_2)\mathcal{R}(E_1, E_2)}.$$

En particular, si $|E| = n + 1$,

$$p_i(x_1, \ldots, x_i) = \sum_{\substack{E_1 \cup E_2 \cup \{\gamma\} = E \\ |E_1| = n-i+1, |E_2| = i-1}} \frac{g(\gamma)\mathcal{R}(\{x_1, \ldots, x_i\}, E_2)}{\mathcal{R}(\{\gamma\}, E_1)\mathcal{R}(\{\gamma\}, E_2)\mathcal{R}(E_1, E_2)}.$$

Demostración. Es resultado de aplicar la Observación 2.2.7 (2) para $Y = \{x_1, \ldots, x_i\}$, $X = \emptyset$, $p = i - 1$ y $q = n - i + 1$. En efecto, $|E| \geq n + 1 \geq \text{máx}\{i - 1, n + 1, n\} = \text{máx}\{|X| + p, |Y| + q, |B|\}$. □

Esta fórmula permite escribir a los polinomios p_i en función de los valores que interpola g en los puntos de E. Y tomando $|E| = n + 1$, su tamaño es óptimo para identificar unívocamente a g vía interpolación.

5.4. Fracciones simples

Veremos aquí cómo se puede interpretar la construcción de la escritura en fracciones simples, en el caso raíces simples, de un modo natural y sencillo gracias a la interpolación simétrica. Además lo extendemos a mayor cantidad de variables.

Proposición 5.4.1. *Sean* K *un cuerpo y* f *un polinomio en* $K[x]$ *con* $\deg(f) = m$ *y con raíces simples. Sean* $X = (x_1, \ldots, x_r)$ *un conjunto de variables y* G *un polinomio de* $K[X]$ *simétrico, con grado en cada variable acotado por* n *(es decir,* $G \in S_{(r,n)}$*) y tal que* $m \geq r + n$. *Sea* A *el conjunto de raíces de* f. *Entonces*

$$\frac{G(X)}{f(x_1) \cdots f(x_r)} = \frac{1}{a_m^r} \sum_{\substack{A' \subset A \\ |A'| = r}} \frac{\left(\frac{G(A')}{\mathcal{R}(A', A \setminus A')}\right)}{\mathcal{R}(X, A')},$$

donde a_m *es el coeficiente principal de* f.

Demostración. Por el Lema 2.2.8 tenemos que

$$G(X) = \sum_{\substack{A_1 \cup A_2 = A \\ |A_1| = m-r, |A_2| = r}} \frac{G(A_2)\mathcal{R}(X, A_1)}{\mathcal{R}(A_2, A_1)}.$$

Dividiendo a ambos lados por $\mathcal{R}(X, A)$, resulta

$$\frac{G(X)}{\mathcal{R}(X, A)} = \sum_{\substack{A_1 \cup A_2 = A \\ |A_1| = m-r, |A_2| = r}} \frac{G(A_2)}{\mathcal{R}(A_2, A_1)\mathcal{R}(X, A_2)}.$$

Pero notemos que $f(x_1) \cdots f(x_r) = a_m^r \mathcal{R}(X, A)$. De modo que multiplicando a ambos lados de la igualdad por $\frac{1}{a_m^r}$ y llamando $A' = A_2$ terminamos la demostración. □

Observemos que el caso $r = 1$ es la escritura usual en fracciones simples de un cociente de dos polinomios univariados:

$$\frac{g(x)}{f(x)} = \sum_{\alpha \in A} \frac{\left(\frac{g(\alpha)}{f'(\alpha)}\right)}{x - \alpha}.$$

Para esto basta observar que $f'(\alpha) = a_m \mathcal{R}(\alpha, A \backslash \alpha)$, para cada $\alpha \in A$, como vimos en (5.6).

Capítulo 6

Subresultantes de $(x-\alpha)^m$ y $(x-\beta)^n$

Este capítulo, totalmente independiente de los anteriores, se concentra en el estudio de las subresultantes para un caso estructurado: $f=(x-\alpha)^m$ y $g=(x-\beta)^n$, con α y β elementos de un cuerpo K. Es decir, f y g tienen una única raíz (múltiple) cada uno.

Si $\alpha=\beta$, las subresultantes son todas nulas, de modo que asumiremos que $\alpha\neq\beta$ y describiremos primero, para $0\leq d<\text{mín}\{m,n\}$, $\text{Sres}_d(f,g)(x)$ en la *base de Bernstein* $\{(x-\alpha)^j(x-\beta)^{d-j}, 0\leq j\leq d\}$ de polinomios de grado menor o igual que d. Para esta construcción usaremos determinantes de *matrices de Hankel*. Posteriormente mostraremos que, de hecho, las subresultantes en este caso son múltiplos escalares, salvo un cambio de variables afín, de *polinomios de Jacobi*, que son una conocida familia de polinomios ortogonales. Y como consecuencia de esto concluiremos un resultado que tiene que ver con la complejidad para calcularla. Esto fue posible luego de un proceso computacional de predicción y prueba, en el que usamos el paquete de Maple ([Map2016]) para sumas hipergeométricas y para el algoritmo de Zeilberger ([Zei1990]).

En la Sección 6.1 presentamos los preliminares con unas identidades conocidas que usaremos después. La Sección 6.2 desarrolla la construcción de la fórmula en la base de Bernstein. Los resultados de dicha sección se encuentran en el trabajo publicado [BDKSV2017], realizado junto con Alin Bostan, Carlos D'Andrea, Teresa Krick y Agnes Szanto. En la Sección 6.3 mostramos la conexión con los polinomios de Jacobi y trabajamos con la complejidad. Los resultados de esta sección son parte de un trabajo en preparación junto con Alin Bostan, Teresa Krick y Agnes Szanto.

6.1. Preliminares

En esta sección introducimos los conceptos y las identidades que necesitamos para construir nuestras fórmulas. Introducimos primero la siguiente notación.

Notación 6.1.1. Sea x una variable indeterminada sobre $\mathbb{Q}$ y sea $j\in\mathbb{N}$. Definimos el j-ésimo *símbolo de Pochhammer* de x como

$$(x)_j := x(x+1)\cdots(x+j-1),$$

y definimos además $(x)_0 := 1$.

El siguiente lema es una fórmula de Ostrowski para el determinante de una matriz particular con coeficientes binomiales.

Lema 6.1.2 ([Ost1964])**.** *Sean $\ell, k \in \mathbb{N}$ y $a_0, a_1, \ldots, a_k \in \mathbb{N}$, con $a_i \geq k$ para $0 \leq i \leq k$. Entonces*

$$\det\left(\binom{\ell}{a_i - j}\right)_{0\leq i,j\leq k} = \ell!^{k+1} \frac{\prod_{i=1}^{k}(\ell+i)^{k+1-i}\prod_{0\leq i<i'\leq k}(a_{i'}-a_i)}{\prod_{i=0}^{k} a_i! \prod_{i=0}^{k}(\ell+k-a_i)!}.$$

La demostración que presentamos aquí del Lema 6.1.2 nos fue comunicada en abril de 2017 por Alin Bostan. Es consecuencia de la siguiente proposición cuya prueba, debida a Alin Bostan, difiere de las pruebas que se encuentran en la literatura.

Proposición 6.1.3. *([Kra1990, Lemma 2.2].) Sean $x_0, \ldots, x_k$ indeterminadas sobre un cuerpo K y $b_1, \ldots, b_k, c_1, \ldots, c_k \in K$. Sea $A \in K[x_0, \ldots, x_k]^{(k+1)\times(k+1)}$ definida por*

$$\begin{aligned} A &= \Big((x_i+b_k)(x_i+b_{k-1})\cdots(x_i+b_{j+1})(x_i+c_j)(x_i+c_{j-1})\cdots(x_i+c_1)\Big)_{0\leq i,j\leq k} \\ &= \begin{pmatrix} (x_0+b_k)\cdots(x_0+b_1) & (x_0+b_k)\cdots(x_0+b_2)(x_0+c_1) & \ldots & (x_0+c_k)\cdots(x_0+c_1) \\ (x_1+b_k)\cdots(x_1+b_1) & (x_1+b_k)\cdots(x_1+b_2)(x_1+c_1) & \ldots & (x_1+c_k)\cdots(x_1+c_1) \\ \vdots & \vdots & & \vdots \\ (x_k+b_k)\cdots(x_k+b_1) & (x_k+b_k)\cdots(x_k+b_2)(x_k+c_1) & \ldots & (x_k+c_k)\cdots(x_k+c_1) \end{pmatrix}. \end{aligned}$$

Entonces

$$\det(A) = \prod_{0\leq i<j\leq k}(x_i - x_j) \prod_{1\leq i\leq j\leq k}(c_i - b_j).$$

Antes de dar la demostración de la Proposición 6.1.3, veremos cómo podemos deducir a partir de ésta el Lema 6.1.2.

