Funciones sin primitiva elemental

Carlos Ivorra
(http://www.uv.es/ivorra)

1 Introducción

La función de densidad de la distribución normal (con media 0 y desviación típica 1) viene dada por la función

$$f(t) = \frac{1}{\sqrt{2\pi}}\, e^{-t^2/2},$$

la celebérrima "campana de Gauss". Esto significa que la probabilidad de que una variable aleatoria con dicha distribución tome su valor en un intervalo $[a, b]$ viene dada por la integral

$$\frac{1}{\sqrt{2\pi}} \int_a^b e^{-t^2/2}\, dt.$$

En la práctica, estas integrales se calculan con la ayuda de tablas (o, más modernamente, de ordenadores), porque, como todos los libros de estadística indican, la función $e^{-t^2/2}$ "no se puede integrar", obviamente, no en el sentido de que no exista la integral (todas las funciones continuas tienen integral), sino en el sentido de que no existe ninguna fórmula "elemental", es decir, en términos de polinomios, raíces, senos, cosenos, exponenciales, logaritmos, etc., que determine una función $F(t)$ tal que $F' = f$.

Lo que no hacen los libros de estadística (ni prácticamente ningún libro) es explicar por qué esto es así. A lo sumo, remiten a un trabajo esotérico de Liouville al respecto. El objeto de este artículo es demostrar precisamente que la función $e^{-t^2/2}$, al igual que otras muchas funciones sencillas, no tiene primitiva elemental.

Para ello, el primer paso obligado es dar una definición rigurosa de "función elemental", y queremos hacerlo de tal forma que sea lo suficientemente simple como para que podamos operar con ella en teoría y, a la vez, lo suficientemente amplia como para que recoja a cualquier función del estilo de

$$f(x) = \frac{x^5 - \operatorname{sen}^4(\sqrt[3]{x^9+7} + \ln x)}{e^{x^4-3x} + \tan x},$$

es decir, a cualquier función que pueda admitirse como "solución explícita" de una integral dada.

En realidad, la definición que daremos será especialmente "generosa", en el sentido de que admitiremos como funciones elementales a algunas funciones para las que sería cuestionable si merecen ser consideradas como tales, pero esto no debe importarnos, ya que nuestra definición está orientada a probar un resultado negativo: cuanto más amplia

sea nuestra definición de función elemental, más potente será la afirmación de que una función dada no admite una primitiva elemental.

Por razones técnicas tendremos que trabajar con funciones de variable compleja, así que dedicaremos la sección 2 a introducir el concepto de función elemental compleja (y, más en general, una definición algebraica abstracta de función elemental) para, posteriormente, definir en la sección 3 el concepto de función elemental real, que será, según veremos, todo lo amplio que cabría exigir (e incluso más).

Para seguir la prueba, el lector deberá estar familiarizado con las funciones meromorfas y con la teoría básica de extensiones de cuerpos. Las aplicaciones a integrales de funciones algebraicas requerirán además algunos resultados básicos de la teoría de cuerpos de funciones algebraicas de una variable.

2 Funciones elementales

Si $D \subset \mathbb{C}$ es un *dominio,* (un abierto conexo), llamaremos $\mathcal{M}(D)$ al conjunto de todas las funciones *meromorfas* $f : D \longrightarrow \mathbb{C}^\infty$, es decir, funciones definidas en D, que toman el valor ∞ a lo sumo en un conjunto discreto de puntos (llamados *polos* de la función), sin puntos de acumulación en D, fuera del cual son derivables, y de modo que son continuas en los polos (lo que quiere decir que $f(z)$ tiende a ∞ cuando la z tiende a un polo).

Es conocido que $\mathcal{M}(D)$ es un cuerpo, es decir, que al sumar, restar, multiplicar y dividir funciones meromorfas, obtenemos de nuevo una función meromorfa.

Esto debe ser bien entendido: si f, $g \in \mathcal{M}(D)$, la unión de los conjuntos de polos de f y g es un cerrado discreto en D (en particular no es todo D), luego su complementario es un abierto $D_0 \subset D$ no vacío. Las restricciones $f|_{D_0}$ y $g|_{D_0}$ son funciones *holomorfas* en D_0, es decir funciones meromorfas sin polos, por lo que podemos definir puntualmente las funciones $f|_{D_0} + g|_{D_0}$ y $f|_{D_0}g|_{D_0}$. La clave es que puede probarse que estas funciones se extienden de forma única a funciones meromorfas en D, que son las funciones a las que llamamos $f + g$ y fg respectivamente.

Así pues, debemos tener presente que las igualdades

$$(f + g)(z) = f(z) + g(z), \qquad (fg)(z) = f(z)g(z)$$

son válidas en todos los puntos $z \in D$ donde ambas funciones toman valores finitos, mientras que en los puntos $z_0 \in D$ que son polos de alguna de las funciones, puede ocurrir que la suma y el producto tengan también polos o no. Ello dependerá de si los límites

$$\lim_{z\to z_0}(f(z) + g(z)), \qquad \lim_{z\to z_0}(f(z)g(z)),$$

sean finitos o infinitos. Por ejemplo, las funciones

$$f(z) = \frac{1}{z}, \qquad g(z) = \frac{z}{z-1}$$

son meromorfas en $\mathbb{C}$, la primera con un polo en 0 y la segunda con un polo en 1. Al operarlas obtenemos

$$(f + g)(z) = \frac{z^2 + z - 1}{z(z-1)}, \qquad (fg)(z) = \frac{1}{z-1},$$

de modo que la suma tiene polos en 0 y en 1, mientras que el producto sólo tiene un polo en 1, ya que $(fg)(0) = -1$.

