Resultante, subresultantes y sumas de Sylvester

Teresa Krick*

Las resultantes, y subresultantes, de dos polinomios univariados se remontan a G.W. Leibniz, L. Euler, E. Bézout y C.G.J. Jacobi. Su presentación moderna se debe a J.J. Sylvester en [Syl1853]. Para una reseña histórica (y más) ver el fantástico libro [vzGG1999].
La resultante es un concepto que aparece en forma esencial en varias ramas de la matemática y es un ingrediente muy natural en muchas demostraciones, además de tener una importancia algorítmica muy reconocida actualmente. Es un elemento clave de la teoría de la eliminación, que estuvo muy en voga hasta los años 50 en cuanto era útil para producir ejemplos y enunciados en el período pre-"haces y esquemas" de la Geometría Algebraica, y renació a partir del desarrollo masivo de la computación a fines de los años 60, cuando se pudo empezar a calcular cosas inimaginables previamente. (A modo de ejemplo, la teoría de la eliminación ocupaba todo un capítulo en las tres primeras ediciones alemanas del 2do volumen de la biblia de muchos algebristas, *Moderne Algebra*, de B.L. van der Waerden [vdW1931-1955], que fue luego removido a partir de la extensamente reescrita edición de 1959.)
Las subresultantes volvieron también a aparecer a fines de los 60 para dar un algoritmo eficiente y paralelizable para el cálculo del máximo común divisor de dos polinomios [Col1967, BrTr1971], y más recientemente son también utilizadas en computación simbólica-numérica.
Las hoy llamadas sumas de Sylvester fueron introducidas por Sylvester también en [Syl1853], donde en ese largo artículo (cuyo título es casi tan largo como el texto) el autor presenta la conexión que existe entre ellas y las subresultantes, siendo las sumas de Sylvester una descripción en raíces de las subresultantes, así como la fórmula de Poisson es una descripción en raíces de la resultante. Muchos dudan que haya efectivamente una demostración de esa conexión en [Syl1853], y desde 2003 en [LaPr2003] han aparecido varias pruebas distintas utilizando diferentes herramientas como los polinomios de Schur, manipulaciones matriciales, inducción e interpolación para obtenerlas.
Las resultantes en varias variables fueron principalmente introducidas por Macaulay en [Mac1902, Mac1916] luego de trabajo previo por Euler, Sylvester y A.L. Cauchy, mientras que la primer generalización de subresultantes a varias variables apareció en [GVe1990, GVe1991], siendo la versión de [Cha1994, Cha1995] la que se suele utilizar en la actualidad. Siguen constituyendo áreas activas de investigación, tanto en cuanto a sus propiedades teóricas como a sus aplicaciones.

1 La resultante de dos polinomios univariados

Sean $f = a_m x^m + \cdots + a_0$ y $g = b_n x^n + \cdots + b_0$ dos polinomios de grados *exactamente* $m, n \geq 1$, es decir $a_m \neq 0$ y $b_n \neq 0$, con coeficientes en un cuerpo K (o eventualmente en un dominio íntegro con cuerpo cociente K). La *resultante* $\mathrm{Res}(f,g)$ de f y g es un número en K (o en el dominino íntegro), que da una condición necesaria y suficiente para que f y g compartan una raíz en $\overline{K}$, una clausura algebraica de K, o lo que es lo mismo, cuando su máximo común divisor $\mathrm{mcd}(f,g) \in K[x]$ tiene grado ≥ 1. Una forma de obtenerla es como el determinante de una matrix

*Mi agradecimiento a Alicia Dickenstein, Eduardo Cattani y Vilmar Trevisan, quienes me instigaron tácitamente a escribir una versión preliminar de este texto an Abril 2015, y también por sus observaciones y comentarios que ayudaron a mejorarlo.

formada con los coeficientes de f y g, introducida por Sylvester.

Definición 1.1 *Sean* $f = a_m x^m + \cdots + a_0, g = b_n x^n + \cdots + b_0 \in K[X]$, *con* K *cuerpo, que satisfacen* $a_m \neq 0$ *y* $b_n \neq 0$. *La* resultante *de* f *y* g *es*

$$\mathrm{Res}(f,g) := \det(S(f,g)),$$

donde $S(f,g)$ *es la matriz de Sylvester de* f *y* g,

$$S(f,g) := \overbrace{\left|\begin{array}{ccc|ccc} a_m & & & b_n & & \\ \vdots & \ddots & & \vdots & \ddots & \\ \vdots & & a_m & \vdots & & \ddots \\ \vdots & & \vdots & b_0 & & b_n \\ a_0 & & \vdots & & \ddots & \vdots \\ & \ddots & \vdots & & & \vdots \\ & & a_0 & & & b_0 \end{array}\right|}^{n \qquad\qquad m}_{m+n} \in K,$$

que se define como esta o su transpuesta, según los textos, ya que esto no tiene importancia al tomar determinante.

Ejemplos 1.2
(1) Sean $f = x - \alpha$ *y* $g = x - \beta$. *Entonces*

$$\mathrm{Res}(f,g) = \det \begin{pmatrix} 1 & 1 \\ -\alpha & -\beta \end{pmatrix} = \alpha - \beta.$$

(2) Sean ahora $f = x - \alpha$ *y* $g = b_n x^n + b_{n-1} x^{n-1} + \cdots + b_0$. *Entonces*

$$\mathrm{Res}(f,g) = \det \left(\begin{array}{ccc|c} 1 & & & b_n \\ -\alpha & \ddots & & b_{n-1} \\ & \ddots & 1 & \vdots \\ & & -\alpha & b_0 \end{array}\right) = g(\alpha),$$

como se ve desarrollando el determinante por la última columna.

Notemos que en estos ejemplos se cumple que $\mathrm{Res}(f,g) = 0 \Leftrightarrow \alpha$ es raíz de g, es decir f y g comparten una raíz. Esto es lo que se mencionó más arriba que vale en general, y que hace que la resultante sea el objeto tan importante que es.

Teorema 1.3 *Sean* $f, g \in K[x]$. *Entonces*

$$\mathrm{Res}(f,g) = 0 \Leftrightarrow \mathrm{gr}(\mathrm{mcd}(f,g)) \geq 1 \Leftrightarrow \exists\, \alpha \in \overline{K} \text{ tal que } f(\alpha) = g(\alpha) = 0.$$

Prueba.- La segunda equivalencia es conocida. Nos dedicamos entonces a la primera.
Para ello consideremos la transformación lineal Φ siguiente entre los K-espacios vectoriales de polinomios

$$K[x]_{<n} \times K[x]_{<m} := \{(s,t) :\ s,t \in K[x], s = 0 \text{ o } \mathrm{gr}(s) < n \text{ y } t = 0 \text{ o } \mathrm{gr}(t) < m\}$$
$$\text{y}\quad K[x]_{<m+n} := \{h \in K[x] :\ h = 0 \text{ o } \mathrm{gr}(h) < m+n\},$$

dada por

$$\begin{array}{rccc} \Phi: & K[x]_{<n} \times K[x]_{<m} & \to & K[x]_{<m+n} \\ & (s,t) & \mapsto & s\,f + t\,g, \end{array} \tag{1}$$

que está bien definida dado que $\mathrm{gr}(s\,f), \mathrm{gr}(t\,g) < m+n$ cuando $\mathrm{gr}(s) < n$ y $\mathrm{gr}(t) < m$ (¡Ojo que ésta es la razón por la cual las dimensiones van "cruzadas"!)

Estos dos espacios vectoriales tienen la misma dimensión $m+n$, y Φ es un isomorfismo si y sólo si su matriz en cualquier par de bases es inversible. Considerando las siguientes bases canónicas ordenadas de $K[x]_{<n} \times K[x]_{<m}$ y $K[x]_{<m+n}$ respectivamente,

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

la matriz $[\Phi]_{\mathcal{B},B'}$ de Φ en las bases $\mathcal{B}$ de $K[x]_{<n} \times K[x]_{<m}$ y $\mathcal{B}'$ de $K[x]_{<n+m}$ resulta ser

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

$$= \begin{array}{c} \overbrace{\phantom{\begin{array}{ccc}a&&\\&&\\&&\end{array}}}^{n} \quad \overbrace{\phantom{\begin{array}{ccc}b&&\\&&\\&&\end{array}}}^{m} \\ \left[\begin{array}{ccc|ccc} a_m & & & b_n & & \\ \vdots & \ddots & & \vdots & \ddots & \\ \vdots & & a_m & \vdots & & \ddots \\ \vdots & & \vdots & b_0 & & b_n \\ a_0 & & \vdots & & \ddots & \vdots \\ & \ddots & \vdots & & & \ddots \\ & & a_0 & & & b_0 \end{array}\right] \end{array} \begin{array}{l} \\ \\ \\ \\ \\ \\ \\ m+n \end{array} = S(f,g) \in K^{(m+n)\times(m+n)}.$$

O sea la matriz de Φ en las bases $\mathcal{B}$ y $\mathcal{B}'$ es justamente la matriz de Sylvester $S(f,g)$. Por lo tanto se tiene

$$\Phi \text{ isomorfimo} \iff \mathrm{Res}(f,g) = \det(S(f,g)) \neq 0,$$

o lo que es lo mismo, Φ no es un isomorfismo si y sólo si $\mathrm{Res}(f,g) = 0$. Esto es equivalente a decir que Φ no es un epimorfismo, o también que Φ no es un monomorfismo.