Demostración del Lema 6.1.2. Observemos que para $0 \leq i, j \leq k$, el coeficiente (i, j) de la matriz del enunciado puede escribirse como

$$\begin{aligned} \binom{\ell}{a_i - j} &= \frac{\ell!}{a_i!(\ell - a_i + k)!} a_i \cdots (a_i - j + 1)(\ell - a_i + k)\cdots(\ell - a_i + j + 1) \\ &= (-1)^{k-j}\frac{\ell!}{a_i!(\ell - a_i + k)!}(a_i - j + 1)_j (a_i - \ell - k)_{k-j}. \end{aligned}$$

Esto implica

$$\det\left(\binom{\ell}{a_i - j}\right)_{0\leq i,j\leq k} = (-1)^{\binom{k+1}{2}} \frac{\ell!^{k+1}}{\prod_{i=0}^{k}\big(a_i!(\ell - a_i + k)!\big)} \det(A),$$

para

$$A = \big((a_i - \ell - k)\cdots(a_i - \ell - j - 1)\cdot a_i \cdots (a_i - j + 1)\big)_{0\leq i,j\leq k}.$$

Notemos que la matriz A coincide con la matriz de la Proposición 6.1.3 para $x_i = a_i$, con $0 \leq i \leq k$, y $b_i = -\ell - i$, $c_i = -i + 1$, con $1 \leq i \leq k$. Luego

$$\begin{aligned}\det(A) &= \prod_{0\leq i<i'\leq k} (a_i - a_{i'}) \prod_{1\leq i\leq j\leq k} (-i+1-(-\ell-j)) \\ &= (-1)^{\binom{k+1}{2}} \prod_{0\leq i<i'\leq k} (a_{i'} - a_i) \prod_{1\leq i\leq j\leq k} (\ell + (j-i) + 1) \\ &= (-1)^{\binom{k+1}{2}} \prod_{0\leq i<i'\leq k} (a_{i'} - a_i) \prod_{1\leq i\leq k} (\ell+i)^{k+1-i}.\end{aligned}$$

Esto concluye la demostración. □

Ahora probamos la Proposición 6.1.3.

Demostración de la Proposición 6.1.3. Como en la demostración del Lema 2.1.3, consideremos, para $0 \leq \ell \leq k$,

$$e_\ell^{(k)}(y_1, \ldots, y_k) = \sum_{1\leq i_1<i_2<\cdots<i_\ell\leq k} y_{i_1} \cdots y_{i_\ell},$$

el ℓ-ésimo polinomio simétrico elemental en k variables $y_1, \ldots, y_k$, con $e_0^{(k)}(y_1, \ldots, y_k) = 1$. (El supraíndice denota aquí el número de variables.) Así, para $0 \leq i, j \leq k$, el coeficiente (i, j) de la matriz A es igual a

$$A_{ij} = \sum_{\ell=0}^{k} e_{k-\ell}^{(k)}(b_k, \ldots, b_{j+1}, c_j, \ldots, c_1) x^\ell.$$

Luego A puede escribirse como el producto entre una matriz de Vandermonde transpuesta y una matriz cuyos coeficientes son polinomios simétricos elementales:

$$A = \mathcal{V} \cdot E$$

con

$$\mathcal{V} = \begin{pmatrix} x_0^k & \ldots & x_0 & 1 \\ \vdots & & \vdots & \vdots \\ x_k^k & \ldots & x_k & 1 \end{pmatrix}$$

y

$$E = \begin{pmatrix} e_0^{(k)}(b_k, \ldots, b_1) & \ldots & e_0^{(k)}(b_k, c_{k-1}, \ldots, c_1) & e_0^{(k)}(c_k, \ldots, c_1) \\ \vdots & & \vdots & \vdots \\ e_k^{(k)}(b_k, \ldots, b_1) & \ldots & e_k^{(k)}(b_k, c_{k-1}, \ldots, c_1) & e_k^{(k)}(c_k, \ldots, c_1) \end{pmatrix}.$$

Entonces tenemos $\det(A) = \det(\mathcal{V}) \det(E)$, con $\det(\mathcal{V}) = \prod_{0\leq i<j\leq k}(x_i - x_j)$, de modo que sólo basta calcular $\det(E)$. Lo haremos por inducción en el tamaño de E. Notemos que para $0 \leq \ell \leq k$ y $1 \leq j \leq k$ se tiene

$$\begin{aligned}&e_\ell^{(k)}(b_k, \ldots, b_{j+1}, c_j, \ldots, c_1) - e_\ell^{(k)}(b_k, \ldots, b_j, c_{j-1}, \ldots, c_1) \\ &\qquad = (c_j - b_j) e_{\ell-1}^{(k-1)}(b_k, \ldots, b_{j+1}, c_{j-1}, \ldots, c_1),\end{aligned}$$

con la convención de que $e_{-1}^{(k-1)}(y_1,\ldots,y_{k-1}) = 0$, y luego, restando la columna j a la columna $j+1$ de E, para $j = k,\ldots,0$, tenemos

$$\begin{aligned}&\det(E)\\ &= \prod_{1\le i\le n}(c_i - b_i)\det\begin{pmatrix} e_0^{(k-1)}(b_k,\ldots,b_2) & \ldots & e_0^{(k-1)}(b_k,c_{k-2},\ldots,c_1) & e_0^{(k-1)}(c_{k-1},\ldots,c_1)\\ \vdots & & \vdots & \vdots\\ e_{k-1}^{(k-1)}(b_k,\ldots,b_2) & \ldots & e_{k-1}^{(k-1)}(b_k,c_{k-2},\ldots,c_1) & e_{k-1}^{(k-1)}(c_{k-1},\ldots,c_1)\end{pmatrix}.\end{aligned}$$

Por hipótesis inductiva este último determinante es igual a

$$\prod_{1\le i<j\le k}(c_i - b_j).$$

Esta última igualdad puede verse haciendo el cambio $d_j := b_{j+1}$ para $1 \le j \le k-1$, con lo cual el último determinante resulta $\prod_{1\le i\le j\le k-1}(c_i - d_j)$. □

Usaremos también en la Sección 6.2 el siguiente lema, que es una identidad de Pfaff-Saalschütz para funciones hipergeométricas.

Lema 6.1.4. *([Pfa1797], [Saa1890], [And1996], [And1997], [Sla1966, §2.3.1]) Sean x, y, z variables independientes sobre $\mathbb{Q}$. Para cada $k \in \mathbb{N}$, se tiene la siguiente igualdad en $\mathbb{Q}(x,y,z)$:*

$$\sum_{j=0}^{k}\frac{(x)_j(y)_j(-k)_j}{(z)_j(1+x+y-z-k)_j\,j!} = \frac{(z-x)_k(z-y)_k}{(z)_k(z-x-y)_k}.$$

Finalmente introducimos los polinomios de Jacobi. Para la siguiente definición necesitamos asumir que la característica no es 2.

Definición 6.1.5. Sea K un cuerpo (o un anillo) tal que $\mathrm{char}(K) \neq 2$ y sean $k, l, r \in \mathbb{Z}$, con $r > 0$. El polinomio de Jacobi $P_r^{(k,l)} \in K[x]$ se define equivalentemente como

- la fórmula de Rodrigues:

$$P_r^{(k,l)}(x) := \frac{(-1)^r}{2^r\,r!}(1-x)^{-k}(1+x)^{-l}\frac{\partial^r}{\partial x^r}\left[(1-x)^{k+r}(1+x)^{l+r}\right],$$

- o la suma hipergeométrica:

$$P_r^{(k,l)}(x) := \sum_{j=0}^{r}\frac{(k+r-j+1)_j}{j!}\frac{(l+j+1)_{r-j}}{(r-j)!}\left(\frac{x-1}{2}\right)^{r-j}\left(\frac{x+1}{2}\right)^{j}.$$

En efecto la definición tiene sentido si $\mathrm{char}(K) \neq 2$ ya que es fácil ver que en los coeficientes

$$\frac{(k+r-j+1)_j}{j!}\frac{(l+j+1)_{r-j}}{(r-j)!},$$

de la suma hipergeométrica no aparecen denominadores. De hecho, para $a, j \in \mathbb{Z}$, con $j \geq 0$ se tiene

$$\frac{(a)_j}{j!} = \begin{cases} \binom{a+j-1}{j} & \text{si } a \geq 0 \\ (-1)^j \binom{-a}{j} & \text{si } a < 0 \text{ y } a+j-1 < 0 \\ 0 & \text{en otro caso .} \end{cases} \tag{6.1}$$

También es sencillo ver la equivalencia de las definiciones desarrollando las derivadas en la fórmula de Rodrigues según la fórmula

$$\frac{\partial^r}{\partial x^r}[f(x)g(x)] = \sum_{j=0}^{r} \binom{r}{j} \frac{\partial^j f}{\partial x^j}(x) \cdot \frac{\partial^{r-i} g}{\partial x^{r-i}}(x).$$

6.2. Fórmula en raíces para este caso estructurado

Fijemos m y n, números naturales, y sea $0 \leq d < \text{mín}\{m, n\}$ o $d = \text{mín}\{m, n\}$ si $m \neq n$. Sea $c = c(m, n, d) := m+n-2d-1$. Introducimos la matriz de Hankel $H(m, n, d) \in \mathbb{Z}^{d \times (d+1)}$ definida por

$$\left(\binom{c}{m-i-j} \right)_{\substack{1 \leq i \leq d \\ 0 \leq j \leq d}} = \begin{pmatrix} \binom{c}{m-1} & \binom{c}{m-2} & \cdots & \cdots & \binom{c}{m-d-1} \\ \binom{c}{m-2} & & \ddots & \ddots & \binom{c}{m-d-2} \\ \vdots & \ddots & \ddots & & \vdots \\ \binom{c}{m-d} & \binom{c}{m-d-1} & \cdots & \cdots & \binom{c}{m-2d} \end{pmatrix}, \tag{6.2}$$

donde convenimos $\binom{c}{k} = 0$ si $k < 0$ o $k > c$.

Notemos $q_j(m, n, d)$ al j-ésimo menor de $H(m, n, d)$ definido por el determinante de la submatriz cuadrada $H_j(m, n, d)$ de $H(m, n, d)$ que resulta al quitar de esta última la columna j, para $0 \leq j \leq d$ (contamos las columnas desde 0). Por convención, $q_0(m, n, 0)$, el determinante de la matriz vacía, es 1. Dado que estos menores son números enteros, podemos verlos como elementos de cualquier cuerpo K bajo la identificación vía el morfismo de anillos de $\mathbb{Z}$ en K que manda el 1 en el elemento 1_K de K.