Como hemos dicho, las funciones de $\mathcal{M}(D)$, con estas operaciones, forman un cuerpo. El hecho de que toda función no nula tenga inversa se debe a que, del mismo modo que los polos de una función meromorfa f forman, por definición, un conjunto cerrado y discreto en su dominio, lo mismo le sucede al conjunto de ceros (salvo que f sea idénticamente nula), y así, salvo en este caso, f^{-1} resulta ser una función meromorfa que tiene polos donde f tiene ceros y viceversa.

El hecho fundamental para tratar con funciones meromorfas desde un punto de vista algebraico es que si $D_1 \subset D_2$ son dominios complejos, la restricción $\mathcal{M}(D_2) \longrightarrow \mathcal{M}(D_1)$ es inyectiva y, más concretamente, es un monomorfismo de cuerpos, de modo que podemos considerar a $\mathcal{M}(D_2)$ como subcuerpo de $\mathcal{M}(D_1)$. Así, en particular, para operar con funciones meromorfas podemos restringirnos a cualquier abierto suficientemente pequeño como para excluir los polos de todas las funciones involucradas.

Lo mismo sucede con la derivación: si f es una función meromorfa en D, en los puntos donde es finita, tenemos definida también su derivada f', la cual se extiende de forma única a una función meromorfa en D (aunque en este caso puede probarse que f' siempre tiene polos donde f los tiene).

Sucede que todas las cuestiones técnicas sobre derivabilidad, dominios de definición, etc. a que dan lugar las funciones meromorfas son irrelevantes para los resultados que queremos probar, y por ello nos será muy cómodo desembarazarnos de ellas considerando un marco de trabajo abstracto puramente algebraico, en el contexto de cuerpos arbitrarios.

En realidad vamos a restringirnos a trabajar con cuerpos con una propiedad adicional que no supone ninguna restricción para nuestros fines: Recordemos que un cuerpo K tiene *característica cero* si el homomorfismo natural $\mathbb{Z} \longrightarrow K$ dado por $n \mapsto n \cdot 1$ es inyectivo, es decir, si $n \cdot 1 \neq 0$ siempre que $n \neq 0$, lo cual se traduce, más en general, en que $n\alpha \neq 0$ para todo $n \in \mathbb{Z}$ y todo $\alpha \in K$ no nulos.

Observemos que la característica 0 depende únicamente de lo que sucede al sumar 1 consigo mismo muchas veces, por lo que si un cuerpo tiene característica 0 lo mismo le sucede a todos sus subcuerpos y a todas sus extensiones. En particular, $\mathbb{C}$ y todos los cuerpos $\mathcal{M}(D)$ tienen característica 0.

Definición 2.1 Una *derivación* en un cuerpo K es una aplicación $K \longrightarrow K$, que representaremos por $f \mapsto f'$, tal que, para todo f, $g \in K$, cumple las dos propiedades siguientes:

$$(f+g)' = f' + g', \qquad (fg)' = f'g + fg'.$$

Un *cuerpo diferencial* es un cuerpo en el que tenemos definida una derivación. En lo sucesivo supondremos tácitamente que *todos los cuerpos diferenciales que consideramos son de característica* 0.

Por abuso de lenguaje, llamaremos *funciones* a los elementos de un cuerpo diferencial arbitrario, aunque en principio no decimos nada sobre la naturaleza conjuntista de sus elementos.

En estos términos podemos decir que, si $D \subset \mathbb{C}$ es un dominio, entonces $\mathcal{M}(D)$ es un cuerpo diferencial con la derivación usual de funciones meromorfas.

Observemos ahora que las propiedades básicas de la derivación usual de funciones son válidas en este contexto general. Por ejemplo, en todo cuerpo diferencial se cumple la regla de derivación del cociente:

$$\left(\frac{f}{g}\right)' = \frac{f'g - fg'}{g^2},$$

pues

$$f' = \left(g\,\frac{f}{g}\right)' = g'\,\frac{f}{g} + g\left(\frac{f}{g}\right)',$$

y basta despejar $(f/g)'$.

También es fácil demostrar inductivamente que $(f^n)' = nf^{n-1}f'$, para todo $f \in K$ y todo entero n (con $f \neq 0$ si $n < 0$).