Podemos continuar ahora con la demostración del teorema.

Es decir existen $s \in K[x]_{<n}$ y $t \in K[x]_{<m}$ no ambos nulos tales que $sf + tg = 0$.

($\Rightarrow$) $\mathrm{Res}(f,g) = 0$ implica como vimos que Φ no es monomorfismo, es decir existen $s \in K[x]_{<n}$ y $t \in K[x]_{<m}$ no ambos nulos tales que $sf + tg = 0$. Por lo tanto

$$sf = -tg \Rightarrow\ s\frac{f}{\mathrm{mcd}(f,g)} = -t\frac{g}{\mathrm{mcd}(f,g)},$$

con lo cual, al ser $\dfrac{f}{\mathrm{mcd}(f,g)}$ y $\dfrac{g}{\mathrm{mcd}(f,g)}$ coprimos,

$$\frac{f}{\mathrm{mcd}(f,g)} \mid t \ \text{ y } \ \frac{g}{\mathrm{mcd}(f,g)} \mid s.$$

Pero si s es no nulo, $\mathrm{gr}(s) < \mathrm{gr}(g)$, y si t es no nulo, $\mathrm{gr}(t) < m$. Se concluye, como alguno de los dos es no nulo, que $\mathrm{gr}(\mathrm{mcd}(f,g)) \geq 1$ porque sino no se puede cumplir la divisibilidad.

($\Leftarrow$) Probaremos la contrarrecíproca. Si $\mathrm{Res}(f,g) \neq 0$, entonces Φ es un epimorfismo y por lo tanto existen s y t tales que $sf + tg = 1$, es decir f y g son coprimos.

□

1.1 Propiedades de la resultante y comentarios.

(0) $\mathrm{Res}(g,f) = (-1)^{mn}\mathrm{Res}(f,g)$, simplemente permutando las columnas de la matriz $\mathrm{Syl}(f,g)$ para obtener $\mathrm{Syl}(g,f)$.

(1) *La resultante es una combinación polinomial de* f *y* g: Existen polinomios $s,t \in K[x]$ no ambos nulos con $\mathrm{gr}(s) < n$ y $\mathrm{gr}(t) < m$ que satisfacen la identidad de Bézout

$$\mathrm{Res}(f,g) = s\,f + t\,g.$$

Esto se debe a que si $\mathrm{Res}(f,g) = 0$, entonces existen $s,t \in K[x]$, como arriba, con las condiciones requeridas que satisfacen $\mathrm{Res}(f,g) = 0 = s\,f + t\,g$, mientras que si $\mathrm{Res}(f,g) \neq 0$, entonces Φ es un epimorfismo y por lo tanto existen s,t con las condiciones requeridas tales que $\mathrm{Res}(f,g) = s\,f + t\,g$. Es más, es fácil identificar quiénes son esos polinomios s y t por la igualdad:

$$\mathrm{Res}(f,g) = \det \begin{array}{|cccc|cccc|l} \multicolumn{4}{c}{\overbrace{}^{n}} & \multicolumn{4}{c}{\overbrace{}^{m}} & \\ a_m & & & & b_n & & & & \\ \vdots & \ddots & & & \vdots & \ddots & & & \\ \vdots & & & a_m & \vdots & & \ddots & & \\ \vdots & & & \vdots & b_0 & & & b_n & m+n-1 \\ a_0 & & & \vdots & & \ddots & & \vdots & \\ & \ddots & & a_1 & & & \ddots & b_1 & \\ \hline x^{n-1}f & \dots & & f & x^{m-1}g & \dots & \dots & g & 1 \end{array} \tag{2}$$

que se obtiene simplemente notando que no se modifica el determinante si a la última fila se le suma x por la penúltima $+$ x^2 por la antepenúltima y así sucesivamente hasta sumarle x^{m+n-1} por la primera. Luego dividiendo este determinante como la suma de dos determinantes escribiendo la última fila como

$$(x^{n-1}f,\dots,f,x^{m-1}g,\dots,g) = (x^{n-1}f,\dots,f,0,\dots,0) + (0,\dots,0,x^{m-1}g,\dots,g),$$

y sacando luego f en factor común del primer determinante y g del segundo, se obtiene $\mathrm{Res}(f,g) = s\,f + t\,g$ con

$$s = \det \begin{array}{|cccc|cccc|l} \multicolumn{4}{c}{\overbrace{}^{n}} & \multicolumn{4}{c}{\overbrace{}^{m}} & \\ a_m & & & & b_n & & & & \\ \vdots & \ddots & & & \vdots & \ddots & & & \\ \vdots & & & a_m & \vdots & & \ddots & & \\ \vdots & & & \vdots & b_0 & & & b_n & m+n-1 \\ a_0 & & & \vdots & & \ddots & & \vdots & \\ & \ddots & & a_1 & & & \ddots & b_1 & \\ \hline x^{n-1} & \dots & & 1 & 0 & \dots & \dots & 0 & 1 \end{array},$$

$$t = \det \begin{array}{c|c|c} \overset{n}{} & \overset{m}{} & \\ \begin{array}{ccc} a_m & & \\ \vdots & \ddots & \\ \vdots & & a_m \\ \vdots & & \vdots \\ a_0 & & \vdots \\ & \ddots & a_1 \end{array} & \begin{array}{ccc} b_n & & \\ \vdots & \ddots & \\ \vdots & & \ddots \\ b_0 & & b_n \\ & \ddots & \vdots \\ & & \ddots \; b_1 \end{array} & \begin{array}{c} \\ \\ \\ m+n-1 \\ \\ \\ \end{array} \\ \hline 0 \;\; \ldots \;\; 0 & x^{m-1} \;\; \ldots \;\; \ldots \;\; 1 & 1 \end{array},$$

que claramente cumplen las condiciones de grado requeridas, desarrollando por la última fila, y son la única solución con esos grados.

(2) *La fórmula de Poisson:* La resultante es nula si y sólo si f y g comparten una raíz en $\overline{K}$. Esto queda de manifiesto en la siguiente descripción de la resultante como producto de diferencias de raíces de f y g, y que generaliza lo visto en el Ejemplo 1.2. Escribamos

$$f = a_m(x-\alpha_1)\cdots(x-\alpha_m),\ g = b_n(x-\beta_1)\cdots(x-\beta_n)\ \in \overline{K}[x].$$

Entonces

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

La segunda igualdad se obtiene simplemente desarrollando $g(\alpha_i)$ para $1 \le i \le m$. Por lo tanto mostremos la validez de la primera igualdad. Lo hacemos aquí para el caso en que f tiene todas sus raíces simples, es decir $\alpha_i \neq \alpha_j$ si $i \neq j$, recordando para ello el determinante de Vandermonde definido (en alguna de sus versiones) como

$$\mathcal{V}(\alpha_1,\ldots,\alpha_m) \;=\; \det \begin{pmatrix} \alpha_1^{m-1} & \ldots & \alpha_m^{m-1} \\ \vdots & & \vdots \\ \alpha_1 & \ldots & \alpha_m \\ 1 & \ldots & 1 \end{pmatrix} \;=\; \prod_{1\le i<j\le m} (\alpha_i - \alpha_j)$$

que es no nulo cuando $\alpha_i \neq \alpha_j$ para $i \neq j$. Consideremos entonces el siguiente producto de matrices

$$\begin{array}{c|c|c} \overset{n}{} & \overset{m}{} & \\ \begin{array}{c} n \\ \\ m \end{array} & \begin{array}{ccc|ccc} \multicolumn{3}{c|}{\multirow{2}{*}{Id_n}} & \multicolumn{3}{c}{\multirow{2}{*}{$\mathbf{0}$}} \\ & & & & & \\ \hline \alpha_1^{m+n-1} & \ldots & \alpha_1^m & \alpha_1^{m-1} & \ldots & 1 \\ \vdots & & & \vdots & & \vdots \\ \alpha_m^{m+n-1} & \ldots & \alpha_m^m & \alpha_m^{m-1} & \ldots & 1 \end{array} & \cdot \\ \hline \end{array} \begin{array}{c|c|c} \overset{n}{} & \overset{m}{} & \\ \begin{array}{ccc} a_m & & \\ \vdots & \ddots & \\ a_0 & & a_m \\ & \ddots & \vdots \\ & & a_0 \end{array} & \begin{array}{ccc} b_n & & \\ \vdots & \ddots & \\ b_0 & & b_m \\ & \ddots & \vdots \\ & & b_0 \end{array} & \begin{array}{c} \\ \\ m+n \\ \\ \\ \end{array} \end{array}$$

$$= \begin{array}{c|c|c} \overset{n}{} & \overset{m}{} & \\ \begin{array}{ccc} a_m & & \\ \vdots & \ddots & \\ * & \ldots & a_m \end{array} & * & \begin{array}{c} n \\ \\ \end{array} \\ \hline \mathbf{0} & \begin{array}{ccc} \alpha_1^{m-1}g(\alpha_1) & \ldots & g(\alpha_1) \\ \vdots & & \vdots \\ \alpha_m^{m-1}g(\alpha_m) & \ldots & g(\alpha_m) \end{array} & \begin{array}{c} \\ m \end{array} \end{array}$$

Calculando determinantes, queda, dado que son matrices triangulares en bloques,

$$\mathcal{V}(\alpha_1,\dots,\alpha_m)\,\mathrm{Res}(f,g) = a_m^n\, g(\alpha_1)\cdots g(\alpha_m)\,\mathcal{V}(\alpha_1,\dots,\alpha_m),$$

y el enunciado se obtiene simplificando $\mathcal{V}(\alpha_1,\dots,\alpha_m)$, que es no nulo en el caso considerado.

