RESULTANTES Y DISCRIMINANTES

MARIANO SUÁREZ-ÁLVAREZ

Índice

Convengamos en que un polinomio nulo tiene grado $-\infty$.

1. Resultantes

Fijemos un cuerpo K. Si n, $m \geq 0$ y no son ambos simultáneamente nulos, y $f = a_nX^n + \cdots + a_0$ y $g = b_mX^M + \cdots + b_0$ son elementos no nulos de $K[X]$ de grados $\deg f \leq n$ y $\deg g \leq m$, la ***(n, m)-resultante de f y g*** es el determinante $\mathsf{Res}^K_{n,m}(f, g) \in K$ de la matriz de Sylvester

$$\mathsf{Syl}^K_{n,m}(f,g) = \begin{pmatrix} a_n & a_{n-1} & a_{n-2} & \cdots & 0 & 0 & 0 \\ 0 & a_n & a_{n-1} & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & a_1 & a_0 & 0 \\ 0 & 0 & 0 & \cdots & a_2 & a_1 & a_0 \\ b_m & b_{m-1} & b_{m-2} & \cdots & 0 & 0 & 0 \\ 0 & b_m & b_{m-1} & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & b_1 & b_0 & 0 \\ 0 & 0 & 0 & \cdots & b_2 & b_1 & b_0 \end{pmatrix}.$$

Si $n = m = 0$, entonces convenimos en poner $\mathsf{Res}_{n,m}(f, g) = 1$.

Explicitamente, la matriz $\mathsf{Syl}^K_{n,m}(f, g)$ es cuadrada con $(n + m)$ filas y columnas, y tiene coeficientes

$$\mathsf{Syl}^K_{n,m}(f,g)_{i,j} = \begin{cases} a_{n+i-j}, & \text{si } 1 \leq i \leq m \text{ y } i \leq j \leq n+i; \\ b_{i-j}, & \text{si } 1+m \leq i \leq n+m \text{ y } i-m \leq j \leq i; \\ 0, & \text{en cualquier otro caso} \end{cases}$$

Fecha: 4 de noviembre, 2014; compilado: 9 de mayo de 2015.

si i, $j \in \{1, \dots, n+m\}$. En particular, si $n = 0$ y $m \geq 1$ entonces la matriz $\mathsf{Syl}^K_{n,m}(f,g)$ es una matriz $m \times m$ diagonal con todos sus elementos diagonales iguales a a_0 y, en consecuencia, $\mathsf{Res}_{n,m}(f,g) = a_0^m$. De la misma forma, si $m = 0$ y $n \geq 1$, entonces $\mathsf{Res}_{n,m}(f,g) = b_0^n$.

Notemos que si L es una extensión de K, entonces $K[X] \subseteq L[X]$ y entonces podemos calcular $\mathsf{Res}^L_{n,m}(f,g)$, que es en principio un elemento de L, pero como la matriz $\mathsf{Syl}^L_{n,m}(f,g)$ coincide con $\mathsf{Syl}^K_{n,m}(f,g)$, tenemos que $\mathsf{Res}^L_{n,m}(f,g) = \mathsf{Res}^K_{n,m}(f,g)$ y que, en particular, $\mathsf{Res}^L_{n,m}(f,g)$ es un elemento de K. Así, podemos calcular la (n,m)-resultante de f y g vistos como polinomios con coeficientes en cualquier cuerpo que contenga a K. Como consecuencia de esto, escribiremos simplemente $\mathsf{Res}_{n,m}(f,g)$ y $\mathsf{Syl}_{n,m}(f,g)$ en lugar de $\mathsf{Res}^K_{n,m}(f,g)$ y $\mathsf{Syl}^K_{n,m}(f,g)$, eliminando el superíndice referido al cuerpo K. En particular, tenemos el siguiente resultado:

{prop:res:coefs}

Proposición 1. *Sean n, $m \geq 0$ y sean f y g dos elementos no nulos de $K[X]$. La (n,m)-resultante $\mathsf{Res}_{n,m}(f,g)$ es un elemento del subanillo de K generado por los coeficientes de f y de g.* □

Por ejemplo, si $n = 2$ y $m = 3$, es

$$\mathsf{Syl}_{2,3}(f,g) = \begin{pmatrix} a_2 & a_1 & a_0 & 0 & 0 \\ 0 & a_2 & a_1 & a_0 & 0 \\ 0 & 0 & a_2 & a_1 & a_0 \\ b_3 & b_2 & b_1 & b_0 & 0 \\ 0 & b_3 & b_2 & b_1 & b_0 \end{pmatrix}$$

y entonces

$$\begin{aligned} \mathsf{Res}_{2,3}(f,g) = a_0^3 b_3^2 + a_2 a_0^2 b_2^2 - 2a_2 a_0^2 b_1 b_3 - a_1 a_0^2 b_2 b_3 + a_2^2 a_0 b_1^2 - 2a_2^2 a_0 b_0 b_2 \\ - a_1 a_2 a_0 b_1 b_2 + 3a_1 a_2 a_0 b_0 b_3 + a_1^2 a_0 b_1 b_3 + a_2^3 b_0^2 \\ - a_1 a_2^2 b_0 b_1 + a_1^2 a_2 b_0 b_2 - a_1^3 b_0 b_3 \end{aligned}$$

El resultado más importante y en gran parte la razón por la que nos interesamos en la resultante de dos polinomios es el siguiente:

Teorema 2. *Sean n, $m \geq 0$ y sean f y g elementos no nulos de $K[X]$ de grados $\deg f = n$ y $\deg g = m$. Las siguientes afirmaciones son equivalentes:* {thm:res}

(*a*) *Es $\mathsf{Res}_{n,m}(f,g) = 0$.*
(*b*) *Los polinomios f y g tienen un divisor común no constante en $K[X]$.*
(*c*) *Los polinomios f y g tienen una raíz común en alguna extensión de K.*

Demostración. Si alguno de f o g es constante, entonces laas tres afirmaciones del enunciado son falsas, así que no hay nada que probar en ese caso. Podemos suponer en lo que sigue, entonces, que n, $m \geq 1$.