Podemos entonces enunciar el teorema principal de este sección. Vamos a escribir en este capítulo $\text{Sres}_d((x-\alpha)^m, (x-\beta)^n)$ en lugar de $\text{Sres}_d((x-\alpha)^m, (x-\beta)^n)(x)$ para no recargar la notación.

Teorema 6.2.1. *Sea K un cuerpo y sean $m, n, d \in \mathbb{N}$ con $0 \leq d < \text{mín}\{m, n\}$, y $\alpha, \beta \in K$, con $\alpha \neq \beta$. Entonces*

$$\text{Sres}_d((x-\alpha)^m, (x-\beta)^n) = (-1)^{\binom{d}{2}} (\alpha-\beta)^{(m-d)(n-d)} \sum_{j=0}^{d} q_j(m, n, d)(x-\alpha)^j (x-\beta)^{d-j}.$$

La igualdad vale trivialmente incluso si $\alpha = \beta$, pero el resultado sólo tiene interés cuando son distintos.

Más aún, daremos también expresiones explícitas para los valores de los menores $q_j(m, n, d)$ para $0 \leq j \leq d$, como productos de cocientes de factoriales.

Teorema 6.2.2. *Sean $m, n, d \in \mathbb{N}$ con $d < \min\{m, n\}$ y sea $c = m+n-2d-1$. Entonces*

$$q_0(m,n,d) = (-1)^{\binom{d}{2}} \prod_{i=1}^{d} \frac{(i-1)!\,(c+i-1)!}{(m-i-1)!(n-i)!},$$

y para $1 \le j \le d$, se tiene:

$$q_j(m,n,d) = \frac{\binom{d}{j}\binom{n-d+j-1}{j}}{\binom{m-1}{j}}\, q_0(m,n,d).$$

Probaremos primero el Teorema 6.2.2.

Demostración del Teorema 6.2.2. Probemos primero la expresión para $q_0(m,n,d)$. Aplicando el Lema 6.1.2 con $k = d-1$ y $a_i = m-i-2$ para $0 \le i \le d-1$, y $\ell = c$ tenemos

$$\begin{aligned} q_0(m,n,d) &= \det\left(\binom{c}{m-i-j}\right)_{1\le i,j\le d} = \det\left(\binom{c}{m-i-j-2}\right)_{0\le i,j\le d-1} \\ &= c!^d \frac{\prod_{i=1}^{d-1}(c+i)^{d-i}\prod_{0\le i<i'\le d-1}(i-i')}{\prod_{i=0}^{d-1}(m-i-2)!\prod_{i=0}^{d-1}(c+d-1-(m-i-2))!} \\ &= \frac{\prod_{i=1}^{d}\left(c!\prod_{j=1}^{i-1}(c+j)\right)\cdot(-1)^{\binom{d}{2}}\prod_{i=1}^{d}(i-1)!}{\prod_{i=1}^{d}(m-i-1)!\prod_{i=1}^{d}(n-d+i-1)!}. \end{aligned}$$

Sólo resta reescribir los factores de manera adecuada.

Probemos ahora la expresión para $q_j(m,n,d)$ con $1 \le j \le d$. Observemos que la matriz H tiene rango máximo d, pues el menor $q_0(m,n,d)$ es no nulo, como acabamos de ver. Un argumento elemental de álgebra lineal muestra que el núcleo de la transformación lineal inducida $H\colon \mathbb{Q}^{d+1} \to \mathbb{Q}^d$ tiene dimensión 1 y está generado por el vector (no nulo)

$$\mathbf{q}(m,n,d) := (q_0(m,n,d), -q_1(m,n,d), \ldots, (-1)^d q_d(m,n,d)).$$

Sea $k_j(m,n,d) := \frac{\binom{d}{j}\binom{n-d+j-1}{j}}{\binom{m-1}{j}}$ para $0 \le j \le d$. Basta ver entonces que

$$\mathbf{k}(m,n,d) := (k_0(m,n,d), -k_1(m,n,d), \ldots, (-1)^d k_d(m,n,d)) \in \ker H, \tag{6.3}$$

pues en tal caso tendríamos $\mathbf{k}(m,n,d) = \lambda\,\mathbf{q}(m,n,d)$ con $\lambda = 1/q_0(m,n,d)$, siendo que $k_0(m,n,d) = 1$.

Luego, para probar (6.3) basta verificar las identidades

$$\sum_{j=0}^{d} \binom{m+n-2d-1}{m-j-i}(-1)^j k_j(m,n,d) = 0, \quad \text{para } 1 \le i \le d. \tag{6.4}$$

De hecho probaremos una identidad más general que vale para cualquier $i \in \mathbb{N}$:

$$\sum_{j=0}^{d} \binom{m+n-2d-1}{m-j-i}(-1)^j \frac{\binom{d}{j}\binom{n-d+j-1}{j}}{\binom{m-1}{j}} = \frac{\binom{i-1}{d}\binom{m+n-d-1}{m-i}}{\binom{m-1}{d}}, \tag{6.5}$$

Así, la identidad (6.4) se obtiene al especializar i en $1, \ldots, d$.

La identidad (6.5) será consecuencia del Lema 6.1.4. Dado que ambos miembros son polinomios en n (de grado menor o igual que $m-i$) basta probarlo para una cantidad infinita de valores de n. Lo haremos para todo $n \geq 2d$.

Observando que $(a+j-1)! = (a-1)!(a)_j$, $\binom{a+j-1}{j} = \frac{(a)_j}{j!}$, $(a-j)! = (-1)^j \frac{a!}{(-a)_j}$ y $\binom{a}{j} = (-1)^j \frac{(-a)_j}{j!}$, deducimos que el miembro izquierdo de (6.5) es igual, para $n \geq 2d$, a

$$\frac{(m+n-2d-1)!}{(m-i)!(n-2d+i-1)!} \sum_{j=0}^{d} \frac{(n-d)_j(-(m-i))_j(-d)_j}{(n-2d+i)_j(-(m-1))_j j!}.$$

Para simplificar esta suma aplicamos el Lema 6.1.4 con $k=d$ y con x, y, z especializados respectivamente en $n-d, -(m-i)$ y $n-2d+i$, y nos queda

$$\begin{aligned}\sum_{j=0}^{d} \frac{(n-d)_j(-(m-i))_j(-d)_j}{(n-2d+i)_j(-(m-1))_j\, j!} &= \frac{(i-d)_d(m+n-2d)_d}{(n-2d+i)_d(m-d)_d} \\ &= \frac{\binom{i-1}{d}(m+n-2d)\cdots(m+n-d-1)}{\binom{m-1}{d}(n-2d+i)\cdots(n-d+i-1)},\end{aligned}$$

de lo que (6.5) se deduce inmediatamente. □

Probaremos ahora el Teorema 6.2.1 siguiendo la siguiente técnica. Obtendremos una escritura de la forma $F \cdot (x-\alpha)^m + G \cdot (x-\beta)^n$, con grado menor o igual a d y con $\deg(F) < n-d$ y $\deg(G) < m-d$ y usaremos la Proposición 1.1.6. Para aplicar esta proposición necesitaremos además verificar que $\mathrm{PSres}_d(f,g)(x) \neq 0$. Definimos, para $0 \leq d < \min\{m,n\}$:

$$h_d(\alpha,\beta,m,n) := (\alpha-\beta)^c \Big(\sum_{j=0}^{d} q_j(m,n,d)(x-\alpha)^j(x-\beta)^{d-j} \Big), \tag{6.6}$$

donde $c = m+n-2d-1$ y los q_j son los de antes. Notemos que $h_d(\alpha,\beta,m,n) \in K[x]$ tiene grado menor o igual que d.

Proposición 6.2.3. *Sean $d, m, n \in \mathbb{N}$ con $0 \leq d < \min\{m,n\}$, y $\alpha, \beta \in K$, con $\alpha \neq \beta$. Existen $F, G \in K[x]$ con $\deg(F) < n-d$ y $\deg(G) < m-d$ tales que*

$$h_d(\alpha,\beta,m,n) = F \cdot (x-\alpha)^m + G \cdot (x-\beta)^n.$$

Demostración. Llamemos $f := (x-\alpha)^m$ y $g := (x-\beta)^n$ y escribamos

$$(\alpha-\beta)^c = (\alpha - x + x - \beta)^c = \sum_{k=0}^{c} (-1)^k \binom{c}{k} (x-\alpha)^k (x-\beta)^{c-k}.$$

Fijemos un $0 \leq j \leq d$. Tenemos

$$(\alpha-\beta)^c (x-\alpha)^j (x-\beta)^{d-j} = \sum_{k=0}^{c} (-1)^k \binom{c}{k} (x-\alpha)^{k+j} (x-\beta)^{c-k+d-j}.$$

Para $k+j \geq m$ los términos correspondientes en el miembro derecho son polinomios múltiplos de f, con coeficientes F_j de grado menor o igual que $(k+j)+(c-k+d-j)-m = n-d-1$. De modo similar, para $c-k+d-j \geq n$, los términos correspondientes son múltiplos de g, con coeficientes G_j de grado menor o igual que $(k+j)+(c-k+d-j)-n = m-d-1$. Los términos restantes satisfacen $k+j < m$, i.e. $k < m-j$ y $c-k+d-j < n$, i.e. $k > m-j-d-1$.