El caso general (la fórmula de Poisson vale independientemente de cómo sean las raíces de f) se obtiene o bien por un argumento de continuidad, o bien haciendo exactamente la misma construcción de producto de matrices, pero en lugar de considerar la matriz de Vandermonde de $(\alpha_1,\dots,\alpha_m)$ se considera la matriz de Vandermonde generalizada que tiene en cuenta la estructura de multiplicidades de las raíces de f. Es una buena ocasión para comentar que existen tales matrices, y su relación con la interpolación de Hermite, así como la matriz de Vandermonde clásica se corresponde con la interpolación de Lagrange.

La fórmula de Poisson tiene una consecuencia inmediata con respecto al algoritmo de división: Sea $f = q\,g + r$, con $k := \mathrm{gr}(r) < n = \mathrm{gr}(g)$, entonces $\mathrm{Res}(f,g) = (-1)^{mn} b_n^{m-k}\mathrm{Res}(g,r)$, ya que $f(\beta_i) = r(\beta_i)$, $1 \le i \le n$, implica

$$\begin{aligned}\mathrm{Res}(f,g) &= (-1)^{mn}\mathrm{Res}(g,f) = (-1)^{mn} b_n^m \prod_{1\le i\le n} f(\beta_i) = (-1)^{mn} b_n^{m-k} b_n^k \prod_{1\le i\le n} r(\beta_i)\\ &= (-1)^{mn} b_n^{m-k}\mathrm{Res}(g,r). \qquad (3)\end{aligned}$$

(3) El *discriminante*: El discriminante es un objeto fundamental en matemática, en particular en teória de números y en geometría algebraica, que indica cuándo un polinomio tiene raíces múltiples. Por ejemplo si $f = ax^2 + bx + c$ se tiene $\mathrm{Disc}(f) := b^2 - 4ac$ y si $f = x^3 + p\,x + q$, $\mathrm{Disc}(f) := -4p^3 - 27q^2$.
Sabemos que f tiene una raíz múltiple si y solo si f y f' tienen una raíz en común, es decir cuando $\mathrm{Res}(f,f') = 0$ (olvidemos aquí el caso $f' = 0$ para que tenga sentido considerar $\mathrm{Res}(f,f')$). Se define para $f = a_m x^m + \cdots + a_0 = a_m \prod_{1\le j\le m}(x-\alpha_j)$ con $a_m \neq 0$,

$$\mathrm{Disc}(f) := (-1)^{\frac{m(m-1)}{2}}\frac{1}{a_m}\mathrm{Res}(f,f') = a_m^{2m-2}\prod_{1\le i<j\le m}(\alpha_i-\alpha_j)^2,$$

donde la última igualdad vale por la fórmula de Poisson y la identidad

$$f' = a_m \sum_{1\le i\le m}\prod_{j\neq i}(x-\alpha_j).$$

Se tiene entonces

$$\mathrm{Disc}(f) = 0 \iff f \text{ tiene una raíz múltiple.}$$

(Las definiciones del discriminante pueden variar levemente según los textos, sobre todo su signo, pero nunca cambia su propiedad esencial. El signo está elegido aquí de manera que coincida para los casos de polinomios cuadráticos o cúbicos mencionados.)

(4) *La propiedad universal de la resultante*: Notemos que si los coeficientes de f y g pertenecen a un dominio íntegro R, entonces $\mathrm{Res}(f,g) \in R$ y además existen $s,t \in R[x]$ tales que $\mathrm{Res}(f,g) = s\,f + t\,g$, pues $\mathrm{Res}(f,g)$, s y t son determinantes de matrices con coeficientes en R. Así podemos considerar en lugar de polinomios f y g con coeficientes en R o K dados, polinomios F y G con coeficientes indeterminados $\boldsymbol{A} := (A_m,\dots,A_0)$ y $\boldsymbol{B} := (B_n,\dots,B_0)$:
Sean

$$F(\boldsymbol{A},x) := A_m x^m + \cdots + A_0 \text{ y } G(\boldsymbol{B},x) := B_n x^n + \cdots + B_0 \ \in\ \mathbb{Z}[\boldsymbol{A},\boldsymbol{B}][x],$$

y sea

$$\mathrm{Res}(F,G) := \det(S(F,G)) \in \mathbb{Z}[A_m,\dots,A_0,B_n,\dots,B_0],$$

definido como arriba por medio de la matriz de Sylvester.
Entonces existen $S,T \in \mathbb{Z}[\boldsymbol{A},\boldsymbol{B}][x]$ tales que $\mathrm{Res}(F,G) = S\,F + T\,G$, y además vale la siguiente "propiedad universal de la resultante": cada vez que se evalúan los coeficientes de F y G en $\boldsymbol{a} := (a_m,\dots,a_0) \in K^{m+1}$ y $\boldsymbol{b} := (b_n,\dots,b_0) \in K^{n+1}$, respectivamente, *con* $a_m \neq 0$ *y* $b_n \neq 0$, se tiene que $f_{\boldsymbol{a}}(x) := F(\boldsymbol{a},x)$ y $g_{\boldsymbol{b}}(x) := G(\boldsymbol{b},x)$ comparten una raíz en $\overline{K}$ si y sólo si $\mathrm{Res}(F,G)(\boldsymbol{a},\boldsymbol{b}) = 0$.
Evaluar los polinomios antes y calcular su resultante específica o calcular la resultante "genérica" y evaluar después da lo mismo, pues si $\mathrm{gr}(f_{\boldsymbol{a}}) = m$ y $\mathrm{gr}(g_{\boldsymbol{b}}) = n$, entonces vale que $\mathrm{Res}(f_{\boldsymbol{a}},g_{\boldsymbol{b}}) = \mathrm{Res}(F,G)(\boldsymbol{a},\boldsymbol{b})$ por como se obtiene la resultante como un determinante que solo involucra productos, sumas y restas de los coeficientes. Pero ojo, hay que evaluar eligiendo siempre $a_m \neq 0$ y $b_n \neq 0$ (o al menos uno de los dos, pensarlo) ya que si sin querer los dos polinomios evaluados bajan su grado, entonces $\mathrm{Res}(F,G)(\boldsymbol{a},\boldsymbol{b}) = 0$ mientras que $\mathrm{Res}(f_{\boldsymbol{a}},g_{\boldsymbol{b}})$, la que tendría que haberse calculado usando la matriz de Sylvester de tamaño correcto, será seguramente (o probablemente) no nula...

(5) *El espacio proyectivo como marco correcto*: La salvedad del inciso (4) que nos vimos forzados a considerar indica de alguna manera que el marco correcto para considerar la resultante no es "polinomios en $K[x]$ con raíces en $\overline{K}$" sino más bien "polinomios homogéneos en $K[x,y]$ con raíces en el espacio proyectivo $\mathbb{P}^1(\overline{K})$": Sean

$$\begin{aligned} F^h(\boldsymbol{A},x,y) :&= A_m x^m + A_{m-1}x^{m-1}y + \cdots + A_1 xy^{m-1} + A_0 y^m \quad \text{y} \\ G^h(\boldsymbol{B},x,y) :&= B_n x^n + B_{n-1}x^{n-1}y + \cdots + B_1 xy^{n-1} + B_0 y^n \ \in \mathbb{Z}[\boldsymbol{A},\boldsymbol{B}][x,y] \end{aligned}$$

las homogeneizaciones de los polinomios F,G del inciso (4), y definamos

$$\mathrm{Res}(F^h,G^h) := \mathrm{Res}(F,G) \in \mathbb{Z}[\boldsymbol{A},\boldsymbol{B}].$$

Entonces existen $S,T \in \mathbb{Z}[\boldsymbol{A},\boldsymbol{B}][x,y]$ tales que $\mathrm{Res}(F,G) = S\,F + T\,G$, y además vale la siguiente propiedad universal: cada vez que se evalúan los coeficientes de F^h y G^h en $\boldsymbol{a} = (a_m,\dots,a_0) \in \mathbb{P}^m(K)$ y $\boldsymbol{b} := (b_n,\dots,b_0) \in \mathbb{P}^n(K)$, se tiene que $f_{\boldsymbol{a}}(x,y) := F^h(\boldsymbol{a},x,y)$ y $g_{\boldsymbol{b}}(x,y) := G^h(\boldsymbol{b},x,y)$ comparten una raíz en $\mathbb{P}^1(\overline{K})$ si y sólo si $\mathrm{Res}(F^h,G^h)(\boldsymbol{a},\boldsymbol{b}) = 0$. El caso $a_m = 0$ y $b_n = 0$ que había que evitar antes se corresponde aquí con la raíz al infinito $(1:0) \in \mathbb{P}^1(\overline{K})$.