Si $k \geq 1$, escribimos $K[X]_{<k}$ al subespacio de $K[X]$ de los polinomios de grado menor que k. Consideremos la función lineal

$$C : (u,v) \in K[X]_{<m} \oplus K[X]_{<n} \longmapsto uf + vg \in K[X]_{<n+m}.$$

Es fácil ver que la matriz de C con respecto a las bases ordenadas

$$(X^{m-1},0),\ (X^{m-2},0),\ \dots,\ (X,0),\ (1,0),\\ (0,X^{n-1}),\ (0,X^{n-2}),\ \dots,\ (0,X),\ (0,1)$$

de $K[X]_{<m} \oplus K[X]_{<n}$ y $X^{n+m-1}, \dots, 1$ de $K[X]_{<n+m}$ es precisamente la matriz transpuesta de $\mathsf{Syl}_{n,m}(f,g)$.

$(a) \Rightarrow (b)$ Si $\mathsf{Res}_{n,m}(f,g) = 0$, entonces la función C tiene núcleo no nulo —ya que su matriz con respecto a esas bases tiene determinante nulo— y entonces existen $u \in K[X]_{<m}$ y $v \in K[X]_{<n}$ no simultáneamente nulos y tales que $uf + vg = 0$. Supongamos que f y g son coprimos. Como $g \mid vg = -uf$, esto implica que g divide a u y, como $\deg u < \deg g$, que de hecho $u = 0$. De la misma forma, es $f \mid uf = -vg$ y $\deg v < \deg f$, así que $v = 0$. Esto es imposible.

$(b) \Rightarrow (a)$ Sea $d \in K[X]$ un divisor común no constante de f y g, de manera que existen polinomios no nulos r, $s \in K[X]$ tales que $f = rd$ y $g = sd$. Como d tiene grado positivo, $\deg r < \deg f = n$ y $\deg s < \deg g = m$, y entonces $(s,-r) \in K[X]_{<m} \oplus K[X]_{<n}$ y $C(s,-r) = 0$. Como $\mathsf{Syl}_{n,m}(f,g)$ es la matriz de la función lineal C para una elección de bases de su dominio y codominio, esto implica que $\mathsf{Res}_{n,m}(f,g) = \det \mathsf{Syl}_{n,m}(f,g) = 0$.

$(b) \Rightarrow (c)$ Si $h \in K[X]$ es un divisor común no constante de f y g en $K[X]$ y L es una extensión de K que contiene una raíz de h, entonces claramente f y g tienen una raíz común en L.

$(c) \Rightarrow (b)$ Si L es una extensión de K y $\alpha \in L$ es una raíz común de f y de g, entonces el polinomio minimal $h \in K[X]$ de α sobre K es un divisor común no constante de f y g en $K[X]$. □

{prop:res:sim}

Proposición 3. *Sean n, $m \geq 0$ y sean f y g elementos no nulos de $K[X]$ de grados $\deg f \leq n$ y $\deg g \leq m$. Es*

$$\mathsf{Res}_{n,m}(f,g) = (-1)^{nm}\mathsf{Res}_{m,n}(g,f).$$

Demostración. Si alguno de f o g es constante, entonces el resultado es inmediato, así que podemos suponer que n, $m \geq 1$. La matriz $\mathsf{Syl}_{m,n}(g,f)$ se obtiene de $\mathsf{Syl}_{n,m}(f,g)$ permutando las filas de acuerdo a la permutación

$$\begin{pmatrix} 1 & \cdots & \cdots & \cdots & \cdots & n+m \\ n+1 & \cdots & n+m & 1 & \cdots & n \end{pmatrix}$$

que tiene exactamente nm inversiones[1], de manera que su signo es $(-1)^{nm}$. □

Al comienzo de esta sección, definimos la (n,m)-resultante $\mathsf{Res}_{n,m}(f,g)$ de dos polinomios f y g con $\deg f \leq n$ y $\deg g \leq m$. El siguiente resultado describe la forma en que aquélla varía cuando cambiamos n y m manteniendo esas condiciones.

{prop:res:var}

Proposición 4. *Sean n, $m \geq 0$ y sean $f = a_n X^n + \cdots + a_0$ y $g = b_m X^M + \cdots + b_0$ elementos no nulos de $K[X]$ de grados $\deg f \leq n$ y $\deg g \leq m$.*

[1] Recordemos que una inversión de una permutación $\sigma \in S_n$ de grado n es un par (i,j) con $1 \leq i < j \leq n$ y $\sigma(i) > \sigma(j)$. Si $\iota(\sigma)$ denota la cantidad de inversiones de σ, entonces el signo de σ es $\operatorname{sgn}\sigma = (-1)^{\iota(\sigma)}$.

(*i*) *Si* $\deg g \leq m' \leq m$, *entonces* $\mathsf{Res}_{n,m}(f,g) = a_n^{m-m'}\mathsf{Res}_{n,m'}(f,g)$.
(*ii*) *Si* $\deg f \leq n' \leq n$, *entonces* $\mathsf{Res}_{n,m}(f,g) = (-1)^{(n-n')m} b_m^{n-n'}\mathsf{Res}_{n',m}(f,g)$.
(*iii*) *Si* $\deg f < n$ *y* $\deg g < m$, *entonces* $\mathsf{Res}_{n,m}(f,g) = 0$.

Demostración. Si alguno de f o g es constante, entonces las tres afirmaciones son inmediatas, así que podemos suponer que no es ese el caso.