Por lo tanto

$$\begin{aligned}
&(\alpha-\beta)^c(x-\alpha)^j(x-\beta)^{d-j} \\
&\qquad = F_j\, f + G_j\, g + \sum_{k=m-j-d}^{m-j-1} (-1)^k \binom{c}{k} (x-\alpha)^{k+j}(x-\beta)^{c-k+d-j} \\
&\qquad = F_j\, f + G_j\, g + \sum_{i=1}^{d} (-1)^{m-i-j} \binom{c}{m-i-j} (x-\alpha)^{m-i}(x-\beta)^{n-d+i-1}.
\end{aligned}$$

Multiplicando cada una de estas ecuaciones por $q_j(m,n,d)$ para $0 \leq j \leq d$ y sumándolas, obtenemos

$$\begin{aligned}
h_d(\alpha,\beta,m,n) &= (\alpha-\beta)^c \Big(\sum_{j=0}^{d} q_j(m,n,d)(x-\alpha)^j(x-\beta)^{d-j} \Big) \\
&= F\, f + G\, g \\
&\qquad + \sum_{j=0}^{d} \Big(\sum_{i=1}^{d} (-1)^{m-i-j} \binom{c}{m-i-j} q_j(m,n,d)(x-\alpha)^{m-i}(x-\beta)^{n-d+i-1} \Big),
\end{aligned}$$

con $F := \sum_{j=0}^{d} q_j(m,n,d)F_j$ y $G := \sum_{j=0}^{d} q_j(m,n,d)G_j$. Pero resulta que

$$\begin{aligned}
&\sum_{j=0}^{d} \Big(\sum_{i=1}^{d} (-1)^{m-i-j} \binom{c}{m-i-j} q_j(m,n,d)\,(x-\alpha)^{m-i}(x-\beta)^{n-d+i-1} \Big) \\
&= \sum_{i=1}^{d} (-1)^{m-i}(x-\alpha)^{m-i}(x-\beta)^{n-d+i-1} \left(\sum_{j=0}^{d} (-1)^j \binom{c}{m-i-j} q_j(m,n,d) \right) \\
&= 0,
\end{aligned}$$

dado que, como observamos en la demostración del Teorema 6.2.2,

$$(q_0(m,n,d), -q_1(m,n,d), \ldots, (-1)^d q_d(m,n,d)),$$

genera $\ker H$. Luego $h_d(\alpha,\beta,m,n) = F \cdot (x-\alpha)^m + G \cdot (x-\beta)^n$ con $\deg(F) < n-d$ y $\deg(G) < m-d$. □

Para poder usar la Proposición 1.1.6 veamos que efectivamente $\mathrm{PSres}_d(f,g)(x) \neq 0$. Usaremos para ello el siguiente sencillo resultado.

Lema 6.2.4. *[ApJo2006, Prop. 8.6(i)] Sean $f, g \in K[x]$. Para cada $\alpha \in K$ se tiene*

$$\mathrm{Sres}_d(f,g)(x+\alpha) = \mathrm{Sres}_d(f(x+\alpha), g(x+\alpha))(x).$$

Proposición 6.2.5. *Sean $d, m, n \in \mathbb{N}$ con $d < \min\{m,n\}$. Sean $\alpha, \beta \in K$, con $\alpha \neq \beta$, y sea $c = m+n-2d-1$. Entonces*

$$\begin{aligned}\mathrm{PSres}_d((x-\alpha)^m,(x-\beta)^n) &= (\alpha-\beta)^{(m-d)(n-d)} \prod_{i=1}^{d} \frac{(i-1)!\,(c+i)!}{(m-i)!(n-i)!} \\ &= (-1)^{\binom{d}{2}} (\alpha-\beta)^{(m-d)(n-d)} \frac{\binom{m+n-d-1}{d}}{\binom{m-1}{d}} q_0(m,n,d).\end{aligned}$$

En particular, como $\alpha \neq \beta$, si $\mathrm{char}(K) = 0$ o $\mathrm{char}(K) \geq m+n-2d$:

$$\mathrm{PSres}_d((x-\alpha)^m,(x-\beta)^n) \neq 0.$$

Demostración. Probemos la primera igualdad:

$$\begin{aligned}\mathrm{PSres}_d((x-\alpha)^m,(x-\beta)^n) &= \mathrm{PSres}_d(x^m,(x+\alpha-\beta)^n) \\ &= \mathrm{PSres}_d(x^m, \sum_{j=0}^{n} \binom{n}{j} (\alpha-\beta)^{n-j} x^j).\end{aligned}$$

Luego

$$\mathrm{PSres}_d((x-\alpha)^m,(x-\beta)^n)$$

$$= \det \begin{array}{|cccccc|}\multicolumn{6}{c}{\overbrace{}^{m+n-2d}} \\ \hline 1 & \cdots & & 0 & \cdots & 0 \\ & \ddots & & \vdots & & \vdots \\ & & 1 & 0 & \cdots & 0 \\ \hline 1 & \cdots & & \binom{n}{d}(\alpha-\beta)^{n-d} & \cdots & \binom{n}{m-1}(\alpha-\beta)^{n-(m-1)} \\ & \ddots & & \vdots & & \vdots \\ & & 1 & \binom{n}{2d-m+1}(\alpha-\beta)^{n-(2d-m+1)} & \cdots & \binom{n}{d}(\alpha-\beta)^{n-d} \\ \hline \end{array} \begin{array}{l} \\ \\ n-d \\ \\ \\ m-d \end{array}$$

$$= \det \begin{array}{|ccc|}\multicolumn{3}{c}{\overbrace{\phantom{\binom{n}{d}(\alpha-\beta)^{n-d}\ \cdots\ \binom{n}{m-1}(\alpha-\beta)^{n-(m-1)}}}^{m-d}} \\ \hline \binom{n}{d}(\alpha-\beta)^{n-d} & \cdots & \binom{n}{m-1}(\alpha-\beta)^{n-(m-1)} \\ \binom{n}{d-1}(\alpha-\beta)^{n-(d-1)} & \cdots & \binom{n}{m-2}(\alpha-\beta)^{n-(m-2)} \\ \vdots & & \vdots \\ \binom{n}{2d-m+1}(\alpha-\beta)^{n-(2d-m+1)} & \cdots & \binom{n}{d}(\alpha-\beta)^{n-d} \\ \hline \end{array} \begin{array}{l} \\ \\ \\ \\ m-d \end{array}$$

$$= (\alpha-\beta)^{(m-d)(n-d)} \det\left(\binom{n}{d-i+j}\right)_{1\leq i,j\leq m-d} \tag{6.7}$$

$$= (\alpha-\beta)^{(m-d)(n-d)} \prod_{i=1}^{d} \frac{(i-1)!\,(c+i)!}{(m-i)!(n-i)!}. \tag{6.8}$$

En efecto, para verificar (6.7), multiplicamos la i-ésima fila de la segunda matriz por $(\alpha-\beta)^{i-1}$, $1 \leq i \leq m-d$. Así, el determinante queda multiplicado por $(\alpha-\beta)^{1+\cdots+(m-d-1)} = (\alpha-\beta)^{\binom{m-d}{2}}$. Pero ahora, para cada $j = 1, \ldots, m-d$, la columna j contiene el mismo factor $(\alpha-\beta)^{n-d+j-1}$ que puede sacarse como factor común obteniendo $(\alpha-\beta)^{(n-d+m-d-1)+\cdots+(n-d+0)} = (\alpha-\beta)^{(m-d)(n-d)+\binom{m-d}{2}}$ y de este modo podemos simplificar $(\alpha-\beta)^{\binom{m-d}{2}}$. La igualdad (6.8) es aplicar el Lema 6.1.2 con $\ell = n$, $k = m-d-1$ y $a_j = d+j+1$ para $0 \leq i \leq m-d-1$.

La segunda igualdad de la proposición se deduce directamente de la expresión para $q_0(m,n,d)$ del Teorema 6.2.2. □

Corolario 6.2.6. *Si* $\operatorname{char}(K) = 0$ *o* $\operatorname{char}(K) \geq m+n-2d$, *existe* $\lambda \in K\backslash\{0\}$ *tal que*

$$h_d(\alpha,\beta,m,n) = \lambda \operatorname{Sres}_d((x-\alpha)^m, (x-\beta)^n).$$

Demostración. Es consecuencia inmediata de las Proposiciones 6.2.3 y 6.2.5 y de la Proposición 1.1.6. □

Si bien tuvimos que imponer una condición sobre la característica de K, luego veremos que podremos probar el Teorema 6.2.1 en el caso general.

Falta entonces que calculemos el coeficiente λ del Corolario 6.2.6. Para eso compararemos los coeficientes principales de los polinomios de ambos miembros de la igualdad de dicho corolario. El del miembro derecho ya lo calculamos en la Proposición 6.2.5. Calculamos en la siguiente proposición el del miembro izquierdo.

Proposición 6.2.7. *Sean* $d, m, n \in \mathbb{N}$ *con* $d < \min\{m,n\}$, *y* $\alpha, \beta \in K$. *Sea* $c = m+n-2d-1$. *Entonces,*

$$\operatorname{coeff}_{x^d}\big(h_d(\alpha,\beta,m,n)\big) = (-1)^{\binom{d}{2}}(\alpha-\beta)^c \prod_{i=1}^{d} \frac{(i-1)!\,(c+i)!}{(m-i)!(n-i)!}.$$

Demostración. Es claro que $\operatorname{coeff}_{x^d}(h_d(\alpha,\beta,m,n)) = (\alpha-\beta)^c \sum_{j=0}^{d} q_j(m,n,d)$.