(6) *Generalización para polinomios en varias variables*: La resultante se generaliza para $n+1$ polinomios homogéneos en $n+1$ variables (Francis Macaulay $\sim$1902):
Sean $F_0,\dots,F_n$ polinomios homogéneos en $n+1$ variables $\boldsymbol{x} := (x_0,\dots,x_n)$ de grados totales respectivos $d_0,\dots,d_n$ y coeficientes indeterminados respectivos
$\boldsymbol{A}_0 := (A_{0,\boldsymbol{\gamma}}, |\boldsymbol{\gamma}| = d_0), \dots, \boldsymbol{A}_n := (A_{n,\boldsymbol{\gamma}}, |\boldsymbol{\gamma}| = d_n)$:

$$F_0(\boldsymbol{A}_0,\boldsymbol{x}) = \sum_{|\boldsymbol{\gamma}|=d_0} A_{0,\boldsymbol{\gamma}}\boldsymbol{x}^{\boldsymbol{\gamma}}, \quad \dots \quad , F_n(\boldsymbol{A}_n,\boldsymbol{x}) = \sum_{|\boldsymbol{\gamma}|=d_n} A_{n,\boldsymbol{\gamma}}\boldsymbol{x}^{\boldsymbol{\gamma}}.$$

Entonces existe un polinomio $\mathrm{Res}(F_0,\dots,F_n) \in \mathbb{Z}[\boldsymbol{A}_0,\dots,\boldsymbol{A}_n]$, multihomogéneo de grado $\prod_{j\neq i} d_j$ en las variables $\boldsymbol{A}_i$, que satisface

- $\mathrm{Res}(F_0,\dots,F_n) \in \langle F_0,\dots,F_n\rangle \subset \mathbb{Z}[\boldsymbol{A}_0,\dots\boldsymbol{A}_n][\boldsymbol{x}]$.
- Cada vez que se evalúan los coeficientes de F_i en $\boldsymbol{a}_i \in \mathbb{P}^{N_i}(K)$, $0 \le i \le n$, donde $N_i := \binom{d_i+n}{n} - 1$ es la cantidad de coeficientes que tiene el polinomio F_i, se tiene que $F_0(\boldsymbol{a}_0,\boldsymbol{x}),\dots,F_n(\boldsymbol{A}_n,\boldsymbol{x})$ comparten una raíz en $\mathbb{P}^n(\overline{K})$ si y sólo si

$$\mathrm{Res}(F_0,\dots,F_n)(\boldsymbol{a}_0,\dots,\boldsymbol{a}_n) = 0.$$

También existe una construcción matricial, desarrollada por Macaulay, para calcular esta resultante, pero lamentablemente no es tan inmediata ni sencilla como en el caso de dos polinomios homogéneos en dos variables.

2 Las subresultantes de dos polinomios univariados

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. $\mathrm{mcd}(f,g)=1$. ¿Habrá una condición similar para determinar cuál es el grado exacto del máximo común divisor $\mathrm{mcd}(f,g)$, y quién es? (otra que aplicar el algoritmo de Euclides para calcular el máximo común divisor). A esto responden en particular las subresultantes.

Definición 2.1 *Sean* $f=a_mx^m+\cdots+a_0, g=b_nx^n+\cdots+b_0\in K[X]$, *con* K *cuerpo, que satisfacen* $a_m\neq 0$ *y* $b_n\neq 0$.
El polinomio subresultante *de orden* d *de* f *y* g *está definido para* $0\le d<\min\{m,n\}$ *o* $d=\min\{m,n\}$ *si* $m\neq n$ *como*

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

Ejemplos 2.2
(1) Para $d=0$, *la identidad* (2) *muestra que* $\mathrm{Sres}_0(f,g)=\mathrm{Res}(f,g)$.
(2) $\mathrm{Sres}_m(f,g)=a_m^{n-m-1}f$ *si* $m<n$ *y* $\mathrm{Sres}_n(f,g)=b_n^{m-n-1}g$ *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

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

Observemos que $\mathrm{Sres}_1(f,g)=0\Leftrightarrow\alpha_1+\alpha_2=\beta_1+\beta_2$ *y* $\alpha_1\alpha_2=\beta_1\beta_2$, *es decir*
$(x-\alpha_1)(x-\alpha_2)=(x-\beta_1)(x-\beta_2)$*:* f *y* g *tienen las mismas raíces, o sea* $\mathrm{gr}(\mathrm{mcd}(f,g))=2$.
Mientras que si solo coincide una raíz, pongamos $\alpha_2=\beta_2$ *pero* $\alpha_1\neq\beta_1$, *o sea* $\mathrm{Res}(f,g)=0$, *y* $\mathrm{mcd}(f,g)=x-\alpha_2$, *entonces*

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

(4) Sea $f=a_mx^m+\cdots+a_0$ *y* $g=b_nx^n+\cdots+b_0$ *con* $m\le n$. *Entonces*

$$\mathrm{Sres}_{m-1}(f,g)=\det\begin{array}{|ccc|l}
\multicolumn{3}{c}{\overbrace{}^{n-m+1}} & \overbrace{}^{1}\\
a_m & & & b_n\\
\vdots & \ddots & & \vdots\\
a_{m-(n-m)} & \cdots & a_m & b_m\\
\hline
x^{n-m}f & \cdots & f & g
\end{array}\begin{array}{l}\\ \\ n-m+1\\ \\ 1\end{array}.$$

Si $f = a_m(x-\alpha_1)\cdots(x-\alpha_m)$ *tiene todas raíces simples, entonces se verifica rapidamente, desarrollando el determinante por la última fila, que* $\mathrm{Sres}_{m-1}(f,g)(\alpha_i) = a_m^{n-m+1} g(\alpha_i)$ *dado que se anula toda la última fila salvo el último término* $= g(\alpha_i)$. *Por lo tanto* $\mathrm{Sres}_{m-1}(f,g)$ *es el único polinomio de grado* $\leq m-1$ *que satisface las* m *condiciones* $\mathrm{Sres}_{m-1}(f,g)(\alpha_i) = a_m^{n-m+1} g(\alpha_i)$. *Por interpolación de Lagrange, éste es el polinomio*

$$\mathrm{Sres}_{m-1}(f,g) = a_m^{n-m+1} \sum_{1\leq i\leq m} g(\alpha_i) \frac{\prod_{j\neq i}(x-\alpha_j)}{\prod_{j\neq i}(\alpha_i-\alpha_j)}.$$

Observación 2.3 *Aunque no resulta inmediato de la definición,* $\mathrm{Sres}_d(f,g)$ *es siempre un polinomio de grado* $\leq d$ *(si no nulo) ya que es inmediato verificar que los coeficientes de los monomios* x^{d+1} *hasta* $x^{m+n-d-1}$ *son nulos pues se corresponden con determinantes de matrices con dos filas repetidas.*

Observación 2.4 *Se satisface la identidad de Bézout*

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

(descomponiendo la última fila de la matriz que define $\mathrm{Sres}_d(f,g)$ *como suma de dos filas:* $(x^{n-d-1},\ldots 1,0,\ldots,0)f + (0,\ldots,0,x^{m-d-1},\ldots,1)g)$ *).*
Por lo tanto

$$\mathrm{Sres}_d(f,g) \in \langle f,g\rangle, \tag{4}$$

el ideal de $K[x]$ *generado por* f *y* g. *Esto implica en particular que*

$$\mathrm{mcd}(f,g) \mid \mathrm{Sres}_d(f,g) \quad \text{para } 0\leq d < \min\{m,n\} \text{ o } d = \min\{m,n\} \text{ si } m\neq n. \tag{5}$$

La propiedad fundamental de las subresultantes, relacionada con este hecho, es la siguiente.

Teorema 2.5 *Sea* $k := \min\{d : \mathrm{Sres}_d(f,g) \neq 0\}$. *Entonces*

$$\mathrm{Sres}_k(f,g) = c\,\mathrm{mcd}(f,g) \quad \text{para algún } c\in K^\times.$$

Prueba.- Por la observacion (5) anterior, ya sabemos que $\mathrm{mcd}(f,g) \mid \mathrm{Sres}_k(f,g)$. Nos falta probar que $k \leq \mathrm{gr}(\mathrm{mcd}(f,g))$ para concluir que tienen mismo grado y por lo tanto uno es múltiplo del otro.