(i) Bastará que probemos que

$$\textit{si } \deg g < m, \textit{ entonces } \mathsf{Res}_{n,m}(f,g) = a_n \mathsf{Res}_{n,m-1}(f,g); \tag{1}$$ {eq:cl:1}

la afirmación (i) de la proposición entonces de una inducción en $m - m'$, cuyo paso inicial es precisamente (1).

Supongamos entonces que $\deg g < m$, de manera que $b_m = 0$. En el desarrollo de Laplace con respecto a la primera columna del determinante de la matriz $\mathsf{Syl}_{n,m}(f,g)$, el cofactor de la entrada $(1,1)$ es precisamente el determinante de la matriz $\mathsf{Syl}_{n,m-1}(f,g)$. Como ésa es la única entrada no nula de esa columna, es claro entonces que $\mathsf{Res}_{n,m}(f,g) = a_n \mathsf{Res}_{n,m-1}$. Esto prueba (1).

(ii) Esto es consecuencia inmediata de la combinación de la Proposición 3 y de la parte (i) de esta proposición, que acabamos de probar.

(iii) Si $\deg f < n$ y $\deg g < m$, la primera columna de la matriz $\mathsf{Syl}_{n,m}(f,g)$ tiene todas sus entradas nulas, así que el determinante de esa matriz es cero. □

{prop:res:red}

Proposición 5. *Sean* n, $m \geq 0$ *y sean* f *y* g *elementos no nulos de* $K[X]$ *de grados* $\deg f \leq n$ *y* $\deg g \leq m$.

(*i*) *Si* $n \geq m$ *y* $h \in K[X]$ *tiene grado* $\deg h \leq n - m$ *y* $f + hg \neq 0$, *entonces*

$$\mathsf{Res}_{n,m}(f,g) = \mathsf{Res}_{n,m}(f + hg, g).$$

(*ii*) *Si* $n \leq m$ *y* $h \in K[X]$ *tiene grado* $\deg h \leq m - n$ *y* $g + hf \neq 0$, *entonces*

$$\mathsf{Res}_{n,m}(f,g) = \mathsf{Res}_{n,m}(f, g + hf).$$

Demostración. Es inmediato ver que la afirmación (ii) se deduce de la (i) usando la Proposición 3, así que bastará que probemos (i). Más aún, como todo polinomio de grado menor que $n - m$ es suma de términos de la forma αX^i con $0 \leq i < n - m$, podemos suponer que, de hecho, $h = \alpha X^i$. Finalmente, si alguno de f o g es constante el resultado es inmediato, así que suponemos que no es ese el caso.

Supongamos entonces que $n \geq m$, que $0 \leq i < n - m$, que $\alpha \in K$ y que $h = \alpha X^i$. La matriz $\mathsf{Syl}_{n,m}(f + hg, g)$ se obtiene de la matriz $\mathsf{Syl}_{n,m}(f,g)$ haciendo operaciones de fila: para cada $j \in \{1, \ldots, m\}$ su fila j-ésima se obtiene de la de $\mathsf{Syl}_{n,m}(f,g)$ sumándole el producto de la fila $(n + j - i)$-ésima de esta última matriz multiplicada por α, y para cada $j \in \{m+1, \ldots, m+n\}$ la fila j-esima de $\mathsf{Syl}_{n,m}(f + hg, g)$ es la misma que la de $\mathsf{Syl}_{n,m}(f,g)$. Se sigue, entonces, que las matrices $\mathsf{Syl}_{n,m}(f,g)$ y $\mathsf{Syl}_{n,m}(f + hg, g)$ tienen el mismo determinante. □

{prop:res:roots}

Proposición 6. *Sean* n, $m \geq 0$ *y sean* $f = a_n X^n + \cdots + a_0$ *y* $g = b_m X^m + \cdots + b_0$ *elementos de* $K[X]$ *de grados* $\deg f = n$ *y* $\deg g = m$. *Si* E *es una extensión de* K, α_1, $\ldots$, α_n, β_1, $\ldots$, $\beta_m \in E$ *y* $f = a_n \prod_{i=1}^n (X - \alpha_i)$ *y* $g = b_n \prod_{i=1}^m (X - \beta_i)$

en $E[X]$*, entonces*

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

Demostración. Que los últimos tres miembros de la igualdad del enunciado son en efecto iguales es inmediato. Bastará entonces que probemos que el primero es igual al segundo. Podemos suponer que $n \geq 1$ y que $m \geq 1$, ya que en caso contrario el resultado es inmediato. Hacemos inducción con respecto a $n+m$, que es un entero mayor o igual que 2.

Si $n+m=2$, entonces $n=m=1$, las raíces de f y de g son $\alpha_1 = -a_0/a_1$ y $\beta_1 = -b_0/b_1$, y

$$\mathsf{Res}_{1,1}(f,g) = \det \begin{pmatrix} a_1 & a_0 \\ b_1 & b_0 \end{pmatrix} = a_1 b_0 - a_0 b_1 = a_1 b_1 (\alpha_1 - \beta_1),$$

que es la expresión deseada en este caso.

Supongamos ahora que $n+m > 2$ y, sin pérdida de generalidad, que $m \geq n$; en efecto, si fuese $m < n$ el razonamiento sería completamente simétrico. Existen q, $r \in K[X]$ tales que $g = qf + r$ y $\deg r < \deg f$.

Si $r = 0$, entonces f divide a g, así que —como f no es constante— sabemos del Teorema 2 que $\mathsf{Res}_{n,m}(f,g) = 0$. Por otro lado, si f divide a g tenemos que $g(\alpha_i) = 0$ para cada $i \in \{1,\dots,n\}$, de manera que por supuesto $a_n^m \prod_{i=1}^n g(\alpha_i) = 0$. Vemos así que la igualdad que queremos vale en este caso.