A partir de aquí, una simple inducción sobre m demuestra la identidad siguiente, que enunciamos como teorema para referencias posteriores:

Teorema 2.2 *Si K es un cuerpo diferencial, $a_1, \ldots, a_m \in K$ son funciones no nulas y $n_1, \ldots, n_m \in \mathbb{Z}$, entonces*

$$\frac{(a_1^{n_1} \cdots a_m^{n_m})'}{a_1^{n_1} \cdots a_m^{n_m}} = n_1\frac{a_1'}{a_1} + \cdots + n_m\frac{a_m'}{a_m}.$$

Es conocido que una función meromorfa sobre un dominio (que es conexo, por definición) tiene derivada nula si y sólo si es constante. Por ello, en un cuerpo diferencial cualquiera K, definimos el *subcuerpo de las constantes* como el conjunto

$$C = \{\alpha \in K \mid \alpha' = 0\}.$$

Es fácil probar que, ciertamente, C es un subcuerpo de K. Notemos que la prueba requiere comprobar que 0 y 1 son constantes. En el caso del 1 esto se debe a que

$$1' = (1 \cdot 1)' = 1' \cdot 1 + 1 \cdot 1' = 1' + 1',$$

luego $1' = 0$. Para el caso del 0 la prueba es aún más simple. Ahora es inmediato que la suma, el producto, el opuesto y el inverso de constantes es constante.

Cuando uno de los factores es constante, la regla del producto se reduce a $(\alpha f)' = \alpha f'$. En otras palabras, la derivación es una aplicación C-lineal de K en K.

Según hemos indicado, en el caso de $\mathcal{M}(D)$, el cuerpo de las constantes está formado por las funciones constantes en el sentido usual, que podemos identificar con el cuerpo $\mathbb{C}$ de los números complejos.

Recordemos que se dice que un cuerpo K es una *extensión* de otro cuerpo k (o que $k \subset K$ es una *extensión de cuerpos,* si k es un subcuerpo de K. Diremos que $k \subset K$ es una *extensión de cuerpos diferenciales,* o que k es un *subcuerpo diferencial* de K, si K es

un cuerpo diferencial y k es un subcuerpo tal que la derivada de toda función de k está también en k, de modo que k se convierte en un cuerpo diferencial con la restricción de la derivación de K.

Por ejemplo, ya hemos observado que si $D_1 \subset D_2$ son dominios complejos, la restricción induce un monomorfismo de cuerpos $\mathcal{M}(D_2) \longrightarrow \mathcal{M}(D_1)$. Si $f \in \mathcal{M}(D_2)$ y $z \in D_1$ es un punto donde f es finita, la derivada $f'(z)$ está definida localmente, lo que se traduce en que $f'(z) = (f|_{D_1})'(z)$ y, en definitiva, tenemos que $f'|_{D_1} = (f|_{D_1})'$. Esto significa que, al considerar a $\mathcal{M}(D_2)$ como subcuerpo de $\mathcal{M}(D_1)$, de hecho se trata de un subcuerpo diferencial.

Recordemos también que si $k \subset K$ es una extensión de cuerpos y $S \subset K$, se llama *adjunción* de S a k al cuerpo $k(S)$ formado por los elementos de K de la forma

$$\frac{p(s_1, \ldots, s_n)}{q(s_1, \ldots, s_n)},$$

donde $n \in \mathbb{N}$, $p, q \in k[X_1, \ldots, X_n]$, $s_1, \ldots, s_n \in S$ y $q(s_1, \ldots, s_n) \neq 0$. Equivalentemente, $k(S)$ es el menor subcuerpo de K que contiene a k y a S.

Cuando el conjunto $S = \{s_1, \ldots, s_n\}$ es finito escribimos también $k(s_1, \ldots, s_n)$ en lugar de $k(S)$. Cuando $K = k(S)$ se dice que S es un *sistema generador* de K sobre k. Cuando $K = k(s)$ se dice que la extensión es *simple* y que s es un *elemento primitivo* de la extensión.

Por ejemplo, si en $\mathcal{M}(\mathbb{C})$ llamamos z a la función identidad (es decir, $f(z) = z$), el subcuerpo $\mathbb{C}(z)$ está formado por las funciones que se expresan como cocientes de polinomios en z (con coeficientes en $\mathbb{C}$). Son las llamadas *funciones racionales.* Es claro que la derivada de una función racional es de nuevo una función racional, por lo que $\mathbb{C}(z)$ es un subcuerpo diferencial de $\mathcal{M}(\mathbb{C})$. En realidad, esto es un caso particular del teorema siguiente:

Teorema 2.3 *Sea $k \subset K$ una extensión de cuerpos diferenciales y $S \subset K$. El cuerpo $k(S)$ es un subcuerpo diferencial de K si y sólo si para todo $s \in S$ se cumple que $s' \in k(S)$.*

Demostración: Una implicación se sigue inmediatamente de la definición de subcuerpo diferencial. Supongamos ahora que las derivadas de elementos de S permanecen en $k(S)$ y consideremos un monomio

$$M = \alpha s_1^{n_1} \cdots s_m^{n_m},$$

donde $\alpha \in k$ y $s_i \in S$. Una simple inducción sobre $n = n_1 + \cdots + n_m$ demuestra que $M' \in k(S)$. Esto implica a su vez que la derivada de todo polinomio $p(s_1, \ldots, s_n)$ con coeficientes en k está en $k(S)$, y esto implica a su vez que lo mismo es válido para todo cociente de polinomios, es decir, para todo elemento de $k(S)$. ∎

A continuación damos la definición abstracta de función elemental que seguidamente particularizaremos al caso de los cuerpos de funciones meromorfas.