Seguimos aquí las líneas del desarrollo realizado para el estudio de la resultante. Para estudiar el máximo común divisor de f y g, nos gustaría introducir la transformación lineal $\widetilde{\Phi}_d$ definida por

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

generalizando la transformación lineal Φ introducida en (1) que coincide con Φ_0. Pero claro, 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 misma dimensión, olvidemos los monomios de grado $<d$: escribamos $h = q_{x^d}(h)\,x^d + r_{x^d}(h)$ por medio del algoritmo de división, donde $q_{x^d}(h)$ y $r_{x^d}(h)$ son el cociente y el resto de dividir h por x^d, y notemos que $\mathrm{gr}(q_{x^d}(h)) < m+n-2d$ cuando $\mathrm{gr}(h) < m+n-d$. Luego "corregimos" la transformación lineal $\widetilde{\Phi}_d$ anterior y definimos la transformación lineal Φ_d:

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

Como antes, Φ_d es un isomorfismo si y solo 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 $\mathcal{B}$ de $K[x]_{<n-d}\times K[x]_{<m-d}$ y $\mathcal{B}'$ de $K[x]_{<n+m-2d}$ resulta ser

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

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

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

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

tiene grado exactamente d ¿Quién es 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 $(s_{n-d-1},\dots,s_0,t_{m-d-1},\dots,t_0)$ 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}, respectivamente t_{m-d-k}, es el determinante de la matriz $[\Phi_d]_{\mathcal{B},B'}$ donde

se reemplazó la columna k, respectivamente $n-d+k$, por $(0,\dots,0,1)^t$. Pero notemos que

$$s_{n-d-1} = \det \begin{array}{|c|c|c|}
\multicolumn{1}{c}{\scriptstyle 1} & \multicolumn{1}{c}{\scriptstyle n-d-1} & \multicolumn{1}{c}{\scriptstyle m-d} \\ \hline
0 & & b_n \\
\vdots & a_m & \vdots \quad \ddots \\
\vdots & \vdots \quad \ddots & \vdots \qquad\quad b_n \\
\vdots & \vdots \qquad\quad a_m & \vdots \qquad\quad \vdots \\
\vdots & \vdots \qquad\quad \vdots & \vdots \qquad\quad \vdots \\
0 & a_{d+1-(n-d-2)} \quad \dots \quad a_{d+1} & b_{d+1-(m-d-1)} \quad \dots \quad b_{d+1} \\
1 & a_{d+1-(n-d-1)} \quad \dots \quad a_d & b_{d-(m-d-1)} \quad \dots \quad b_d
\end{array} \begin{array}{l} \\ \\ \\ \\ \\ \\ m+n-2d \end{array}$$

$$= \det \begin{array}{|c|c|c|}
\multicolumn{1}{c}{\scriptstyle n-d} & & \multicolumn{1}{c}{\scriptstyle m-d} \\ \hline
a_m & & b_n \\
a_{m-1} \quad a_m & & \vdots \quad \ddots \\
\vdots \quad \vdots \quad \ddots & & \vdots \qquad\quad b_n \\
\vdots \quad \vdots \qquad\quad a_m & & \vdots \qquad\quad \vdots \\
\vdots \quad \vdots \qquad\quad \vdots & & \vdots \qquad\quad \vdots \\
a_{d+1-(n-d-1)} \quad a_{d+1-(n-d-2)} \quad \dots \quad a_{d+1} & & b_{d+1-(m-d-1)} \quad \dots \quad b_{d+1} \\
1 \qquad\quad 0 \qquad\quad \dots \quad 0 & & 0 \qquad\quad \dots \quad 0
\end{array} \begin{array}{l} \\ \\ \\ \\ \\ \\ m+n-2d-1 \end{array}, \quad \begin{array}{l} \\ \\ \\ \\ \\ \\ 1 \end{array}$$

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

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

$$= \det \begin{array}{|c|c|}
\multicolumn{1}{c}{\scriptstyle n-d} & \multicolumn{1}{c}{\scriptstyle m-d} \\ \hline
a_m & b_n \\
\vdots \quad \ddots & \vdots \quad \ddots \\
\vdots \qquad\quad a_m & \vdots \qquad\quad b_n \\
\vdots \qquad\quad \vdots & \vdots \qquad\quad \vdots \\
a_{d+1-(n-d-1)} \quad \dots \quad a_{d+1} & b_{d+1-(m-d-1)} \quad \dots \quad b_{d+1} \\
x^{n-d-1} \quad \dots \quad 1 & 0 \qquad\quad \dots \quad 0
\end{array} \begin{array}{l} \\ \\ \\ \\ \\ m+n-2d-1 \end{array} \quad \begin{array}{l} \\ \\ \\ \\ \\ 1 \end{array}$$

y

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

$$= \det \begin{array}{|c|c|}
\multicolumn{1}{c}{\scriptstyle n-d} & \multicolumn{1}{c}{\scriptstyle m-d} \\ \hline
a_m & b_n \\
\vdots \quad \ddots & \vdots \quad \ddots \\
\vdots \qquad\quad a_m & \vdots \qquad\quad b_n \\
\vdots \qquad\quad \vdots & \vdots \qquad\quad \vdots \\
a_{d+1-(n-d-1)} \quad \dots \quad a_{d+1} & b_{d+1-(m-d-1)} \quad \dots \quad b_{d+1} \\
0 \qquad\quad \dots \quad 0 & x^{m-d-1} \quad \dots \quad 1
\end{array} \begin{array}{l} \\ \\ \\ \\ \\ m+n-2d-1 \end{array} \quad \begin{array}{l} \\ \\ \\ \\ \\ 1 \end{array}.$$

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

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

$$= \mathrm{Sres}_d(f,g).$$

Podemos seguir ahora con la demostración del teorema. Llamemos $h = \mathrm{mcd}(f,g)$. Usando que $\frac{f}{h}$ y $\frac{g}{h}$ son coprimos, y por lo tanto su resultante es no nula, la construcción de la sección anterior para la resultante muestra que existen únicos $s,t \in K[x]$ con $\mathrm{gr}(s) < \mathrm{gr}(\frac{g}{h}) = n - \mathrm{gr}(h)$ y $\mathrm{gr}(t) < \mathrm{gr}(\frac{f}{h}) = m - \mathrm{gr}(h)$ que satisfacen $1 = s\frac{f}{h} + t\frac{g}{h}$, o equivalentemente, $h = sf + tg$. Esto implica que $\Phi_{\mathrm{gr}(h)}$ es un monomorfismo, y por lo tanto un isomorfismo, con lo cual $c_{\mathrm{gr}(h)} \neq 0$ y en particular $\mathrm{Sres}_{\mathrm{gr}(h)}(f,g) \neq 0$. Por lo tanto $\mathrm{gr}(h) \geq k$ como se quería probar. En definitiva acabamos de probar que para $k = \min\{d : \mathrm{Sres}_d(f,g) \neq 0\}$, se tiene

$$\mathrm{Sres}_k(f,g) = c_k \mathrm{mcd}(f,g).$$

□

Más aún, el *Teorema fundamental de la sucesión de restos polinomiales* describe exactamente toda la sucesión de subresultantes $\mathrm{Sres}_0(f,g), \mathrm{Sres}_1(f,g), \ldots$ en función de los sucesivos restos que se obtienen cuando se realiza el algoritmo de Euclides para calcular $\mathrm{mcd}(f,g)$. Enunciado informalmente dice lo siguiente.

Teorema 2.6 *[Col1967, Th.1] [BrTr1971, Fund.Th.], [GCL1992, Th.7.4], [vzGG1999, Cor.6.48 y Th.11.13] Existe un resto r_i en el algoritmo de Euclides de f y g con $\mathrm{gr}(r_i) = d$ si y solo si $c_d(f,g) \neq 0$, y en ese caso $\mathrm{Sres}_d(f,g)$ es un múltiplo escalar de r_i. Más aún, todas las subresultantes son múltiplos escalares de los distintos restos que aparecen en el algoritmo de Euclides.*

Retomaremos este resultado al final de este texto, luego de presentar las sumas de Sylvester.

3 Sumas de Sylvester

Vimos que $\mathrm{Res}(f,g)$ satisface la fórmula de Poisson

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

Nos preguntamos cuál es la "fórmula de Poisson" correspondiente para $\mathrm{Sres}_d(f,g)$. Esto se puede responder mediante las sumas de Sylvester, introducidas por él también en [Syl1853].

Sean $A = \{\alpha_1, \ldots, \alpha_m\}$ y $B = \{\beta_1, \ldots, \beta_n\}$, conjuntos de elementos distintos dos a dos, o de indeterminadas distintas. Dados $0 \leq p \leq m$ y $0 \leq q \leq n$, la *suma doble* $\mathrm{Syl}_{p,q}(f,g)$ de f y g está definida como:

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

donde $\mathcal{R}(Y,Z) := \prod_{y\in Y, z\in Z}(y-z)$.
Se observa que $\mathrm{Syl}_{p,q}(A,B)$ es un polinomio en x de grado acotado por $p+q$, que está bien definido solo cuando los elementos de A son todos distintos, igual que los de B.
En lo que sigue asociamos a los conjuntos A y B los polinomios mónicos

$$f = a_m x^m + \cdots + a_0 = (x-\alpha_1)\cdots(x-\alpha_m),$$
$$g = b_n x^n + \cdots + b_0 = (x-\beta_1)\cdots(x-\beta_n)$$

con $a_m = 1 = b_n$, que recordamos tienen raíces simples.