Supongamos, por el contrario, que $r \neq 0$, de manera que $0 \leq \deg r < n \leq m$. Si ponemos $m' = \deg r$, entonces

$$\mathsf{Res}_{n,m}(f,g) = \mathsf{Res}_{n,m}(f,qf+r) = \mathsf{Res}_{n,m}(f,r) = a_n^{m-m'} \mathsf{Res}_{n,m'}(f,r).$$

Como $n + m' < n + m$, la hipótesis inductiva nos dice que

$$\mathsf{Res}_{n,m'}(f,r) = a_n^{m'} \prod_{i=1}^n r(\alpha_i)$$

y entonces, como $g(\alpha_i) = q(\alpha_i)f(\alpha_i) + r(\alpha_i)$ para cada $i \in \{1,\dots,n\}$, es

$$\mathsf{Res}_{n,m}(f,g) = a_n^{m-m'} \mathsf{Res}_{n,m'}(f,r) = a_n^{m-m'} a_n^{m'} \prod_{i=1}^n r(\alpha_i) = a_n^m \prod_{i=1}^n g(\alpha_1).$$

Esto completa la inducción. □

{prop:res:fmla}

Proposición 7. *Sean* n, $m \geq 0$, *sean* $A_0, \dots, A_n, B_0, \dots, B_m$ *algebraicamente independientes sobre* $\mathbb{Q}$, *y consideremos el cuerpo* $\mathscr{K} = \mathbb{Q}(A_0,\dots,A_n,B_0,\dots,B_m)$ *y el anillo* $\mathscr{O} = \mathbb{Z}[A_0,\dots,A_n,B_0,\dots,B_m]$.

(*i*) *Si* $F = A_n X^n + \cdots + A_0$ *y* $G = B_m X^m + \cdots + B_0$, *dos elementos de* $\mathscr{K}[X]$, *entonces la* (n,m)*-resultante* $\mathsf{Res}_{n,m}(F,G)$ *pertenece a* $\mathscr{O}$.

(*ii*) *Si* $f = a_n X^n + \cdots + a_0$ *y* $g = b_m X^m + \cdots + b_0$ *son dos elementos de* $K[X]$ *y* $\phi : \mathscr{O} \to K$ *es el morfismo de anillos tal que* $\phi(A_i) = a_i$ *para cada* $i \in \{1,\dots,n\}$ *y* $\phi(B_i) = b_i$ *para cada* $i \in \{1,\dots,m\}$, *entonces*

$$\phi\big(\mathsf{Res}_{n,m}(F,G)\big) = \mathsf{Res}_{n,m}(f,g).$$

Demostración. Hacer. □

2. Discriminantes

Fijemos nuevamente un cuerpo K. Si $n \geq 1$ y $f = a_n X^n + \cdots + a_0$ es un elemento no constante de $K[X]$ de grado $\deg f = n$, ponemos

$$\Delta_n(f) = \frac{(-1)^{n(n-1)/2}}{a_n} \mathsf{Res}_{n,n-1}(f, f').$$

Como en el caso de las resultantes, el discriminante de un polinomio puede calcularse considerándolo como polinomio con coeficientes en cualquier cuerpo que efectivamente contenga a sus coeficientes.

{thm:disc}

Teorema 8. *Sea $f \in K[X]$ un polinomio no constante de grado $n \geq 1$. Entonces $\Delta_n(f) = 0$ si y solamente si f tiene una raíz doble en alguna extensión de K.*

Demostración. Sea $n' = \deg f'$ y sea a_n el coeficiente principal de f. De acuerdo a la Proposición 4, es

$$\mathsf{Res}_{n,n-1}(f, f') = a_n^{n-1-n'} \mathsf{Res}_{n,n'}(f, f'),$$

y de acuerdo al Teorema 2, el segundo miembro de esta igualdad se anula si y solamente si f y f' tienen un factor común no constante en $K[X]$ o, equivalentemente, si f tiene una raíz doble en alguna extensión. En vista de la definición de $\Delta_n(f)$, esta observación prueba el teorema. $\square$

A pesar de que en la definición de Δ_n hay un denominador, esto es solo aparente ya que se cancela. Una forma precisa de enunciar esto es la siguiente proposición.

{prop:disc:int}

Proposición 9. *Sea $n \geq 1$ y sean $A_0, \ldots, A_n$ algebraicamente independientes sobre $\mathbb{Q}$.*

(i) Si $\mathscr{K} = \mathbb{Q}(A_0, \ldots, A_n)$ y $F = A_n X^n + \cdots + A_0 \in \mathscr{K}[X]$, entonces

$$\Delta_n(F) \in \mathbb{Z}[A_0, \ldots, A_n].$$

(ii) Si $f = a_n X^n + \cdots + a_0 \in K[X]$ un polinomio no constante de grado $\deg f = n$ y $\phi : \mathbb{Z}[A_0, \ldots, A_n] \to K$ el morfismo de anillos tal que $\phi(A_i) = a_i$ para cada $i \in \{1, \ldots, n\}$, entonces

$$\phi\big(\Delta_n(F)\big) = \Delta_n(f).$$

Demostración. Para probar a afirmación (i) basta observar que la primera columna de la matriz $\mathsf{Syl}_{n,n-1}(F, F')$ tiene todas sus entradas divisibles por A_n, de manera que el determinante de esta matriz, $\mathsf{Res}_{n,n-1}(F, F')$, es un elemento de $\mathbb{Z}[A_0, \ldots, A_n]$ divisible por A_n.