Mostraremos ahora que $\sum_{j=1}^{d} q_j(m,n,d) = q_0(m+1,n,d)$, que prueba el enunciado debido al Teorema 6.2.2. Observemos que

$$\sum_{j=0}^{d} q_j(m,n,d) = \det \overbrace{\begin{bmatrix} 1 & \cdots & (-1)^d \\ \binom{c}{m-1} & \cdots & \binom{c}{m-d-1} \\ \vdots & & \vdots \\ \binom{c}{m-d} & \cdots & \binom{c}{m-2d} \end{bmatrix}}^{d+1}{}^{d+1}.$$

Para $0 \leq j \leq d$ notemos $\mathbf{c}(j)$ a la $(j+1)$-ésima columna de la matriz de arriba. En dicha matriz hacemos las operaciones elementales $\mathbf{c}(j) + \mathbf{c}(j-1) \to \mathbf{c}(j)$, para $j = d, \ldots, 0$.

Usando la identidad $\binom{c}{k-1} + \binom{c}{k} = \binom{c+1}{k}$, tenemos

$$\det \overset{d+1}{\left[\begin{array}{ccc} 1 & \dots & (-1)^d \\ \binom{c}{m-1} & \dots & \binom{c}{m-d-1} \\ \vdots & & \vdots \\ \binom{c}{m-d} & \dots & \binom{c}{m-2d} \end{array}\right]}_{d+1} = \det \overset{1}{\underset{d}{\left[\begin{array}{c|ccc} 1 & 0 & \dots & 0 \\ \hline \binom{c}{m-1} & \binom{c+1}{m-1} & \dots & \binom{c+1}{m-d} \\ \vdots & \vdots & & \vdots \\ \binom{c}{m-d-1} & \binom{c+1}{m-d} & \dots & \binom{c+1}{m-2d+1} \end{array}\right]}}_{1} \begin{matrix} \\ \\ \\ d \end{matrix}$$

$$= q_0(m+1, n, d).$$

□

Con esto podemos completar la demostración del Teorema 6.2.1.

Demostración del Teorema 6.2.1. Asumamos primero que $\operatorname{char}(K) = 0$ o $\operatorname{char}(K) \geq m + n - 2d$. Por las Proposiciones 6.2.5 y 6.2.7, tenemos que $\operatorname{Sres}_d((x-\alpha)^m, (x-\beta)^n)$ y $h_d(\alpha, \beta, m, n)$ son ambos polinomios de grados exactamente d, y por el Corolario 6.2.6 se tiene

$$h_d(\alpha, \beta, m, n) = \lambda \operatorname{Sres}_d((x-\alpha)^m, (x-\beta)^n),$$

con $\lambda \neq 0$. Luego

$$\begin{aligned} \frac{1}{\lambda} &= \frac{\operatorname{PSres}_d((x-\alpha)^m, (x-\beta)^n)}{\operatorname{coeff}_{x^d}(h_d(\alpha, \beta, m, n))} \\ &= \frac{(\alpha-\beta)^{(m-d)(n-d)} \prod_{i=1}^{d} \frac{(i-1)!\,(c+i)!}{(m-i)!(n-i)!}}{(-1)^{\binom{d}{2}} (\alpha-\beta)^c \prod_{i=1}^{d} \frac{(i-1)!\,(c+i)!}{(m-i)!(n-i)!}} \\ &= (-1)^{\binom{d}{2}} (\alpha-\beta)^{(m-d)(n-d)-c}, \end{aligned}$$

con $c = m+n-2d-1$, y donde hemos usado las identidades que vimos en las Proposiciones 6.2.5 y 6.2.7. Además la última igualdad vale incluso para $d = 0$. Esto prueba el enunciado.

Para el caso general usamos el hecho que el Teorema 6.2.1 vale para $(x-u_\alpha)^m$ y $(x-u_\beta)^n$ en el cuerpo $\mathbb{Q}(u_\alpha, u_\beta)$, donde u_α y u_β son variables independientes en $\mathbb{Q}$. Pero por la definición de subresultante, en este caso ésta pertenece de hecho a $\mathbb{Z}[u_\alpha, u_\beta][x]$. Luego, la igualdad del teorema se obtiene mediante la especialización $u_\alpha \mapsto \alpha$, $u_\beta \mapsto \beta$, y la identificación vía el morfismo de anillos standard de $\mathbb{Z}$ en K. □

6.3. Las subresultantes como polinomios de Jacobi

En esta sección iremos más allá con el estudio del caso estructurado que tratamos en este capítulo y mostraremos el sorprendente hecho que la subrestultante en este caso resulta ser un múltiplo escalar de un polinomio de Jacobi, salvo un cambio de variables afín. Esto implicará además una consecuencia respecto a la complejidad: debido a una ecuación diferencial que satisfacen ciertos polinomios de Jacobi, veremos que, en este caso,

pueden obtenerse en tiempo lineal los coeficientes de la subresultante en la base monomial.

Aquí presentamos el teorema central de esta sección. Vamos a volver a asumir $\alpha \neq \beta$; si son iguales ya sabemos que el caso es trivial.

Teorema 6.3.1. *Sean $m, n \in \mathbb{N}$, $0 \leq d < \min\{m, n\}$ y sea K un cuerpo. Sean $\alpha, \beta \in K$ con $\alpha \neq \beta$. Entonces*

$$\begin{aligned}&\operatorname{Sres}_d((x-\alpha)^m, (x-\beta)^n)\\ &\quad = (\alpha-\beta)^{(m-d)(n-d)+d} \prod_{i=1}^{d} \frac{i!(m+n-d-i-1)!}{(m-i)!(n-i)!}\, P_d^{(-n,-m)}\left(\frac{2x-\alpha-\beta}{\beta-\alpha}\right).\end{aligned}$$

Observemos que, si bien el polinomio de Jacobi $P_d^{(-n,-m)}$ sólo está definido si $\operatorname{char}(K) \neq 2$, al evaluarlo en $\left(\frac{2x-\alpha-\beta}{\beta-\alpha}\right)$ esa condición deja de ser necesaria. En efecto:

$$\begin{aligned}&P_d^{(-n,-m)}\left(\frac{2x-\alpha-\beta}{\beta-\alpha}\right)\\ &= \sum_{j=0}^{d} \frac{(-n+d-j+1)_j}{j!} \frac{(-m+j+1)_{d-j}}{(d-j)!} \left(\frac{\left(\frac{2x-\alpha-\beta}{\beta-\alpha}\right)-1}{2}\right)^{d-j} \left(\frac{\left(\frac{2x-\alpha-\beta}{\beta-\alpha}\right)+1}{2}\right)^{j}\\ &= \sum_{j=0}^{d} \frac{(-n+d-j+1)_j}{j!} \frac{(-m+j+1)_{d-j}}{(d-j)!} \left(\frac{x-\beta}{\beta-\alpha}\right)^{d-j} \left(\frac{x-\alpha}{\beta-\alpha}\right)^{j}\\ &= \frac{(-1)^d}{(\beta-\alpha)^d} \sum_{j=0}^{d} \binom{n-d+j-1}{j} \binom{m-j-1}{d-j} (x-\alpha)^j (x-\beta)^{d-j}, \qquad (6.9)\end{aligned}$$

usando en (6.9) lo que observamos en (6.1). De este modo vemos que el polinomio pertenece a $\mathbb{Z}[\alpha, \beta]$, por lo que podemos identificar sus coeficientes como elementos de K sin importar su característica, como hicimos en la demostración del Teorema 6.2.1. Pero más aún, la escritura del polinomio de Jacobi en (6.9) es exactamente la expansión de dicho polinomio en la base de Bernstein del Teorema 6.2.1, de modo que para probar el Teorema 6.3.1 basta ver que los coeficientes de dicha expansión son los mismos que en el Teorema 6.3.1.

Demostración del Teorema 6.3.1. Comparando coeficientes en el enunciado del Teorema 6.3.1 con en el Teorema 6.2.1 y usando la identidad (6.9), basta verificar que

$$\begin{aligned}&\binom{n-d+j-1}{j} \binom{n-j-1}{d-j} \prod_{i=1}^{d} \frac{i!(m+n-d-i-1)!}{(m-i)!(n-i)!}\\ &\qquad = \frac{\binom{d}{j}\binom{n-d+j-1}{j}}{\binom{m-1}{j}} \prod_{i=1}^{d} \frac{(i-1)!(m+n-2d+i-2)!}{(m-i-1)!(n-i)!},\end{aligned}$$

es decir, luego de una sencilla simplificación, que

$$\frac{(m-1)!}{(m-d)!} \prod_{i=1}^{d} \frac{i!}{(m-i)!} = d! \prod_{i=1}^{d} \frac{(i-1)!}{(m-i-1)!},$$

lo cual vale trivialmente.

Para el caso general, hacemos exactamente el mismo razonamiento que hicimos en la demostración del Teorema 6.2.1. Usamos el hecho que el Teorema 6.3.1 vale para $(x-u_\alpha)^m$ y $(x-u_\beta)^n$ en el cuerpo $\mathbb{Q}(u_\alpha, u_\beta)$, donde u_α y u_β son variables independientes en $\mathbb{Q}$, y observando que la subresultante en este caso pertenece a $\mathbb{Z}[u_\alpha, u_\beta][x]$, terminamos la demostración mediante la especialización $u_\alpha \mapsto \alpha$, $u_\beta \mapsto \beta$, y la identificación vía el morfismo de anillos standard de $\mathbb{Z}$ en K. □

Esta demostración que dimos resulta muy elemental y directa y pudimos hacerla una vez que sabíamos qué fórmula debíamos probar, luego de un proceso computacional de predicción y prueba. No fue la primera demostración que encontramos en sentido cronológico. De todos modos daremos otra demostración que nos provee además más información. Antes, como consecuencia del Teorema 6.3.1, enunciamos el siguiente corolario, que da una recurrencia que satisfacen los coeficientes de $\mathrm{Sres}_d((x-\alpha)^m, (x-\beta)^n)$ en la base monomial.