Ejemplos 3.1 *A comparar con el Ejemplo 2.2(1-2).*
(1) $\mathrm{Syl}_{0,0}(A,B) = \mathrm{Res}(f,g)$.
(2) $\mathrm{Syl}_{m,0}(A,B) = f$ *(*$= \mathrm{Sres}_m(f,g)$ *si* $m<n$*)* *y* $\mathrm{Syl}_{0,n}(A,B) = g$ *(*$= \mathrm{Sres}_n(f,g)$ *si* $n<m$*)*.
(3) $\mathrm{Syl}_{m,n}(A,B) = \mathrm{Res}(f,g)\,f\,g$.

La suma doble se especializa para $p\le m$ y $q=0$ en la siguiente *suma simple*:

$$\begin{aligned}\mathrm{Syl}_p(A,B) &= (-1)^{p(m-p)} \sum_{A'\subset A,|A'|=p} \mathcal{R}(A\backslash A', B)\,\frac{\mathcal{R}(x,A')}{\mathcal{R}(A\backslash A', A')}\\ &= (-1)^{p(m-p)} \sum_{A'\subset A,|A'|=p} \Big(\prod_{\alpha\notin A'} g(\alpha)\Big)\,\frac{\mathcal{R}(x,A')}{\mathcal{R}(A\backslash A', A')},\end{aligned}$$

donde ya no importa que g tenga raíces simples o múltiples.

Ejemplos 3.2 *Para* $p=m-1$, $q=0$,

$$\begin{aligned}\mathrm{Syl}_{m-1}(A,B) &= (-1)^{m-1} \sum_{\substack{A'\subset A\\ |A'|=m-1}} \Big(\prod_{\alpha\notin A'} g(\alpha)\Big)\,\frac{\mathcal{R}(x,A')}{\mathcal{R}(A\backslash A', A')}\\ &= (-1)^{m-1} \sum_{1\le i\le m} g(\alpha_i)\frac{\prod_{j\neq i}(x-\alpha_j)}{\prod_{j\neq i}(\alpha_i-\alpha_j)}\\ &= (-1)^{m-1}\mathrm{Sres}_{m-1}(f,g) \quad \textit{si } m\le n,\ \textit{por el Ejemplo 2.2(4).}\end{aligned}$$

Sylvester observa en [Syl1853, Art.21] que esta conexión que observamos en los ejemplos entre las subresultantes y las sumas dobles (que están definidas únicamente para polinomios f,g con raíces simples), y en particular las sumas simples (definidas cuando f tiene raíces simples) vale en todos los casos: en ese caso las sumas dobles, o simples, describen las subresultantes en términos de las raíces de f y g, un análogo a la fórmula de Poisson para la resultante.

Teorema 3.3 *Sean* $1\le n\le m$ *y sean* p,q *con* $0\le p\le m$ *y* $0\le q\le n$ *tales que* $d := p+q$ *satisface* $1\le d<n$ *o eventualmente* $d=n$ *si* $n<m$*, entonces*

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

En particular,

$$\mathrm{Syl}_d(A,B) = (-1)^{d(m-d)}\mathrm{Sres}_d(f,g) \quad \textit{para } 0\le d<n\le m \textit{ o } d=n<m.$$

Notemos que esta descripción también incluye el caso $m > n$ dadas las simetrías

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

Como mencionado en la introducción, aparecieron desde 2003 varias demostraciones distintas de este hecho, que incluyen también descripciones de las sumas dobles para los parámetros p, q fuera del rango considerado en el teorema. Aquí nos concentraremos en una demostración muy natural via interpolación de polinomios simétricos para la descripción de la suma simple, en el caso particular $p := m-2$. Mencionamos al final como se obtiene en forma análoga para los casos $0 \le p \le m-2$, y también como conduce via una regla de intercambio a la descripción de todas las sumas dobles para valores arbitrarios de $0 \le p \le m$ y $0 \le q \le n$.

Teorema 3.4 *Sean $m, n \in \mathbb{N}$ arbitrarios. Entonces*

$$\mathrm{Syl}_{m-2}(A,B) = \begin{cases} \mathrm{Sres}_{m-2}(f,g) & si\ m-2 \le n, \\ 0 & si\ n < m-2. \end{cases}$$

La prueba de este teorema es consecuencia de describir a $\mathrm{Syl}_{m-2}(A,B)$ como un coeficiente de un polinomio interpolador adecuado, generalizando lo que ocurre en el caso $\mathrm{Syl}_{m-1}(A,B)$, que es directamente un polinomio interpolador.
Por definición,

$$\mathrm{Syl}_{m-2}(A,B) = \sum_{A' \subset A, |A'|=m-2} \Big(\prod_{\alpha \notin A'} g(\alpha) \Big) \frac{\mathcal{R}(x,A')}{\mathcal{R}(A \backslash A', A')}.$$

Lamentablemente, en este caso, los polinomios

$$\Big\{ \mathcal{R}(x,A') = \prod_{\alpha \in A'} (x-\alpha);\ A' \subset A,\ |A'| = m-2 \Big\}$$

ya no forman una base para los polinomios de grado $\le m-2$ (pues hay $\binom{m}{2}$ de ellos), al contrario de lo que ocurría en el caso de $\mathrm{Syl}_{m-1}(A,B)$ donde los polinomios

$$\Big\{ \mathcal{R}(x,A') = \prod_{\alpha \in A'} (x-\alpha)\,;\ A' \subset A,\ |A'| = m-1 \Big\}$$

sí formaban una base para los polinomios de grado $\le m-1$... Pero esto se puede solucionar "duplicando" las variables y considerando el espacio vectorial de los polinomios $S_{(2,m-2)} \subset K[x,y]$ *simétricos* y de grado en x y en y acotado por d, independientemente, y obteniendo una base de interpolación de Lagrange análoga a la que tenemos para $p = m-1$.

Lema 3.5 *[ChLo1996, Th.2.1.] Dado $A = \{\alpha_1, \ldots, \alpha_m\}$, el conjunto*

$$\mathcal{B} := \big\{ \mathcal{R}(x,A')\mathcal{R}(y,A')\,;\ A' \subset A,\ |A'| = m-2 \big\} \subset S_{(2,m-2)} \subset K[x,y]$$

es una base de $S_{(2,m-2)}$.
Más aún, todo polinomio simétrico $h(x,y) \in S_{(2,m-2)}$ satisface

$$h(x,y) = \sum_{A' \subset A, |A'|=m-2} h(A \backslash A') \frac{\mathcal{R}(x,A')\mathcal{R}(y,A')}{\mathcal{R}(A \backslash A', A')}$$

donde $h(A \backslash A') := h(\alpha_i, \alpha_j)$ si $A \backslash A' = \{\alpha_i, \alpha_j\}$.

Prueba.- Primero calculemos la dimensión $\dim_K(S_{(2,m-2)})$. Por el teorema fundamental de los polinomios simétricos elementales, todo polinomio simétrico en $K[x,y]$ es un polinomio en $e_1(x,y) = x+y$ y $e_2(x,y) = x\,y$, que son polinomios homogéneos de grado 1 en x y también en y. Por lo tanto para que h simétrico tenga grado acotado por $m-2$ tanto en x como en y, tiene que ser de la forma $h = \sum_{i,j} c_{i,j} e_1^i e_2^j$ con $i+j \le m-2$, es decir es un polinomio en e_1, e_2 de grado total $\le m-2$: esto tiene dimensión $\binom{m-2+2}{m-2} = \binom{m}{2}$.
Ahora bien, como en $\mathcal{B}$ tenemos también exactamente $\binom{m}{2} = \dim_K(S_{(2,m-2)})$ polinomios simétricos de grado $\le m-2$, alcanza con probar que son todos linealmente independientes. Sea

$$\sum_{A' \subset A, |A'|=m-2} c_{A'} \mathcal{R}(x, A') \mathcal{R}(y, A') = 0.$$

Evaluando esta identidad en cada $A \backslash A' = \{\alpha_i, \alpha_j\}$ con $i < j$, todos los términos se anulan excepto para $A' = A \backslash \{\alpha_i, \alpha_j\}$ donde da exactamente $c_{A'} \mathcal{R}(A \backslash A', A')$ y por lo tanto $c_{A'} = 0$ dado que $\mathcal{R}(A \backslash A', A') \neq 0$. Esto demuestra la independencia lineal, o sea $\mathcal{B}$ es base.
Finalmente, del mismo modo,

$$\begin{aligned} h(x,y) &= \sum_{A' \subset A, |A'|=m-2} c_{A'} \mathcal{R}(x, A') \mathcal{R}(y, A') \;\Rightarrow\; h(A \backslash A') = c_{A'} \mathcal{R}(A \backslash A', A') \\ &\Rightarrow\; c_{A'} = \frac{h(A \backslash A')}{\mathcal{R}(A \backslash A', A')} \\ &\Rightarrow\; h(x,y) = \sum_{A' \subset A, |A'|=m-2} h(A \backslash A') \frac{\mathcal{R}(x, A') \mathcal{R}(y, A')}{\mathcal{R}(A \backslash A', A')}. \end{aligned}$$