(ii) Terminar. $\square$

La definición de $\Delta_n(f)$ que dimos se aplica a polinomio f de grado exactamente n. Sin embargo, la Proposición 9 implica que podemos extender esa definición a la situación en que f tiene grado *a lo sumo* n. En efecto, si $f = a_n X^n + \cdots + a_0$ es un elemento de $K[X]$ de grado a lo sumo n y $\phi : \mathbb{Z}[A_0, \ldots, A_n] \to K$ es el morfismo de anillos tal que $\phi(A_i) = a_i$ para cada $i \in \{1, \ldots, n\}$, entonces podemos definir $\Delta_n(f)$ poniendo

$$\Delta_n(f) = \phi\big(\Delta_n(F)\big),$$

con $F = A_n X^n + \cdots + A_0 \in \mathbb{Q}(A_0, \ldots, A_n)[X]$ como en aquella proposición. En efecto, la segunda parte de la proposición nos dice que esta definición y la original coinciden cuando el polinomio f tiene grado exactamente n.

Este detalle es mayormente de naturaleza técnica, y podemos precisar la forma en que $\Delta_n(f)$ depende de n.

{prop:disc:var}

Proposición 10. *Sea $n \geq 1$ y sea $f = a_n X^n + \cdots + a_0$ un elemento no constante de $K[X]$ de grado $\deg f \leq n$. Si $a_n = 0$, entonces*

$$\Delta_n(f) = a_{n-1}^2 \Delta_{n-1}(f).$$

Si además es $a_{n-1} = 0$, entonces $\Delta_n(f) = 0$.

Demostración. Hacer. □

{prop:disc:deriv}

Proposición 11. *Sean $n \geq 1$ y $f \in K[X]$ un polinomio de grado n. Si E es una extensión de K y $a_n \in K$, $\alpha_1, \ldots, \alpha_n \in E$ son tales que $f = a_n \prod_{i=1}^n (X - \alpha_i)$, entonces*

$$\Delta_n(f) = (-1)^{n(n-1)/2} a_n^{n-2} \prod_{i=1}^n f'(\alpha_i).$$

Demostración. Si $n' = \deg f'$, entonces $\mathsf{Res}_{n,n-1}(f, f') = a_n^{n-1-n'} \mathsf{Res}_{n,n'}(f, f')$, de acuerdo a la Proposición 4, y la Proposición 6 nos dice que

$$\mathsf{Res}_{n,n'}(f, f') = a_n^{n'} \prod_{i=1}^n f'(\alpha_i).$$

La igualdad que afirma la proposición sigue de estas dos observaciones y de la definición de $\Delta_n(f)$. □

{coro:disc:norm}

Corolario 12. *Si E/K es una extensión de cuerpos de grado n, $\alpha \in E$ es tal que $E = K(\alpha)$ y $f \in K[X]$ es el polinomio minimal de α sobre K, entonces*

$$\Delta_n(f) = (-1)^{n(n-1)/2} N_{E/K}(f'(\alpha)).$$

Aquí $N_{E/K}$ denota la aplicación norma de la extensión E/K; ver [Lan02, VI, §5].

Demostración. Sea $\bar{K}$ una clausura algebraica de E y sean $\alpha_1, \ldots, \alpha_r$ las raíces *distintas* de f en $\bar{K}$. Para cada $j \in \{1, \ldots, r\}$ hay un morfismo de cuerpos K-lineal $\sigma_j : E \to \bar{K}$ tal que $\sigma_j(\alpha) = \alpha_j$ y el conjunto $\{\sigma_1, \ldots, \sigma_r\}$ es de hecho el conjunto de todos los morfismos de cuerpos K-lineales de E en $\bar{K}$. Si $[E : K]_i$ denota el grado de inseparabilidad de la extensión E/K, entonces por definición es

$$N_{E/K}(f'(\alpha)) = \left(\prod_{j=1}^r \sigma_j(f'(\alpha)) \right)^{[E:K]_i} = \left(\prod_{j=1}^r f'(\alpha_j) \right)^{[E:K]_i}.$$

Como cada una de las raíces α_i de f tiene multiplicidad exactamente $[E : K]_i$ y f es mónico, usando esto y la igualdad de la Proposición 11 vemos inmediatamente que $\Delta_n(f) = (-1)^{n(n-1)/2} N_{E/K}(f'(\alpha))$, que es precisamente lo que queremos. □

3. Polinomios y revestimientos

Si $z \in \mathbb{C}$, escribimos $\mathrm{ev}_z : \mathbb{C}[Z] \to \mathbb{C}$ al morfismo de $\mathbb{C}$-álgebras tal que $\mathrm{ev}_z(Z) = z$, y $\mathrm{Ev}_z : \mathbb{C}[Z, X] \to \mathbb{C}[X]$ al morfismo de $\mathbb{C}$-álgebras tal que $\mathrm{Ev}_z(Z) = z$ y $\mathrm{Ev}_z(X) = X$.

{lema:disc:ev}

Lema 13. *Si $f = X^n + f_{n-1}X^{n-1} \cdots + f_0 \in \mathbb{C}[Z, X]$, con $f_0, \ldots, f_{n-1} \in \mathbb{C}[Z]$ y $z \in \mathbb{C}$, entonces*

$$\Delta_n\big(\mathrm{Ev}_z(f)\big) = \mathrm{ev}_z\big(\Delta_n(f)\big).$$

Demostración. Sean $A_0, \ldots, A_n$ algebraicamente independientes sobre $\mathbb{Q}$. Sean $\phi : \mathbb{Z}[A_0, \ldots, A_n] \to \mathbb{C}$ y $\Phi : \mathbb{Z}[A_0, \ldots, A_n] \to \mathbb{C}[Z]$ los morfismos de anillos tal es que $\phi(A_n) = 1$, $\phi(A_i) = f_i(z)$, $\Phi(A_n) = 1$ y $\Phi(A_i) = f_i$ para cada $i \in \{0, \ldots, n-1\}$. Es inmediato que el siguiente diagrama conmuta

$$\begin{tikzcd} & \mathbb{Z}[A_0, \ldots, A_n] \arrow[dl, "\Phi"'] \arrow[dr, "\phi"] & \\ \mathbb{C}[Z] \arrow[rr, "\mathrm{ev}_z"'] & & \mathbb{C} \end{tikzcd}$$