Corolario 6.3.2. *Sean $m, n \in \mathbb{N}$, $0 \le d < \min\{m, n\}$ y sea K un cuerpo con $\mathrm{char}(K) = 0$ o $\mathrm{char}(K) \ge m + n$. Sean $\alpha, \beta \in K$ con $\alpha \ne \beta$. Si escribimos*

$$\mathrm{Sres}_d((x-\alpha)^m, (x-\beta)^n) = \sum_{k=0}^{d} s_k x^k,$$

los coeficientes s_k, para $0 \le k \le d$, quedan definidos por la siguiente recurrencia de segundo orden:

$$s_k = \frac{-(k+1)\Big(\big((n-k-1)\alpha + (m-k-1)\beta\big)s_{k+1} + (k+2)\alpha\beta s_{k+2}\Big)}{(d-k)(m+n-d-1-k)},$$

si $k = d-2, \ldots, 0$, y con condiciones iniciales

$$\begin{aligned} s_d &= \mathrm{PSres}_d((x-\alpha)^m, (x-\beta)^n) \text{ y} \\ s_{d-1} &= \frac{-d((n-d)\alpha + (m-d)\beta)}{m+n-2d}\,\mathrm{PSres}_d((x-\alpha)^m, (x-\beta)^n). \end{aligned}$$

Con este resultado lograremos obtener el resultado de complejidad que mencionamos, en el Teorema 6.3.4 más abajo. Ahora daremos la segunda demostración del Teorema 6.3.1.

Otra demostración del Teorema 6.3.1. Aquí también supondremos primero $\mathrm{char}(K) = 0$. Se puede verificar (o ver en [Sze1975, Th 4.23.1]) que los polinomios

$$P_d^{(-n,-m)}(z),\ (1+z)^m P_{n-d-1}^{(-n,m)}(z) \text{ y } (1-z)^n P_{m-d-1}^{(n,-m)}(z),$$

satisfacen la ecuación diferencial

$$(1-z^2)y''(z) + \big(-m+n+(m+n-2)z\big)y'(z) + d(d-m-n+1)y(z) = 0.$$

Haciendo la sustitución $z = \frac{2x-\alpha-\beta}{\beta-\alpha}$ en esta ecuación diferencial podemos ver que los polinomios

$$\begin{aligned}
y_1(x) &:= P_d^{(-n,-m)}\left(\frac{2x-\alpha-\beta}{\beta-\alpha}\right),\\
y_2(x) &:= \left(\frac{2}{\beta-\alpha}\right)^m (x-\alpha)^m P_{n-d-1}^{(-n,m)}\left(\frac{2x-\alpha-\beta}{\beta-\alpha}\right),\\
y_3(x) &:= \left(\frac{-2}{\beta-\alpha}\right)^n (x-\beta)^n P_{m-d-1}^{(n,-m)}\left(\frac{2x-\alpha-\beta}{\beta-\alpha}\right),
\end{aligned}$$

satisfacen la ecuación diferencial

$$\begin{aligned}
(x-\alpha)(x-\beta)y''(x)+\big(\alpha(n-1)+\beta(m-1)-(m+n-2)x\big)y'(x)\\
+ d(m+n-d-1)y(x) = 0.
\end{aligned} \tag{6.10}$$

Pero dado que el espacio solución de esta ecuación tiene dimensión 2, los tres polinomios son necesariamente linealmente dependientes. Si especializamos y_2 en β, se obtiene $P_{n-d-1}^{-n,-m}(1)$. Pero por definición es claro que esto es distinto de cero. De hecho, en general, vemos que

$$P_r^{(k,l)}(1) = \frac{(k+1)_r}{r!} \quad \text{y} \quad P_r^{(k,l)}(-1) = (-1)^r \frac{(l+1)_r}{r!}. \tag{6.11}$$

Luego, β es raíz de y_3 pero no lo es de y_2, por lo que dichos polinomios no son múltiplos uno del otro. Así, necesariamente y_1 es combinación lineal de y_2 y de y_3. Esto es, existen constantes A y B tales que

$$\begin{aligned}
P_d^{(-n,-m)}\left(\frac{2x-\alpha-\beta}{\beta-\alpha}\right) =& A\left(\frac{2}{\beta-\alpha}\right)^m (x-\alpha)^m P_{n-d-1}^{(-n,m)}\left(\frac{2x-\alpha-\beta}{\beta-\alpha}\right)\\
&+ B\left(\frac{-2}{\beta-\alpha}\right)^n (x-\beta)^n P_{m-d-1}^{(n,-m)}\left(\frac{2x-\alpha-\beta}{\beta-\alpha}\right).
\end{aligned} \tag{6.12}$$

Observemos que $P_d^{(-n,-m)}\left(\frac{2x-\alpha-\beta}{\beta-\alpha}\right) \neq 0$. Esto lo vemos, por ejemplo, notando que al evaluar en β resulta $P_d^{(-n,-m)}(1)$, que no es cero por (6.11). Además tenemos

$$\begin{aligned}
&\deg(P_d^{(-n,-m)}\left(\frac{2x-\alpha-\beta}{\beta-\alpha}\right)) \leq d,\\
&\deg(P_{n-d-1}^{(-n,m)}\left(\frac{2x-\alpha-\beta}{\beta-\alpha}\right)) \leq n-d-1 \quad \text{y}\\
&\deg(P_{m-d-1}^{(n,-m)}\left(\frac{2x-\alpha-\beta}{\beta-\alpha}\right)) \leq m-d-1.
\end{aligned}$$

Luego, por la Proposición 1.1.6, existe $\mu := 1/\lambda \in K$ tal que

$$\operatorname{Sres}_d((x-\alpha)^m,(x-\beta)^n) = \mu\, P_d^{(-n,-m)}\left(\frac{2x-\alpha-\beta}{\beta-\alpha}\right). \tag{6.13}$$

Calculemos ahora μ comparando los coeficientes principales.

El coeficiente principal de $P_d^{(-n,-m)}\left(\frac{2x-\alpha-\beta}{\beta-\alpha}\right)$ es igual, por (6.9), a

$$\frac{(-1)^d}{(\beta-\alpha)^d}\sum_{j=0}^{d}\binom{n-d+j-1}{j}\binom{m-j-1}{d-j}=\frac{1}{(\alpha-\beta)^d}\binom{m+n-d-1}{d}.$$

Esta igualdad puede verse fácilmente pensando en una combinación con repetición de un conjunto de $m+n-2d$ elementos tomados de a d, calculada del siguiente modo. Escribimos al conjunto como una unión disjunta de dos subconjuntos de $n-d$ y $m-d$ elementos y sumamos, para $j=0,\dots,d$, la combinación con repetición del conjunto de $n-d$ elementos tomados de a j, multiplicada por la combinación con repetición del conjunto de $m-d$ elementos tomados de a $d-j$.

Hemos visto entonces que

$$\mu=\frac{(\alpha-\beta)^d}{\binom{m+n-d-1}{d}}\mathrm{PSres}_d((x-\alpha)^m,(x-\beta)^n), \tag{6.14}$$

pero por la Proposición 6.2.5 sabemos que

$$\mathrm{PSres}_d((x-\alpha)^m,(x-\beta)^n)=(\alpha-\beta)^{(m-d)(n-d)}\prod_{i=1}^{d}\frac{(i-1)!\,(m+n-2d+i-1)!}{(m-i)!(n-i)!}.$$

Esto implica entonces que

$$\begin{aligned}\mu&=(\alpha-\beta)^{(m-d)(n-d)+d}\frac{\prod_{i=1}^{d}\frac{(i-1)!\,(m+n-2d+i-1)!}{(m-i)!(n-i)!}}{\binom{m+n-d-1}{d}}\\&=(\alpha-\beta)^{(m-d)(n-d)+d}\prod_{i=1}^{d}\frac{i!(m+n-d-i-1)!}{(m-i)!(n-i)!},\end{aligned}$$

que prueba el enunciado.

El caso general, para cualquier característica, sigue del mismo razonamiento que hicimos en las demostraciones de los Teoremas 6.2.1 y 6.3.1. □

La ventaja de esta segunda demostración que dimos, respecto de la primera, es que nos brinda más información. Dado que los coeficientes en (6.12) son polinomios de Jacobi, se tiene como consecuencia que los polinomios $F_d(f,g)$ y $G_d(f,g)$ de la identidad de Bézout, definidos en la Proposición 1.1.4, son también, así como lo es la subresultante, múltiplos escalares de polinomios de Jacobi, salvo el mismo cambio de variables afín. Esto lo precisamos en el siguiente corolario.