Definición 2.4 Si $k \subset K$ es una extensión de cuerpos diferenciales, diremos que una función[1] $f \in K$ es *elemental* sobre k si existe una cadena de subcuerpos

$$k = K_0 \subset K_1 \subset \cdots \subset K_n \subset K$$

de modo que $f \in K_n$ y, para cada índice i, se cumple que $K_i = K_{i-1}(t_i)$, y t_i se encuentra en uno de los tres casos siguientes:

1. t_i es *algebraico* sobre K_{i-1}, es decir, existe un polinomio $p(X) \in K_{i-1}[X]$ no nulo tal que $p(t_i) = 0$.

2. t_i es no nulo y existe una función $f \in K_{i-1}$ tal que $f' = t_i'/t_i$, en cuyo caso diremos que t_i es una *exponencial* de f.

3. Existe una función $f \in K_{i-1}$ no nula tal que $t_i' = f'/f$, en cuyo caso diremos que t_i es un *logaritmo* de f.

Si $D \subset \mathbb{C}$ es un dominio, podemos considerar a $\mathbb{C}(z) \subset \mathcal{M}(\mathbb{C}) \subset \mathcal{M}(D)$ como subcuerpo diferencial de $\mathcal{M}(D)$. Llamaremos *funciones elementales* en D a las funciones de $\mathcal{M}(D)$ que son elementales sobre $\mathbb{C}(z)$ en el sentido de la definición anterior.

A continuación demostraremos algunas propiedades básicas de las funciones elementales. En la sección siguiente mostraremos ejemplos concretos. Empezamos con un par de precisiones sobre la definición de función elemental:

Teorema 2.5 *Todos los cuerpos K_i que aparecen en la definición anterior son subcuerpos diferenciales de K. En particular, si $f \in K$ es elemental, f' también lo es.*

DEMOSTRACIÓN: Razonamos por inducción sobre i. Obviamente, $K_0 = k$ es un subcuerpo diferencial de K. Si esto es cierto para K_{i-1}, tenemos que $K_i = K_{i-1}(t_i)$, luego basta probar que $t_i' \in K_i$. Esto es trivial si t_i es una exponencial o un logaritmo de una función $f \in K_{i-1}$, pues en el primer caso $t_i'/t_i = f' \in K_{i-1}$, con lo que $t_i' = t_i f' \in K_i$, y en el segundo $t_i' = f'/f \in K_{i-1} \subset K_i$.

Nos falta considerar el caso en que la función t_i es algebraica sobre K_{i-1}. Esto significa que

$$\sum_{j=0}^{n} c_j t_i^j = 0,$$

para ciertos $c_j \in K_{i-1}$ no todos nulos. Podemos suponer que n es el mínimo natural tal que existe un polinomio no nulo de grado n con coeficientes en K_{i-1} que se anula en t_i. Derivando obtenemos que

$$c_0' + \sum_{j=1}^{n} (c_j' t_i^j + j c_j t_i^{j-1} t_i') = 0,$$

[1]Recordemos que llamamos "funciones" a los elementos arbitrarios de un cuerpo diferencial, aunque no sean necesariamente funciones en el sentido conjuntista.

luego

$$t_i' = -\frac{\displaystyle\sum_{j=0}^{n} c_j' t_i^j}{\displaystyle\sum_{j=1}^{n} j c_j t_i^{j-1}} \in K_i,$$

donde observamos que el denominador es no nulo porque se trata de un polinomio en t_i con coeficientes en K_{i-1} de grado[2] $n-1$, luego no puede anularse sobre t_i por la minimalidad de n. ∎

Teorema 2.6 *Si $k \subset K$ es una extensión de cuerpos diferenciales y $f_1, \dots, f_m \in K$ son funciones elementales sobre k, entonces existe una cadena de cuerpos*

$$k = K_0 \subset K_1 \subset \cdots \subset K_n \subset K$$

en las condiciones de la definición 2.4 tal que $f_1, \dots, f_m \in K_n$.

DEMOSTRACIÓN Razonamos por inducción sobre m. Para $m = 1$ se trata de la propia definición de función elemental. Supongamos el teorema cierto para $m-1$ y sea

$$k = K_0 \subset K_1 \subset \cdots \subset K_n \subset K$$

una cadena de subcuerpos tal que $f_1, \dots, f_{m-1} \in K_n$. Como f_m es elemental, existe otra cadena

$$k = L_0 \subset L_1 \subset \cdots \subset L_r \subset K$$

en las condiciones de 2.4 tal que $f_m \in L_r$. Pongamos que $L_i = L_{i-1}(u_i)$ y definamos recurrentemente $K_{n+i} = K_{n+i-1}(u_i)$. Así tenemos una cadena de subcuerpos

$$k = K_0 \subset \cdots \subset K_n \subset K_{n+1} \subset \cdots \subset K_{n+r} \subset K$$

que cumple la definición 2.4, pues inductivamente se prueba que $L_{i-1} \subset K_{n+i-1}$ y, si la función u_i es algebraica sobre L_{i-1}, o es una exponencial o un logaritmo de un elemento de L_{i-1}, *a fortiori* cumple lo mismo con K_{n+i-1}. Además, $f_1, \dots, f_m \in K_{n+r}$. ∎