De acuerdo a la Proposición 9, si $F = A_nX^n + \cdots + A_0 \in \mathbb{Z}[A_0, \ldots, A_n][X]$, es

$$\Phi(\Delta_n(F)) = \Delta_n(f). \qquad (2)$$

{eq:phis}

Por otro lado, como $\mathrm{Ev}_z(f) = f_n(z)X^n + \cdots + f_0(z) \in \mathbb{C}[X]$, es

$$\phi(\Delta_n(F)) = \Delta_n(\mathrm{Ev}_z(f)).$$

De esto, de la igualdad que se obtiene aplicando el morfismo ev_z a ambos lados de (2) y de la conmutatividad del diagrama obtenemos el resultado deseado. □

{prop:fibers}

Proposición 14. *Sea $f = X^n + f_{n-1}X^{n-1} + \cdots + f_0 \in \mathbb{C}[Z, X]$, con coeficientes $f_0, \ldots, f_{n-1} \in \mathbb{C}[Z]$, y sea $\Delta = \Delta_n(f) \in \mathbb{C}[Z]$ el discriminante de f. Sea*

$$\Gamma_f = \{(z, w) \in \mathbb{C} \times \mathbb{C} : f(z, w) = 0\},$$

sea $p : \Gamma_f \to \mathbb{C}$ la restricción de la proyección $\pi_1 : (z, w) \in \mathbb{C} \times \mathbb{C} \mapsto z \in \mathbb{C}$, y consideremos el conjunto $S = \{z \in \mathbb{C} : \Delta(z) = 0\}$.

- *(i) Para cada $z \in \mathbb{C} \setminus S$, el conjunto $p^{-1}(z)$ tiene exactamente n elementos.*
- *(ii) Si $z_0 \in \mathbb{C} \setminus S$ y $(z_0, w_0) \in p^{-1}(z_0)$, entonces hay un abierto $U \subseteq \mathbb{C} \setminus S$ que contiene a z_0 y una función holomorfa $x : U \to \mathbb{C}$ tal que para cada $z \in U$ es $f(z, x(z)) = 0$.*

Demostración. (*i*) Sea $z \in \mathbb{C} \setminus S$. Es claro que si $w \in \mathbb{C}$, es $(z, w) \in p^{-1}(z)$ sii $f(z, w) = 0$ sii w es una raíz del polinomio $\mathrm{Ev}_z(f)$. Así, hay tantos puntos en la fibra $p^{-1}(z)$ como raíces distintas de este polinomio. El grado de $\mathrm{Ev}_z(f)$ es n y su discriminante, según el Lema 13, es igual a $\mathrm{ev}_z(\Delta_n(f))$, esto es, a $\Delta(z)$; como $z \notin S$, sabemos que este valor es no nulo y el Teorema 8 nos dice entonces que todas las raíces de $\mathrm{Ev}_z(f)$ son simples. Vemos de esta forma que $p^{-1}(z)$ tiene exactamente n elementos.

(*ii*) Sea $z_0 \in \mathbb{C} \setminus S$ y $(z_0, w_0) \in p^{-1}(z_0)$, de manera que $f(z_0, w_0) = 0$. Esto nos dice que $\mathrm{Ev}_{z_0}(f)$ se anula en w_0. Supongamos por un momento que $\frac{\partial f}{\partial X}(z_0, w_0) = 0$, esto es, que el polinomio $\mathrm{Ev}_{z_0}(f)' = \mathrm{Ev}_{z_0}(\frac{\partial f}{\partial X})$ también tiene un cero en w_0. En vista del Teorema 2 y la definición del discriminante, esto implica que $\Delta_n(\mathrm{Ev}_{z_0}(f)) = 0$, y el Lema 13 nos dice que entonces $\mathrm{ev}_{z_0}(\Delta_n(f)) = 0$, es decir, que $\Delta(z_0) = 0$. Como esto es absurdo, ya que $z_0 \notin S$, podemos concluir que, contra lo supuesto, es de hecho $\frac{\partial f}{\partial X}(z_0, w_0) \neq 0$.

El teorema de la función implicita para funciones holomorfas nos dice que existe un abierto $U \subseteq \mathbb{C}$ que contiene a z_0 y una función holomorfa $x : U \to \mathbb{C}$ tal que $f(z, x(z)) = 0$ para cada $z \in U$; ver [Car61, IV, Proposition 6.1]. Esto es precisamente lo que afirma el enunciado. □

{prop:cover}

Proposición 15. *Sea $f \in \mathbb{C}[Z, X]$, $p : \Gamma_f \to \mathbb{C}$ y $S \subseteq \mathbb{C}$ como en la Proposición 14. Si ponemos $\Gamma_f^\circ = p^{-1}(\mathbb{C} \setminus S)$ y denotamos $p^\circ : \Gamma_f^\circ \to \mathbb{C} \setminus S$ a la restricción de p a Γ_f°, entonces p° es un revestimiento de grado n.*

Demostración. Sea $z_0 \in \mathbb{C} \setminus S$. La primera parte de la Proposición 14 nos dice que hay que n números distintos $w_1, \ldots, w_n \in \mathbb{C}$ tales que $p^{-1}(z_0) = \{(z_0, w_i) : 1 \leq i \leq n\}$ y se deduce inmediatamente de la segunda parte que hay un abierto $U \subseteq \mathbb{C} \setminus S$ tal que $z_0 \in U$ y funciones holomorfas $x_1, \ldots, x_n : U \to \mathbb{C}$ tales que $x_i(z_0) = w_i$ y $f(z, x_i(z)) = 0$ para cada $i \in \{1, \ldots, n\}$ y cada $z \in U$.