□

Corolario 3.6 *El único polinomio $h_{m-2}(x,y) \in S_{(2,m-2)}$ que satisface las $\binom{m}{2}$ condiciones*

$$h_{m-2}(\alpha_i, \alpha_j) = g(\alpha_i) g(\alpha_j) \quad \textit{para todo} \quad 1 \le i < j \le m$$

es el polinomio

$$h_{m-2}(x,y) = \sum_{|A'|=m-2} \Big(\prod_{\alpha \notin A'} g(\alpha) \Big) \frac{\mathcal{R}(x, A') \mathcal{R}(y, A')}{\mathcal{R}(A \backslash A', A')} \quad \in S_{(2,m-2)}.$$

Más aún,

$$\mathrm{Syl}_{m-2}(A,B)(y) = \mathrm{coeff}_{x^{m-2}}\big(h_{m-2}(x,y)\big).$$

Se deduce inmediatamente para el caso $\mathrm{gr}(g) = n \le m-2$ una parte del Teorema 3.4.

Corolario 3.7 *Si $n \le m-2$, entonces $h_{m-2}(x,y) = g(x)g(y)$, y por lo tanto*

$$\mathrm{Syl}_{m-2}(A,B) = \begin{cases} 0 & \textit{si } n < m-2 \\ g \;=\; \mathrm{Sres}_{m-2}(f,g) & \textit{si } n = m-2 \quad \textit{por el Ejemplo } 2.2(2). \end{cases}$$

Únicamente falta entonces resolver el caso $m-2 < n$ para terminar de probar el Teorema 3.4. Probamos a continuación una expresión matricial para el polinomio h_{m-2} en ese caso que permite deducirlo simplemente.

Lema 3.8 *Sea* $m-2 \leq n$. *Entonces*

$$h_{m-2}(x,y) = \frac{\det \begin{array}{|cccc|cc|} \multicolumn{4}{c}{\overbrace{}^{n-m+2}} & \multicolumn{2}{c}{\overbrace{}^{2}} & \\ a_m & & & & b_n & & \\ \vdots & \ddots & & & \vdots & b_n & n-m+2 \\ \vdots & & \ddots & & \vdots & \vdots & \\ a_{m-(n-m+1)} & \cdots & \cdots & a_m & b_{m-1} & b_m & \\ \hline x^{n-m+1}f(x) & \cdots & \cdots & f(x) & x\,g(x) & g(x) & 2 \\ y^{n-m+1}f(y) & \cdots & \cdots & f(y) & y\,g(y) & g(y) & \end{array}}{x-y}.$$

Prueba.- Es inmediato que el denominador a la derecha divide al numerador pues haciendo $x=y$ anula el numerador, luego la expresión a la derecha es un polinomio. Además es simétrico pues permutando x e y cambia el signo arriba y abajo. Falta ver que su grado en x (y por lo tanto en y) está acotado por $m-2$. Esto se ve de la misma manera que vimos que $\mathrm{gr}(\mathrm{Sres}_d(f,g)) \leq d$: el grado en x de la matriz del numerador está acotado por $m-1$ ya que es fácil verificar que los coeficientes de los monomios x^m hasta x^{n+1} son nulos pues se corresponden con determinantes de matrices con dos filas repetidas. Luego al dividir por el denominador $x-y$ el grado en x está acotado por $m-2$.
Finalmente verifiquemos que este polinomio interpola como h_{m-2} en $A\backslash A' = \{\alpha_i, \alpha_j\}$ para todo $1 \leq i < j \leq m$. En ese caso la expresión a la derecha da simplemente

$$a_m^{n-m+2}\frac{\alpha_i g(\alpha_i)g(\alpha_j) - \alpha_j g(\alpha_i)g(\alpha_j)}{\alpha_i - \alpha_j} = g(\alpha_i)g(\alpha_j) = h(\alpha_i, \alpha_j),$$

lo que termina la demostración.

□

Notemos que esta expresión matricial para $h_{m-2}(x,y)$ es muy parecida a la que define $\mathrm{Sres}_{m-2}(f,g)$. Simplemente hay que mirar el coeficiente en x^{m-2} de h_{m-2} para concluir la demostración completa del Teorema 3.4.

Proposición 3.9 *Sea* $m-2 \leq n$, *entonces*

$$\mathrm{Syl}_{m-2}(A,B) = \mathrm{Sres}_{m-2}(f,g).$$

Prueba.- Si llamamos $\delta(x,y)$ al determinante de la matriz del numerador en el Lema 3.8, tenemos

$$\mathrm{coeff}_{x^{m-2}}(h_{m-2}(x,y)) = \mathrm{coeff}_{x^{m-1}}(\delta(x,y)).$$

Pero

$$\mathrm{coeff}_{x^{m-1}}(\delta(x,y)) = \det \begin{array}{|cccc|cc|} \multicolumn{4}{c}{\overbrace{}^{n-m+2}} & \multicolumn{2}{c}{\overbrace{}^{2}} & \\ a_m & & & & b_n & & \\ \vdots & \ddots & & & \vdots & b_n & n-m+2 \\ \vdots & & \ddots & & \vdots & \vdots & \\ a_{m-(n-m+1)} & \cdots & \cdots & a_m & b_{m-1} & b_m & \\ \hline a_{m-1-(n-m+1)} & \cdots & \cdots & a_{m-1} & b_{m-2} & b_{m-1} & 2 \\ y^{n-m+1}f(y) & \cdots & \cdots & f(y) & y\,g(y) & g(y) & \end{array}$$

$$= \mathrm{Sres}_{m-2}(f,g)(y),$$

lo que concluye la demostración.

□

Comentarios.-
(1) Esta forma de calcular $\mathrm{Syl}_{m-2}(A,B)$ mediante interpolación de Lagrange simétrica se generaliza directamente por medio de la misma construcción al caso $\mathrm{Syl}_p(A,B)$, $0 \le p \le m-2$, considerando el espacio $S_{(m-p,p)}$ de polinomios simétricos en $m-p$ variables $x_1,\dots,x_{m-p}$ y grado $\le p$ en cada una de las variables, y su base

$$\mathcal{B} := \big\{\mathcal{R}(\{x_1,\dots,x_{m-p}\},A')\,;\, A'\subset A,\, |A'|=p\big\} \subset S_{(m-p,p)}.$$

En particular se obtiene

$$\mathrm{Syl}_d(A,B) = 0 \quad \text{para} \quad n < d < m-1. \tag{6}$$

(2) Esta interpolación simétrica también permite probar la relación entre todas las sumas dobles $\mathrm{Syl}_{p,q}(A,B)$ con $\mathrm{Syl}_d(A,B)$ para $0 \le d := p+q < \min\{m,n\}$, y también para los otros valores de p y q, mediante la para nada obvia *regla de intercambio* siguiente:

Lema 3.10 *Sean A con $|A|=m$, $0\le p\le m$ y B con $|B|=n\ge m-p$. Entonces*

$$\sum_{\substack{A'\subset A\\ |A'|=p}} \mathcal{R}(A\backslash A',B)\frac{\mathcal{R}(\{x_1,\dots,x_{m-p}\},A')}{\mathcal{R}(A\backslash A',A')} = \sum_{\substack{B'\subset B\\ |B'|=p}} \mathcal{R}(A,B\backslash B')\frac{\mathcal{R}(\{x_1,\dots,x_{m-p}\},B')}{\mathcal{R}(B',B\backslash B')}.$$

Esto se debe a que ambos son polinomios simétricos de grado $\le p$ en $x_1,\dots,x_{m-p}$. El de la izquierda es el polinomio que evaluado en $A\backslash A'$ vale $\mathcal{R}(A\backslash A',B)$, luego alcanza con probar que el de la derecha da lo mismo en $A\backslash A'$. Pero

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

y por lo tanto alcanza con probar que el polinomio simétrico y de grado $\le m-p$ en $x_1,\dots,x_p$ definido como

$$\sum_{\substack{B'\subset B\\ |B'|=p}} \frac{\mathcal{R}(\{x_1,\dots,x_p\},B\backslash B')}{\mathcal{R}(B',B\backslash B')}$$

es igual al polinomio 1. Esto es claro por interpolación simétrica de Lagrange ya que evaluando en todo $B'\subset B$ con $|B'|=p$ da 1. Los detalles de (1) y (2) se pueden ver en [KSV2015].