De aquí deducimos varias propiedades:

Teorema 2.7 *Si $k \subset K$ es una extensión de cuerpos diferenciales, entonces el conjunto K_e de las funciones $f \in K$ elementales sobre k es un subcuerpo diferencial de K.*

DEMOSTRACIÓN: Si $f, g \in K$ son elementales sobre k, por el teorema anterior existe una cadena de subcuerpos

$$k = K_0 \subset \cdots \subset K_n \subset K,$$

según la definición 2.4 tal que $f, g \in K_n$ y, como éste es un subcuerpo, también contiene a $f+g$, $f-g$, $-f$ y $1/f$ (si $f \neq 0$).

Esto prueba que K_e es un subcuerpo de K y el teorema 2.5 prueba que, de hecho, se trata de un subcuerpo diferencial. ∎

[2]Aquí usamos por primera vez nuestra hipótesis de que los cuerpos diferenciales son de característica 0.

Teorema 2.8 *Sea $k \subset K$ una extensión de cuerpos elementales y sea K_e el subcuerpo diferencial de las funciones $f \in K$ elementales sobre k. Entonces:*

1. *Toda función $f \in K$ algebraica sobre K_e está en K_e.*

2. *Toda exponencial y todo logaritmo de una función $g \in K_e$ está en K_e.*

DEMOSTRACIÓN: Si $f \in K$ es algebraica sobre K_e, esto significa que existe un polinomio no nulo $P(X)$ con coeficientes en K_e tal que $P(f) = 0$. Por el teorema 2.6, existe una cadena de subcuerpos

$$k = K_0 \subset K_1 \subset \cdots \subset K_n \subset K$$

que cumpla la definición 2.4 de modo que todos los coeficientes de $P(X)$ estén en K_n. Prolongando la cadena con $K_{n+1} = K_n(f)$ tenemos una nueva cadena que sigue cumpliendo la definición 2.4 (porque f es algebraica sobre K_n) y ahora $f \in K_{n+1}$, luego $f \in K_e$.

Si f es una exponencial o un logaritmo de una función $g \in K_e$, entonces tomamos una cadena según la definición 2.4 tal que $g \in K_n$ y la prolongamos con $K_{n+1} = K_n(f)$, y nuevamente concluimos que $f \in K_e$. ∎

Ejercicio Probar que si $k \subset K$ es una extensión de cuerpos diferenciales, el cuerpo K_e de las funciones $f \in K$ elementales sobre k es el menor subcuerpo diferencial de K que contiene a k y que es cerrado para elementos algebraicos, exponenciales y logaritmos (es decir, el menor subcuerpo que contiene a k y cumple el teorema anterior).

Teorema 2.9 *Si $D_1 \subset D_2$ son dominios en $\mathbb{C}$, entonces la restricción a D_1 de una función elemental sobre D_2 es elemental sobre D_1.*

DEMOSTRACIÓN: Basta tener presente que la restricción $\mathcal{M}(D_2) \longrightarrow \mathcal{M}(D_1)$ es un monomorfismo de cuerpos que nos permite identificar a $\mathcal{M}(D_2)$ con un subcuerpo diferencial de $\mathcal{M}(D_1)$. Por ello, si $f \in \mathcal{M}(D_2)$ cumple la definición 2.4 con una cadena de cuerpos

$$\mathbb{C}(z) = K_0 \subset K_1 \subset \cdots \subset K_n \subset \mathcal{M}(D_2),$$

al aplicar la restricción obtenemos una cadena idéntica

$$\mathbb{C}(z) = K_0 \subset K_1 \subset \cdots \subset K_n \subset \mathcal{M}(D_2) \subset \mathcal{M}(D_1)$$

que prueba que f, vista como elemento de $\mathcal{M}(D_1)$, es decir, identificada con $f|_{D_1}$, es también elemental. ∎

En general, la composición de funciones elementales no es elemental, porque no es cierto que la composición de funciones meromorfas sea una función meromorfa. Por ejemplo, las funciones $1/z$ y e^z son meromorfas en $\mathbb{C}$, pero su composición $e^{1/z}$ tiene una singularidad esencial en 0, luego no es meromorfa en $\mathbb{C}$. No obstante, sí que es cierto que la composición de una función holomorfa con una función meromorfa es meromorfa,[3] y a continuación probamos que si ambas son elementales, la composición también lo es:

[3]Toda función meromorfa es un cociente de dos funciones holomorfas, luego la composición de una función holomorfa con una meromorfa es también cociente de dos funciones holomorfas, con lo que es meromorfa.