Corolario 6.3.3. *Sean $m,n\in\mathbb{N}$, $0\le d<\min\{m,n\}$ y sea K un cuerpo. Sean $\alpha,\beta\in K$ con $\alpha\neq\beta$. Entonces*

$$\begin{aligned}F_d(f,g)&=\frac{(-1)^{n-1}\mu}{(\beta-\alpha)^m}\,P_{n-d-1}^{(-n,m)}\left(\frac{2x-\alpha-\beta}{\beta-\alpha}\right),\\G_d(f,g)&=\frac{(-1)^{n}\mu}{(\beta-\alpha)^n}\,P_{m-d-1}^{(n,-m)}\left(\frac{2x-\alpha-\beta}{\beta-\alpha}\right),\end{aligned}$$

donde μ es la constante definida en (6.14)*, y $F_d(f,g)$ y $G_d(f,g)$ son los coeficientes de la identidad de Bézout de la Proposición 1.1.4, con $f=(x-\alpha)^m$ y $g=(x-\beta)^n$.*

Demostración. Por la Proposición 1.1.4 y la igualdad (6.13) los coeficientes de la identidad (6.12) son necesariamente, salvo la constante μ, los polinomios $F_d(f,g)$ y $G_d(f,g)$ de dicha proposición. Especializando esta identidad en α y luego en β y aplicando (6.11) tenemos

$$\begin{aligned}\binom{m-1}{d} &= P_d^{(-n,-m)}(-1) = B\left(\frac{-2}{\beta-\alpha}\right)^n P_{m-d-1}^{(n,-m)}(-1)(\alpha-\beta)^n \\ &= 2^n\binom{m-1}{d}B, \\ (-1)^d\binom{n-1}{d} &= P_d^{(-n,-m)}(1) = A\left(\frac{2}{\beta-\alpha}\right)^m P_{n-d-1}^{(-n,m)}(1)(\beta-\alpha)^m \\ &= (-1)^{n-d-1}2^m\binom{n-1}{d}A.\end{aligned}$$

Luego, $A=\frac{(-1)^{n-1}}{2^m}$ y $B=\frac{1}{2^n}$. Reemplazando estos valores en (6.12) y multiplicando por la constante μ, definida en (6.14), probamos lo que queremos. □

Ahora probaremos el Corolario 6.3.2.

Demostración del Corolario 6.3.2. La igualdad $s_d = \mathrm{PSres}_d((x-\alpha)^m,(x-\beta)^n)$ es simplemente por definición. Notemos ahora que, por la identidad (6.13), se tiene que $s(x) := \mathrm{Sres}_d((x-\alpha)^m,(x-\beta)^n)$ satisface la ecuación diferencial (6.10), así como lo hace el polinomio de Jacobi de la misma identidad. Esto nos hará deducir la expresión para s_{d-1} y la recurrencia. Tenemos

$$s(x)=\sum_{k=0}^{d}s_kx^k,\ s'(x)=\sum_{k=1}^{d}ks_kx^{k-1}\ \text{y}\ s''(x)=\sum_{k=2}^{d}k(k-1)s_kx^{k-2}.$$

Así

$$\begin{aligned}(x-\alpha)(x-\beta)s''(x) &= \sum_{k=2}^{d}k(k-1)s_kx^k-(\alpha+\beta)\sum_{k=2}^{d}k(k-1)s_kx^{k-1} \\ &\quad+\alpha\beta\sum_{k=2}^{d}k(k-1)s_kx^{k-2} \\ &= \sum_{k=0}^{d}k(k-1)s_kx^k-(\alpha+\beta)\sum_{k=0}^{d-1}(k+1)ks_{k+1}x^k \\ &\quad+\alpha\beta\sum_{k=0}^{d-2}(k+2)(k+1)s_{k+2}x^k,\end{aligned}$$

$$(\alpha(n-1)+\beta(m-1)-(m+n-2)x)\,s'(x) = -(m+n-2)\sum_{k=1}^{d} k s_k x^k$$
$$+(\alpha(n-1)+\beta(m-1))\sum_{k=1}^{d} k s_k x^{k-1}$$
$$= -(m+n-2)\sum_{k=0}^{d} k s_k x^k + (\alpha(n-1)+\beta(m-1))\sum_{k=0}^{d-1}(k+1)s_{k+1}x^k,$$

y

$$d(m+n-d-1)s(x) = d(m+n-d-1)\sum_{k=0}^{d} s_k x^k.$$

Comparando entonces el coeficiente de grado $d-1$ en (6.10), obtenemos

$$(d-1)(d-2)s_{d-1} - (\alpha+\beta)d(d-1)s_d - (m+n-2)(d-1)s_{d-1}$$
$$+\big(\alpha(n-1)+\beta(m-1)\big)ds_d + d(m+n-d-1)s_{d-1} = 0.$$

Luego

$$s_{d-1} = \frac{-d((n-d)\alpha+(m-d)\beta)}{m+n-2d}\,s_d,$$

como queríamos.

Comparemos ahora el coeficiente de grado k en (6.10) para $k = 0,\dots,d-2$:

$$\big(k(k-1)-(m+n-2)k+d(m+n-d-1)\big)s_k + \big(-(\alpha+\beta)(k+1)k$$
$$+(\alpha(n-1)+\beta(m-1))(k+1)\big)s_{k+1} + \alpha\beta(k+2)(k+1)s_{k+2} = 0.$$

De aquí resulta,

$$s_k = \frac{-(k+1)\Big(\big((n-k-1)\alpha+(m-k-1)\beta\big)s_{k+1} + (k+2)\alpha\beta s_{k+2}\Big)}{(d-k)(m+n-d-1-k)},$$

lo cual termina la demostración. □

Finalmente, gracias a la recurrencia del Corolario 6.3.2, vamos a concluir un interesante resultado referido a la complejidad para calcular la subresultante. Pero también mostraremos la complejidad para calcular las subresultantes principales.

Teorema 6.3.4. *Sean $m,n \in \mathbb{N}$ y K un cuerpo tal que $\mathrm{char}(K) = 0$ o $\mathrm{char}(K) \geq m+n$. Sean $\alpha,\beta \in K$. Entonces es posible calcular, usando $O(m+n)$ operaciones en K:*

1. *Todas las subresultantes prinicpales $\mathrm{PSres}_d((x-\alpha)^m,(x-\beta)^n)$ para $0 \leq d < \min\{m,n\}$.*
2. *Los coeficientes de la d-ésima subresultante $\mathrm{Sres}_d((x-\alpha)^m,(x-\beta)^n)$ en la base monomial, para cualquier $d < \min\{m,n\}$.*

Demostración. Para probar 1. notemos, para $1 \leq d < \text{mín}\{m, n\}$,

$$u(d) := \frac{\text{PSres}_d((x-\alpha)^m, (x-\beta)^n)}{\text{PSres}_{d-1}((x-\alpha)^m, (x-\beta)^n)}.$$

Podemos ver, por la Proposición 6.2.5, que para $1 \leq d < \text{mín}\{m, n\} - 1$ se tiene,

$$\begin{aligned}\frac{u(d+1)}{u(d)} &= \frac{\text{PSres}_{d+1}((x-\alpha)^m, (x-\beta)^n)\text{PSres}_{d-1}((x-\alpha)^m, (x-\beta)^n)}{\text{PSres}_d((x-\alpha)^m, (x-\beta)^n)^2} \\ &= (\alpha-\beta)^2 \frac{d(m-d)(n-d)(m+n-d)}{(m+n-2d-1)(m+n-2d)^2(m+n-2d+1)}.\end{aligned}$$

Así, una vez calculado $u(1)$, podemos calcular todos los $u(d)$ para $1 \leq d < \text{mín}\{m, n\}$ agregando $O(\text{mín}\{m, n\})$ operaciones aritméticas en K. Dado que

$$u(1) = \frac{(m+n-2)!}{(\alpha-\beta)^{m+n-1}(m-1)!(n-1)!},$$

éste puede ser calculado mediante multiplicaciones usando $O(m+n)$ operaciones en K. Luego, todos los $u(d)$ pueden calcularse usando $O(m+n)$ operaciones en K. Con esto podemos calcular todas las subresultantes principales $\text{PSres}_d((x-\alpha)^m, (x-\beta)^n)$ para $0 \leq d < \text{mín}\{m, n\}$ del siguiente modo:

$$\text{PSres}_d((x-\alpha)^m, (x-\beta)^n) = \text{PSres}_0((x-\alpha)^m, (x-\beta)^n) \cdot u(1) \cdots u(d),$$

donde $\text{PSres}_0((x-\alpha)^m, (x-\beta)^n) = (\alpha-\beta)^{mn}$, que sólo agrega $\text{mín}\{m, n\}$ operaciones.

Notemos que las únicas divisiones en K que hicimos fueron por números enteros no nulos de valor absoluto menor o igual que $m+n-1$, los cuales son inversibles en K bajo la hipótesis que tenemos para $\text{char}(K)$.

Ahora probamos 2. usando la recurrencia del Corolario 6.3.2. Dicha recurrencia implica inmediatamente que se pueden calcular todos los coeficientes de la d-ésima subresultante en la base monomial usando $O(\text{máx}\{m+n-d, d\})$ operaciones en K. Primero, del mismo modo que lo hicimos al demostrar 1., la Proposición 6.2.5 nos muestra que s_d puede calcularse usando $O(m+n-d)$ operaciones aritméticas en K. Luego calculamos s_{d-1} agregando $O(1)$ operaciones. Y a partir de estos, al calcular cada s_k, desde $k = d-2$ hasta $k = 0$, se van agregando, en cada uno de estos $d-1$ pasos, $O(1)$ operaciones en K, y esto prueba el enunciado. Notemos que aquí tampoco hay problemas con las divisiones que hicimos bajo la hipótesis que tenemos para la característica de K. □

Notemos por $M(D)$ a la complejidad aritmética de la multiplicación de dos polinomios en $K[x]$ de grados a lo sumo D. Es un resultado clásico que puede verse, por ejemplo, en [GaGe2013, Ch. 8], que $M(D)$ puede ser del orden de $O(D \log D \log\log D)$. Para polinomios arbitrarios en $K[x]$ de grados a lo sumo D, los algoritmos más rápidos calculan usando $O(M(D)\log D)$ operaciones en K o bien una subresultante fija ([Rei1997]), o bien todas las subresultantes principales ([GaGe2013, Cor. 11.18]). Es un problema abierto saber si esto puede mejorarse a $O(M(D))$ operaciones, incluso para la resultante. Según nuestro conocimiento, el Teorema 6.3.1 exhibe la primera familia estructurada de polinomios para los cuales la subresultante puede calcularse con una complejidad óptima, esto es, lineal.