(3) Pero esta fórmula "à la Poisson" para las subresultantes solo es válida para polinomios con raíces simples. Hasta la fecha no hay una descripción de las subresultantes en término de raíces en el caso de polinomios con raíces múltiples.

Como consecuencia de la "fórmula de Poisson" descrita en el Teorema 3.3 para las subresultantes, y de la Identidad (6) se obtiene una demostración alternativa simple del resultado siguiente, clave para probar el Teorema Fundamental de la Sucesión de Restos Polinomiales de [Col1967, BrTr1971] enunciado informalmente en el Teorema 2.6. Aquí asumiremos que g tiene raíces simples, pero el resultado vale por continuidad para todo g.

Lema 3.11 *[GCL1992, Lem.7.1] Sea $f = q\,g + r$ con $\mathrm{gr}(r) =: k < n = \mathrm{gr}(g)$, y notemos por r_k el coeficiente principal de r. Entonces*

$$\mathrm{Sres}_d(f,g) = (-1)^{(m-d)(n-d)}\begin{cases} b_n^{m-k}\mathrm{Sres}_d(g,r) & \text{para} \quad 0\le d<k\\ b_n^{m-k}r_k^{n-k-1}r & \text{para} \quad d=k\\ 0 & \text{para} \quad k<d<n-1\\ b_n^{m-n+1}r & \text{para} \quad d=n-1.\end{cases}$$

Prueba.- La idea aquí es análoga a la de la Identidad (3), aunque hay que tener un poco de cuidado ya que las sumas de Sylvester están definidas para polinomios mónicos.
Notamos $f = a_m\widetilde{f}$, $g = b_n\widetilde{g}$ y $r = r_k\widetilde{r}$, donde $\widetilde{f}$, $g = b_n\widetilde{g}$ y $\widetilde{r}$ son mónicos. Observando que $f(\beta) = r(\beta) = r_k\widetilde{r}(\beta)$ para todo $\beta \in B$, y llamando C el conjunto de las k raíces de r, obtenemos del Teorema 3.3 para $d \leq n-1$,

$$\begin{aligned}
\mathrm{Sres}_d(f,g) &= a_m^{n-d}b_n^{m-d}\mathrm{Sres}_d(\widetilde{f},\widetilde{g}) \\
&= a_m^{n-d}b_n^{m-d}\mathrm{Syl}_{0,d}(A,B) \\
&= (-1)^{m(n-d)}a_m^{n-d}b_n^{m-d}\sum_{B'\subset B,|B'|=d}\Big(\prod_{\beta\notin B'}\widetilde{f}(\beta)\Big)\frac{\prod_{\beta\in B'}(x-\beta)}{\mathcal{R}(B',B\backslash B')} \\
&= (-1)^{m(n-d)}b_n^{m-d}\sum_{B'\subset B,|B'|=d}\Big(\prod_{\beta\notin B'}f(\beta)\Big)\frac{\prod_{\beta\in B'}(x-\beta)}{\mathcal{R}(B',B\backslash B')} \\
&= (-1)^{(m-k)(n-d)}(-1)^{k(n-d)}b_n^{m-d}\sum_{B'\subset B,|B'|=d}\Big(\prod_{\beta\notin B'}r_k\widetilde{r}(\beta)\Big)\frac{\prod_{\beta\in B'}(x-\beta)}{\mathcal{R}(B',B\backslash B')} \\
&= (-1)^{(m-k)(n-d)}b_n^{m-d}r_k^{n-d}\mathrm{Syl}_{0,d}(C,B) \\
&= (-1)^{m(n-d)}b_n^{m-d}r_k^{n-d}\mathrm{Syl}_{d,0}(B,C).
\end{aligned}$$

Pero por otro lado, para $k < n \leq m$, tenemos por el Teorema 3.3, la Identidad (6) y el Ejemplo 3.2,

$$\mathrm{Syl}_{d,0}(B,C) = \begin{cases} (-1)^{d(n-d)}\mathrm{Sres}_d(\widetilde{g},\widetilde{r}) & \text{para} \quad 0 \leq d \leq k \\ 0 & \text{para} \quad k < d < n-1 \\ (-1)^{n-1}\widetilde{r} & \text{para} \quad d = n-1. \end{cases}$$

Juntando la información, usando que $\mathrm{Sres}_d(g,r) = b_n^{k-d}r_k^{n-d}\mathrm{Sres}_d(\widetilde{g},\widetilde{r})$ y que $\mathrm{Sres}_k(\widetilde{g},\widetilde{r}) = \widetilde{r}$, obtenemos

$$\mathrm{Sres}_d(f,g) = \begin{cases} (-1)^{(m-d)(n-d)}b_n^{m-k}\mathrm{Sres}_d(g,r) & \text{para} \quad 0 \leq d < k \\ (-1)^{(m-k)(n-k)}b_n^{m-k}r_k^{n-k-1}r & \text{para} \quad d = k \\ 0 & \text{para} \quad k < d < n-1 \\ (-1)^{m-(n-1)}b_n^{m-n+1}r & \text{para} \quad d = n-1. \end{cases}$$

□

4 Personajes clásicos que fueron apareciendo en esta historia.

- Euclides, matemático griego, 325-265 AC, el "padre de la geometría".
- Gottfried Wilhelm Leibniz, filósofo y matemático alemán, 1646-1716.
- Gabriel Cramer, matemático suizo, 1704-1752.
- Leonhard Euler, físico y matemático suizo que ejerció en Rusia, 1707-1783, el "cíclope de la matemática".

- Etienne Bézout, matemático francés, 1730-1783.
- Alexandre-Théophile Vandermonde, químico, matemático y músico francés, 1735-1796.
- Joseph-Louis Lagrange, astrónomo y matemático italiano que ejerció en Francia, 1736-1813.
- Siméon-Denis Poisson, matemático francés, 1781-1840.
- Augustin-Louis Cauchy, matemático francés, 1789-1857.
- Carl Gustav Jacob Jacobi, matemático alemán, 1804-1851.
- James Joseph Sylvester, matemático inglés, 1814-1897.
- Charles Hermite, matemático francés, 1822-1901.
- Francis Sowerby Macaulay, matemático inglés, 1862-1937.
- Issai Schur, matemático ruso que ejerció en Alemania, 1875-1941.
- Bartel Leendert van der Waerden, matemático e historiador de la matemática holandés, 1903-1996.

References

[ChLo1996] Chen, William Y. C.; Louck, James D.. *Interpolation for symmetric functions.*, Adv. Math. 117 (1996), no. 1, 147–156.

[BrTr1971] Brown, W. S.; Traub, J. F. *On Euclid's algorithm and the theory of subresultants.* J. Assoc. Comput. Mach. 18 (1971), 505–514.

[Cha1994] Chardin, Marc. *Formules à la Macaulay pour les sous-résultants en plusieurs variables.* C. R. Acad. Sci. Paris Sér. I Math. 319 (1994), no. 5, 433–436.

[Cha1995] Chardin, Marc. *Multivariate subresultants.* J. Pure Appl. Algebra 101 (1995), no. 2, 129–138.

[Col1967] Collins, George. *Subresultants and Reduced Polynomial Remainder Sequences.* J. ACM 14, 1 (1967), 128–142.

[LaPr2003] Lascoux, Alain; Pragacz, Piotr. *Double Sylvester sums for subresultants and multi-Schur functions.* J. Symbolic Comput. 35 (2003), no. 6, 689–710.

[vzGG1999] von zur Gathen, Joachim; Gerhard, Jürgen. *Modern computer algebra.* Cambridge University Press, Cambridge, 1999.

[GCL1992] Geddes, Keith; Czapor, S.; Labahn, George. *Algorithms for Computer Algebra.* Kluwer Academic Publishers, 1992.

[GVe1990] González-Vega, Laureano. *A subresultant theory for multivariate polynomials.* Extracta Math. 5 (1990), no. 3, 150–152.

[GVe1991] González-Vega, Laureano. *Determinantal formulae for the solution set of zero-dimensional ideals.* J. Pure Appl. Algebra 76 (1991), no. 1, 57–80.

[KSV2015] Krick, Teresa; Szanto, Agnes; Valdettaro, Marcelo. *Understanding Sylvester sums via symmetric Lagrange interpolation.* Enviado (2015).

[Mac1902] Macaulay, Francis. *On some formulae in elimination.* Proc. London. Math. Soc. 3 (1902) 3–27.

[Mac1916] Macaulay, Francis. *The alegebraic theory of modular systems.* Cambridge U. Press, 1916.

[Syl1853] Sylvester, James Joseph. *On a theory of the syzygetic relations of two rational integral functions, comprising an application to the theory of Sturm's functions, and that of the greatest algebraical common measure.* Philosophical Transactions of the Royal Society of London, Part III (1853), 407–548. Appears also in Collected Mathematical Papers of James Joseph Sylvester, Vol. **1**, Chelsea Publishing Co. (1973) 429–586.

[vdW1931-1955] van der Waerden, Bartel Leendert. *Moderne Algebra. Vol. II.* Springer, 1era edición, 1931, 2da edición 1940, 3era edición 1955.