Teorema 2.10 *Sean D_1 y D_2 dominios complejos, sean $f \in \mathcal{M}(D_1)$, $g \in \mathcal{M}(D_2)$ funciones elementales y supongamos que $D_1 \subset f^{-1}[D_2]$ y que f no tiene polos en D_1. Entonces $f \circ g$ es elemental en D_1.*

DEMOSTRACIÓN: Consideremos una cadena de cuerpos

$$\mathbb{C}(z) = K_0 \subset K_1 \subset \cdots \subset K_n \subset \mathcal{M}(D_2)$$

tal que $g \in K_n$, según la definición de función elemental. Vamos a probar, por inducción sobre i, que, para todo $h \in K_i$, se cumple que $f \circ h$ es elemental sobre D_1. En particular, esto implica que lo es $f \circ g$.

Para $i = 0$ es trivial pues, si $h \in \mathbb{C}(z)$, entonces $f \circ h$ es un cociente de polinomios evaluados en f, y es elemental porque las funciones elementales sobre D_1 forman un cuerpo.

Supongamos que es cierto para $i-1$ y sea $K_i = K_{i-1}(t_i)$. Basta probar que $f \circ t_i$ es elemental sobre D_1, ya que todas las demás funciones de K_i son cocientes de polinomios evaluados en t_i, luego las composiciones correspondientes son cocientes de polinomios evaluados en $f \circ t_i$, que serán elementales de nuevo porque las funciones elementales sobre D_1 forman un cuerpo.

Ante todo, según hemos indicado antes del teorema, como f es holomorfa y t_i es meromorfa, sabemos que $f \circ t_i \in \mathcal{M}(D_1)$. Supongamos en primer lugar que t_i es algebraica sobre K_{i-1}, es decir, que existen $c_j \in K_{i-1}$ tales que

$$\sum_{j=0}^{n} c_j t_i^j = 0.$$

Más concretamente, esto significa que

$$\sum_{j=0}^{n} c_j(z) t_i(z)^j = 0$$

para todo $z \in D_2$ donde sean finitas tanto t_i como las c_j (que es todo D_2 salvo un conjunto discreto de puntos). Entonces

$$\sum_{j=0}^{n} c_j(f(z)) t_i(f(z))^j = 0$$

para todo $z \in D_1$ donde sean finitas las composiciones $f \circ c_j$ y $f \circ t_i$. Esto es equivalente a que

$$\sum_{j=0}^{n} (f \circ c_j)(f \circ t_i)^j = 0.$$

Por hipótesis de inducción, las funciones $f \circ c_j$ pertenecen al cuerpo $\mathcal{M}(D_1)_e$ de las funciones elementales sobre D_1, y la igualdad anterior muestra que $f \circ t_i$ es algebraico sobre este cuerpo, luego, por el teorema 2.8, también $f \circ t_i$ es elemental.

Similarmente, si t_i es una exponencial de una función $g \in K_{i-1}$, esto significa que

$$\frac{t_i'(z)}{t_i(z)} = g'(z)$$

para todo $z \in D_2$ donde todas las funciones involucradas sean finitas, luego

$$\frac{t_i'(f(z))}{t_i(f(z))} = g'(f(z))$$

para todo $z \in D_1$ donde todas las funciones sean finitas. Por hipótesis de inducción tenemos que $f \circ g$ es elemental sobre D_1 y

$$\frac{t_i(f(z))'}{t_i(f(z))} = \frac{t_i'(f(z))f'(z)}{t_i(f(z))} = g'(f(z))f'(z),$$

es decir,

$$\frac{(f \circ t_i)'}{f \circ t_i} = (f \circ g)',$$

luego $f \circ t_i$ es una exponencial de $f \circ g$, luego es elemental sobre D_1 por el teorema 2.8.

Igualmente se razona que si t_i es un logaritmo de una función $g \in K_{i-1}$, entonces $f \circ t_i$ es un logaritmo de $f \circ g$, ésta es elemental sobre D_1 por hipótesis de inducción y $f \circ t_i$ lo es entonces de nuevo por 2.8. ∎

3 Funciones elementales reales

Finalmente estamos en condiciones de definir la noción de función elemental (de variable real) que estábamos persiguiendo:

Definición 3.1 Diremos que una función continua $f : [a, b] \longrightarrow \mathbb{R}$ es *elemental* si existe un dominio $[a, b] \subset D \subset \mathbb{C}$ tal que f se extiende a una función (meromorfa) elemental sobre D.

De la definición se sigue que toda función elemental es infinitamente derivable en un intervalo abierto que contiene a $[a, b]$.

Las propiedades que hemos probado en la sección anterior sobre funciones elementales complejas nos dan fácilmente propiedades análogas para las funciones elementales reales. Empecemos con un hecho técnico:

Teorema 3.2 *Si $f_1, \ldots, f_n : [a, b] \longrightarrow \mathbb{R}$ son funciones elementales, existe un dominio $[a, b] \subset D \subset \mathbb{C}$ tal que todas las funciones dadas se extienden a funciones holomorfas elementales sobre D.*

Demostración: En principio, según la definición, cada f_i se extiende a una función meromorfa elemental sobre un dominio complejo D_i. Como f_i es continua en $[a, b]$, la extensión no puede tener polos sobre $[a, b]$. Como el conjunto de polos no puede tener puntos de acumulación en D_i, para cada $x \in [a, b]$ existe un disco D_x, centrado en x y contenido en todos los dominios D_i, que no contiene ningún polo de ningún f_i. La unión D de los D_x es claramente un dominio (conexo) contenido en todos los D_i y que contiene a $[a, b]$. Cada f_i se restringe a una función holomorfa elemental en D (teorema 2.9) que, obviamente, sigue extendiendo a la función correspondiente sobre $[a, b]$. ∎