Bibliografía

[ApJo2006] F. Apéry, J.-P. Jouanolou. *Résultant et sous-résultants: le cas d'une variable avec exercices corrigés.* Hermann, Paris 2006. 477 pp. (based on Cours DESS 1995-1996).

[And1996] G. Andrews. *Pfaff's method. II. Diverse applications.* J. Comput. Appl. Math. 68 (1996), no. 1-2, 15-23.

[And1997] E. Andrews. *Pfaff's method. III. Comparison with the WZ method. The Foata Festschrift.* Electron. J. Combin. 3 (1996), no. 2, 18 pp.

[BDKSV2017] A. Bostan, C. D'Andrea, T. Krick, A. Szanto, M. Valdettaro. *Subresultants in multiple roots: An extremal case.* Linear Algebra Appl. 529 (2017), 185-198. https://doi.org/10.1016/j.laa.2017.04.019 Disponible en https://arxiv.org/abs/1608.03740

[Bez1764] E. Bézout. *Recherches sur le degré des équations résultantes de l'evanouuissement des inconnues, et sur le moyens qu'il convenient d'employer pour trouver ces équations.* Mém. Acad. Roy. Sci Paris (1764), 288–338.

[BeLa2000] B. Beckermann, G. Labahn. *Fraction-free computation of matrix rational interpolants and matrix GCDs.* SIAM J. Matrix Anal. Appl. 22 (2000), no. 1, 114-144.

[BrTr1971] W. S. Brown, J. F. Traub. *On Euclid's algorithm and the theory of subresultants.* J. Assoc. Comput. Mach. 18 (1971), 505-514.

[ChLo1996] W. Y. Chen, J.D. Louck. *Interpolation for symmetric functions.*, Adv. Math. 117 (1996), no. 1, 147-156.

[CLO2007] D. Cox, J. Little, D. O'Shea. *Ideals, varietes and algorithms.* Undergraduate texts in mathematics, Springer-Verlag, 2007.

[Col1967] G. Collins. *Subresultants and reduced polynomial remainder sequences.* J. Assoc. Comput. Mach. 14 (1967), 128-142.

[Dar1876] G. Darboux. *Sur la théorie l'élimination entre deux équations a une inconnue.* Bull. Sci. Math. (1876), no. 10, 56-64.

[DHKS2007] C. D'Andrea, H. Hong, T. Krick, A. Szanto. *An elementary proof of Sylvester's double sums for subresultants.* J. Symbolic Comput. 42 (2007), no. 3, 290-297.

[DHKS2009] C. D'Andrea, H. Hong, T. Krick, A. Szanto. *Sylvester's double sums: the general case.* J. Symbolic Comput. 44 (2009), no. 9, 1164-1175.

[DKS2013] C. D'Andrea, T. Krick, A. Szanto. *Subresultants in multiple roots.* Linear Algebra Appl. 438 (2013), no. 5, 1969-1989.

[DKS2015] C. D'Andrea, T. Krick, A. Szanto. *Subresultants, Sylvester sums and the rational interpolation problem.* J. Symbolic Comput. 68 (2015), part 1, 72-83.

[DKSV2017] C. D'Andrea, T. Krick, A. Szanto, M. Valdettaro. *Closed Formula For Univariate Subresultants In Multiple Roots.* Aceptado para su presentación en MEGA 2017, Nice (France), June 12-16, 2017. Disponible en https://arxiv.org/abs/1612.05160

[GCL1992] K. O. Geddes, S. R. Czapor, G. Labahn. *Algorithms for computer algebra.* Kluwer Academic Publishers (1992), xxii+585 pp. ISBN: 0-7923-9259-0.

[GaGe2013] J. von zur Gathen, J. Gerhard. *Modern computer algebra, 3rd Edition.* Cambridge University Press (2013), xiv+795 pp. ISBN: 978-1-107-03903-2.

[GaLu2003] J. von zur Gathen, T. Lücking. *Subresultants revisited.* Theoret. Comput. Sci. 297 (2003), no. 1-3, 199-239.

[Jac1836] C. G. J. Jacobi. *De eliminatione variabilis e duabus aequationibus algebraicis.* J. Reine Angew. Math. 15 (1836), 101-124.

[Kal1984] D. Kalman. *The generalized Vandermonde matrix.* Math. Mag. 57 (1984), no. 1, 15-21.

[Kra1990] Christian Krattenthaler. *Generating functions for plane partitions of a given shape.* Manuscripta Math. 69, (1990), no. 2, 173-201.

[Kri2017] T. Krick. *Resultante, subresultantes y sumas de Sylvester (2017).* Disponible en http://mate.dm.uba.ar/ krick/Subresultantes2017.pdf

[KrSz2012] T. Krick, A. Szanto. *Sylvester's double sums: an inductive proof of the general case.* J. Symbolic Comput. 47 (2012), no. 8, 942-953.

[KST2006] S. Kaplan, A. Shapiro, M. Teicher. *Several applications of Bézout matrices (2006).* Disponible en arXiv:math/0601047.

[KSV2017] T. Krick, A. Szanto, M. Valdettaro. *Symmetric interpolation, exchange lemma and Sylvester sums.* Comm. Algebra 45 (2017), no. 8, 3231-3250. http://dx.doi.org/10.1080/00927872.2016.1236121 Disponible en https://arxiv.org/abs/1503.00607

[Las] A. Lascoux. *Notes on Interpolation in one and several variables.* Disponible en http://igm.univ-mlv.fr/ al/ARTICLES/interp.dvi.gz

[LaPr2003] A. Lascoux, P. Pragacz. *Double Sylvester sums for subresultants and multi-Schur functions.* J. Symbolic Comput. 35 (2003), no. 6, 689-710.

[MaGa1990] K. Ma, J. von zur Gathen. *Analysis of euclidean algorithms for polynomials over finite fields.* J. Symbolic Comput. 9 (1990), no. 4, 429-455.

[Map2016] Maple 2016. *Maplesoft, a division of Waterloo Maple Inc., Waterloo, Ontario.*

[Mis1993] B. Mishra. *Algorithmic algebra.* Texts and Monographs in Computer Science. Springer-Verlag, New York (1993), xii+416 pp. ISBN: 0-387-94090-1.

[Ost1964] A. M. Ostrowski. *On some determinants with combinatorial numbers.* J. Reine Angew. Math 216 (1964), 25-30.

[Pfa1797] J. F. Pfaff. *Observationes analyticae ad L. Euleri Institutiones Calculi Integralis, Vol. IV, Supplem. II et IV.* Histoire de l'Académie Impériale des Sciences (1793). In: Nova Acta Academiae Scientiarum Imperialis Petropolitanae XI (1797), 37-57.

[Poi1802] S.-D. Poisson. *Mémoire sur l'élimination dans les équations algébriques.* Journal de l'École polytechnique, tome IV, 11e cahier (1802), 199-203.

[Rei1997] D. Reischert. *Asymptotically fast computation of subresultants.* Proceedings of the 1997 International Symposium on Symbolic and Algebraic Computation (Kihei, HI), ACM, New York (1997), 233–240.

[RoSz2011] M.-F. Roy, A. Szpirglas. *Sylvester double sums and subresultants.* J. Symbolic Comput. 46 (2011), no. 4, 385-395.

[Saa1890] L. Saalschütz. *Eine Summationsformel.* Zeitschr. für Math. u. Phys. 35 (1890), 186-188.

[Sha2004] A. Shakoori. *The Bézout matrix in the Lagrange basis.* EACA (2004), 295–299.

[Sla1966] L. J. Slater. *Generalized hypergeometric functions.* Cambridge University Press (1966), xiii+273 pp.

[Syl1839] J. J. Sylvester. *On rational derivation from equations of coexistence, that is to say, a new and extended theory of elimination.* Philos. Mag. 15 (1839), 428-435. Also appears in the Collected Mathematical Papers of James Joseph Sylvester, Vol. 1, Chelsea Publishing Co. (1973), 40–46.

[Syl1840] J. J. Sylvester. *A method of determining by mere inspection the derivatives from two equations of any degree.* Philos. Mag. 16 (1840), 132-135. Also appears in the Collected Mathematical Papers of James Joseph Sylvester, Vol. 1, Chelsea Publishing Co. (1973), 54-57.

[Syl1840b] J. J. Sylvester. *Note on elimination.* Philos. Mag. 17 (1840), no. 11, 379-380. Also appears in the Collected Mathematical Papers of James Joseph Sylvester, Vol. 1, Chelsea Publishing Co. (1973), p. 58.

[Syl1853] J. J. Sylvester. *On a theory of syzygetic relations of two rational integral functions, comprising an application to the theory of Sturm's function and that of the greatest algebraical common measure.* Philosophical Transactions of the Royal Society of London, Part III (1853), 407-548. Also appears in Collected Mathematical Papers of James Joseph Sylvester, Vol. 1, Chelsea Publishing Co. (1973) 429-586.

[Sze1975] G. Szegö. *Orthogonal Polynomials.* American Mathematical Society, 4th edition, Colloquium Publications, Vol. XXIII., Providence, R.I. (1975), xiii+432 pp.

[Zei1990] Doron Zeilberger. *The method of creative telescoping.* J. Symbolic Comput. 11 (1991), no. 3, 195-204.