Sea $\epsilon = \min\{|w_i - w_j| : 1 \leq i < j \leq n\}$, que es un número positivo, y sea $\delta \in (0, \frac{1}{8}\epsilon)$ tal que la bola $B = B_\delta(z_0)$ está contenida en U y es $|x_i(z) - w_i| < \frac{1}{4}\epsilon$ para cada $z \in B$ y cada $i \in \{1, \ldots, n\}$. Sean $\tilde{x}_1, \ldots, \tilde{x}_n : B \to \mathbb{C} \times \mathbb{C}$ las funciones dadas por $\tilde{x}_i(z) = (z, x_i(z))$ para cada $z \in B$ y cada $i \in \{1, \ldots, n\}$. Si $1 \leq i < j \leq n$ y z, $z' \in B$, es

$$\begin{aligned}
&\|(z_0, w_i) - \tilde{x}_i(z)\|_1 + \|\tilde{x}_i(z) - \tilde{x}_j(z')\|_1 + \|\tilde{x}_j(z') - (z_0, w_j)\|_1 \\
&\qquad \geq \|(z_0, w_i) - (z_0, w_j)\|_1 = |w_i - w_j| > \epsilon,
\end{aligned}$$

así que

$$\begin{aligned}
\|\tilde{x}_i(z) - \tilde{x}_j(z')\|_1 &> \epsilon - \|(z_0, w_i) - \tilde{x}_i(z)\|_1 - \|\tilde{x}_j(z') - (z_0, w_j)\|_1 \\
&= \epsilon - |z_0 - z| - |w_i - x_i(z)| - |z' - z_0| - |x_j(z') - w_j| \\
&> \epsilon - 2\delta - 2\tfrac{1}{4}\epsilon > \tfrac{1}{4}\epsilon > 0.
\end{aligned}$$

Esto nos dice que si ponemos $V_i = \tilde{x}_i(B)$ para cada $i \in \{1, \ldots, n\}$, los conjuntos $\{V_1, \ldots, V_n\}$ son disjuntos dos a dos.

Es claro que $V_i \subseteq p^{-1}(B)$ para cada $i \in \{1, \ldots, n\}$. Sea $(z, w) \in p^{-1}(B)$. Como $z \in B$ y $f(z, w) = 0$, w es una raíz del polinomio $\mathrm{Ev}_z(f)$, que tiene grado n. Como sabemos que $f(z, x_i(z)) = 0$ para cada $i \in \{1, \ldots, n\}$ y que $x_i(z) \neq x_j(z)$ si $1 \leq i < j \leq n$, las raíces de $\mathrm{Ev}_z(f)$ son los números $x_1(z), \ldots, x_n(z)$ y, en consecuencia, existe $k \in \{1, \ldots, n\}$ tal que $w = x_k(z)$. Así, $(z, w) = \tilde{x}_k(z) \in V_k$. Vemos de esta forma que $p^{-1}(B) = \bigsqcup_{i=1}^n V_i$.

Sea $i \in \{1, \ldots, n\}$ y supongamos que $(z, w) \in p^{-1}(B) \cap (\mathbb{C} \times B_{\epsilon/4}(w_i))$. Como $(z, w) \in p^{-1}(B)$, sabemos ya que existe $j \in \{1, \ldots, n\}$ tal que $w = x_j(z)$ y, como $(z, w) \in \mathbb{C} \times B_{\epsilon/4}(w_i)$, es $|x_j(z) - w_i| < \frac{1}{4}\epsilon$. Si fuese $i \neq j$, tendríamos que

$$|x_j(z) - w_i| \geq |w_i - w_j| - |x_j(z) - w_j| > \epsilon - \tfrac{1}{4}\epsilon = \tfrac{3}{4}\epsilon,$$

lo que es absurdo. Vemos así que necesariamente es $i = j$ y, entonces, que

$$V_i = p^{-1}(B) \cap (\mathbb{C} \times B_{\epsilon/4}(w_i)).$$

Esto muestra que V_i es un abierto de Γ_f y, como está contenido en Γ_f°, también de este subespacio.

Sea otra vez $i \in \{1, \dots, n\}$ y sea $p_i : V_i \to B$ la restricción a V_i de la proyección $p : \Gamma_f \to \mathbb{C}$. Es inmediato verificar que p_i y x_i son funciones mutuamente inversas y continuas, así que en particular p_i es un homeomorfismo. Esto completa la prueba de que $p^\circ : \Gamma_f^\circ \to \mathbb{C} \setminus S$ es un revestimiento; ver [Mun75, Ch. 9, §53]. Como cada fibra tiene exactamente n puntos, el grado de ese revestimiento es n. □

El revestimiento construido en la Proposición 15 no es necesariamente conexo. Por ejemplo, sea $f = (X - Z - 1)(X - Z) \in \mathbb{C}[Z, X]$, que tiene grado 2 en tanto polinomio en X. Su discriminante es $\Delta_2(f) = 1$, de manera que $S = \emptyset$, y es fácil verificar que el espacio $\Gamma_f^\circ \subset \mathbb{C} \times \mathbb{C}$ tiene exactamente dos componentes conexas.

4. Prolongación analítica

Un ***elemento de función meromorfa*** es un par (U, x) con $U \subseteq \mathbb{C}$ un abierto conexo y $x : U \to \mathbb{C}$ una función meromorfa. Si $z_0 \in \mathbb{C}$ y (U, x) es un elemento de función meromorfa tal que $z_0 \in U$, entonces decimos que (U, x) es un ***elemento de función meromorfa definido alrededor de z_0***. Escribimos $\mathscr{M}(z_0)$ al conjunto de los elementos de funciones meromorfas definidos alrededor de z_0.