De aquí se siguen varias consecuencias básicas:

Teorema 3.3 *La suma y el producto de funciones elementales sobre un intervalo $[a,b]$ es elemental, así como el cociente si el denominador no se anula en ningún punto de $[a,b]$.*

DEMOSTRACIÓN: Si f y g son elementales en $[a,b]$, por el teorema anterior se extienden a funciones elementales sobre un mismo dominio complejo D, luego $f+g$, fg y f/g son también elementales en D, luego también lo son en $[a,b]$, salvo en el caso del cociente, en el que hemos de exigir además que g no se anule en ningún punto para que el cociente sea continuo en $[a,b]$. ∎

Teorema 3.4 *La composición de funciones elementales es elemental.*

DEMOSTRACIÓN: Supongamos que $f:[a,b]\longrightarrow[c,d]$ y $g:[c,d]\longrightarrow\mathbb{R}$ son elementales. Entonces f se extiende a una función holomorfa en un dominio complejo D_1 y g se extiende igualmente a un dominio complejo D_2. Mediante el mismo argumento empleado en la prueba del teorema 3.2 podemos suponer que $D_1\subset f^{-1}[D_2]$, y así podemos aplicar el teorema 2.10 para concluir que $f\circ g$ es elemental en D_1, luego también en $[a,b]$. ∎

Hasta aquí no hemos dado ningún ejemplo concreto de función elemental. No obstante, hay un ejemplo obvio:

Teorema 3.5 *Los polinomios (con coeficientes reales) son funciones elementales sobre cualquier intervalo $[a,b]$. Lo mismo sucede con los cocientes de polinomios cuyo denominador no se anula en $[a,b]$.*

DEMOSTRACIÓN: Todo polinomio se extiende a una función de $\mathbb{C}(z)\subset\mathcal{M}(\mathbb{C})$, y toda función de $\mathbb{C}(z)$ es trivialmente elemental sobre $\mathbb{C}(z)$. El caso del cociente se sigue del teorema 3.3. ∎

Veamos ahora los ejemplos que se siguen inmediatamente de la definición abstracta de función elemental:

Teorema 3.6 *La función exponencial e^x es elemental en todo intervalo $[a,b]$.*

DEMOSTRACIÓN: La exponencial real e^x se extiende a la función exponencial compleja $e^z\in\mathcal{M}(\mathbb{C})$. Basta probar que ésta es elemental en el sentido complejo. Ahora bien, e^z es una exponencial de z en el sentido abstracto de la sección anterior, pues

$$z' = 1 = \frac{(e^z)'}{e^z}.$$

La función z es elemental y toda exponencial de una función elemental es elemental. ∎

Teorema 3.7 *Si $0<a<b$, la función $\log x$ es elemental en $[a,b]$.*

DEMOSTRACIÓN: La función $\log x$ se extiende a una función holomorfa $\log z$ definida sobre todo el abierto $H = \mathbb{C} \setminus]-\infty, 0]$. Basta probar que este logaritmo complejo es elemental. Para ello basta observar que $\log z$ es un logaritmo de z, pues

$$(\log z)' = \frac{1}{z} = \frac{z'}{z}.$$

Como la función z es elemental, la función $\log z$ también lo es. ∎

Ahora es inmediato que la función

$$a^x = e^{x \log a},$$

para $a > 0$, es elemental en cualquier intervalo (porque es composición del polinomio $x \log a$ con la función elemental e^x), al igual que las funciones

$$\log_a x = \frac{\log x}{\log a}, \qquad x^\alpha = e^{\alpha \log x}, \qquad \sqrt[n]{x} = x^{1/n},$$

para $a > 0$, $\alpha \in \mathbb{R}$, $n \geq 2$, en cualquier intervalo $[u, v]$ con $0 < u < v$.

Si n es un número natural impar, la función $\sqrt[n]{x}$ también es elemental en cualquier intervalo $[u, v]$ con $u < v < 0$, pues la podemos definir como $\sqrt[n]{x} = -\sqrt[n]{-x}$, pero no es elemental en intervalos que contengan al cero porque no es derivable en 0.

El teorema siguiente muestra la importancia de admitir funciones de variable compleja para conseguir una definición sencilla de función elemental:

Teorema 3.8 *Las funciones* $\operatorname{sen} x$, $\cos x$ *son elementales en cualquier intervalo cerrado.*

DEMOSTRACIÓN: Las funciones seno y coseno se extienden a funciones holomorfas $\operatorname{sen} z$ y $\cos z$ definidas sobre todo el plano complejo. Basta probar que son elementales en el sentido complejo. Nos basamos en las relaciones

$$\operatorname{sen} z = \frac{e^{iz} - e^{-iz}}{2i}, \quad \cos z = \frac{e^{iz} + e^{-iz}}{2}.$$

Hemos de probar que estas funciones son elementales en el sentido complejo. Para ello observamos que e^{iz} es una exponencial de la función iz, pues

$$\frac{(e^{iz})'}{e^{iz}} = i = (iz)'.$$

Como iz es elemental, concluimos que e^{iz} también lo es, al igual que su inversa, e^{-iz}, lo que a su vez implica que también son elementales las funciones $\operatorname{sen} z$ y $\cos z$. ∎

Por consiguiente, la función $\tan x$ también es elemental en cualquier intervalo en el que esté definida.