Fijemos $z_0 \in \mathbb{C}$. Si (U, x), $(V, y) \in \mathscr{M}(z_0)$, decimos que (U, x) y (V, y) ***tienen el mismo germen en z_0*** si existe un abierto $W \subseteq U \cap V$ tal que $z_0 \in W$ y $x|_W = y|_W$, y en ese caso escribimos $(U, x) \sim_{z_0} (V, y)$. Es inmediato verificar que esto define una relación de equivalencia $\sim_{z_0}$ en el conjunto $\mathscr{M}(z_0)$. Si $(U, x) \in \mathscr{M}(z_0)$, escribimos $[U, x]_{z_0}$ a su clase de equivalencia con respecto a esta relación; llamamos a $[U, x]_{z_0}$ el ***germen*** del elemento (U, x) en z_0.

Sea $I = [0, 1]$, sea $\gamma : I \to \mathbb{C}$ una curva continua y supongamos que para cada $t \in I$ tenemos un elemento de función meromorfa $(U_t, x_t) \in \mathscr{M}(\gamma(t))$ de manera tal que

para cada $t \in I$ existe $\delta > 0$ tal que si $s \in I \cap B_\delta(t)$ se tiene que $\gamma(s) \in U_t$ y $[U_t, x_t]_{\gamma(s)} = [U_s, x_s]_{\gamma(s)}$.

Decimos entonces que la familia $((U_t, x_t))_{t \in I}$ es una ***continuación analítica de funciones meromorfas a lo largo de la curva γ*** o, simplemente, que es una ***continuación a lo largo de γ***.

Proposición 16. *Sea $\gamma : I \to \mathbb{C}$ una curva y sean $((U_t, x_t))_{t \in I}$ y $((V_t, y_t))_{t \in I}$ continuaciones analíticas de funciones meromorfas a lo largo de γ.*

Si $[U_0, x_0]_{\gamma(0)} = [V_0, y_0]_{\gamma(0)}$, entonces $[U_t, x_t]_{\gamma(t)} = [V_t, y_t]_{\gamma(t)}$ para todo $t \in I$.

Demostración. Hacer □

Sea (U, x) un elemento de función meromorfa y sea $\Omega \subseteq \mathbb{C}$ un abierto conexo que contiene a U. Decimos que (U, x) ***admite continuación irrestricta en Ω*** si para cada curva $\gamma : I \to \Omega$ tal que $\gamma(0) \in U$ existe una continuación analítica de funciones meromorfas $((U_t, x_t))_{t\in I}$ tal que $[U_0, x_0]_{\gamma(0)} = [U, x]_{\gamma(0)}$.

Proposición 17. *Sea (U, x) un elemento de función meromorfas y sea $\Omega \subseteq \mathbb{C}$ un abierto conexo que contiene a U y en el que (U, x) admite continuación irrestricta. Sean $z_0 \in U$ y $z_1 \in \Omega$, sean γ, $\eta : I \to \Omega$ dos curvas tales que $z_0 = \gamma(0) = \eta(0)$ y $z_1 = \gamma(1) = \eta(1)$, y sean $((U_t, x_t))_{t\in I}$ y $((V_t, y_t))_{t\in I}$ continuaciones analíticas de funciones meromorfas a lo largo de γ y η, respectivamente, tales que $[U_0, x_0]_{z_0} = [V_0, y_0]_{z_0} = [U, x]_{z_0}$. Si las curvas γ y η son homotópicas relativamente a sus extremos en Ω, entonces $[U_1, x_1]_{z_1} = [V_1, y_1]_{z_1}$.*

Demostración. Hacer □

En general, es muy difícil decidir si un elemento de función meromorfa admite o no prolongaciones analíticas. En la situación en la que estamos interesados, sin embargo, esto es automático:

{prop:prol:mu}

Proposición 18. *Sea $f = X^n + f_{n-1}X^{n-1} + \cdots + f_0 \in \mathbb{C}[Z, X]$, con coeficientes f_0, …, $f_{n-1} \in \mathbb{C}[Z]$, sea $\Delta = \Delta_n(f) \in \mathbb{C}[Z]$ el discriminante de f y sea $S = \{z \in \mathbb{C} : \Delta(z) = 0\}$. Sea $z_0 \in \mathbb{C} \setminus S$ y sean $U \subseteq \mathbb{C} \setminus S$ un abierto conexo que contiene a z_0 y $x : U \to \mathbb{C}$ una función holomorfa tal que $f(z, x(z)) = 0$ para todo $z \in U$. Si $\mathscr{M}(U)$ es el cuerpo de las funciones meromorfas en U y $\mathbb{C}(z, x)$ es el subcuerpo de $\mathscr{M}(U)$ generado por $\mathbb{C}(z)$ y la función x, entonces todo elemento de $\mathbb{C}(z, x)$ admite prolongación analítica irrestricta en $\mathbb{C} \setminus S$.*

Demostración. Hacer □

Referencias

[Car61] Henri Cartan, *Théorie élémentaire des fonctions analytiques d'une ou plusieurs variables complexes*, Avec le concours de Reiji Takahashi, Enseignement des Sciences. Hermann, Paris, 1961 (French). MR0147623 (26 #5138)

[Lan02] Serge Lang, *Algebra*, 3rd ed., Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York, 2002. MR1878556 (2003e:00003)

[Mun75] James R. Munkres, *Topology: a first course*, Prentice-Hall, Inc., Englewood Cliffs, N.J., 1975. MR0464128 (57 #4063)