Teorema 3.9 *La función* $\arctan x$ *es elemental en cualquier intervalo.*

DEMOSTRACIÓN: Observemos que, dado un $x \in \mathbb{R}$ existen infinitos números reales w tales que $x = \tan w$, y dos cualesquiera de ellos se diferencian en un múltiplo entero de π. La función $\arctan x$ es, por definición, la que toma valores en $]-\pi/2, \pi/2[$.

Por otra parte, consideremos nuevamente el dominio $H = \mathbb{C} \setminus]-\infty, 0]$ y la rama uniforme holomorfa del logaritmo $\log : H \longrightarrow \mathbb{C}$. En realidad hay también infinitos logaritmos holomorfos definidos sobre H, y dos cualesquiera se diferencian en un múltiplo entero de $2\pi i$. Concretamente, tomamos como log la función dada por

$$\log z = \log |z| + i \arg z,$$

donde $\arg z$ es el argumento de z en $]-\pi, \pi[$. Se trata del logaritmo que extiende al logaritmo real usual.

Observemos ahora que si w es un número complejo y $z = \tan w$, entonces

$$z = \frac{\operatorname{sen} w}{\cos w} = -i\,\frac{e^{iw} - e^{-iw}}{e^{iw} + e^{-iw}},$$

de donde, despejando,

$$e^{2iw} = \frac{i - z}{i + z} = \frac{1 - |z|^2 + 2i\operatorname{Re} z}{1 + |z|^2 + 2\operatorname{Im} z}.$$

La fracción sólo toma valores en $]-\infty, 0]$ cuando su parte imaginaria es nula, es decir, $\operatorname{Re} z = 0$, y la parte real es negativa o nula, es decir, $|z| \geq 1$. Así pues, la función

$$\arctan z = \frac{1}{2i} \log \frac{i - z}{i + z}$$

está definida excepto en dichos puntos, en particular sobre el dominio

$$D = \{z \in \mathbb{C} \mid |\operatorname{Im} z| < 1\},$$

y es una extensión holomorfa de la función arco tangente real. En efecto, si z es real, la función $\arctan z$ ha de ser uno de los arcos cuya tangente es z, pero todos ellos son reales, luego es un número real y, como, por definición, la parte imaginaria del logaritmo está en $]-\pi, \pi[$, resulta que $\arctan z \in]-\pi/2, \pi/2[$, luego se trata del arco tangente usual.

Hemos de probar que este arco tangente holomorfo es elemental. A su vez, basta probar que lo es la función

$$\log \frac{i - z}{i + z},$$

y esto se debe a que es obviamente un logaritmo de la función elemental $(i - z)/(i + z)$. ∎

Ahora es inmediato que las funciones

$$\operatorname{arcsen} x = \arctan \frac{x}{\sqrt{1 - x^2}}, \qquad \arccos x = \frac{\pi}{2} - \operatorname{arcsen} x$$

son elementales en cualquier intervalo $[u, v]$ con $-1 < u < v < 1$, y de aquí se sigue ya sin dificultad el carácter elemental de cualquier función trigonométrica.

Ejercicio Probar que las funciones hiperbólicas (senh, cosh, tanh, etc.) y sus inversas son elementales.

Con esto hemos probado que todas las funciones "usuales" son elementales.

4 Primitivas elementales

En esta sección daremos una condición necesaria y suficiente para que una función tenga una primitiva elemental. Vamos a necesitar algunos resultados adicionales de la teoría de extensiones de cuerpos.

Consideremos una extensión simple $K = k(u)$. Podemos definir un homomorfismo natural de anillos

$$\phi : k[X] \longrightarrow K$$

dado por $p(X) \mapsto p(u)$. Si u es *trascendente* sobre k, es decir, si no es algebraico, si no es raíz de ningún polinomio no nulo de $k[X]$, estamos diciendo que ϕ es inyectivo, y podemos extenderlo a un isomorfismo

$$k(X) \longrightarrow K,$$

donde $k(X)$ es el cuerpo de cocientes del anillo de polinomios $k[X]$, dado por

$$\frac{p(X)}{q(X)} \mapsto \frac{p(u)}{q(u)}.$$

Observemos que es suprayectivo por definición de $k(u)$.

Por el contrario, si u es algebraico sobre k, esto significa que el núcleo de ϕ es un ideal no nulo de $k[X]$, y es conocido que todos los ideales de $k[X]$ son principales, es decir, que están generados por un único elemento, un polinomio $p(X)$, en este caso, que resulta ser único si exigimos que sea *mónico* (es decir, tenga coeficiente director igual a 1). Esto quiere decir que los polinomios $q(X)$ que cumplen $q(u) = 0$ (los elementos del núcleo de ϕ) son exactamente los múltiplos de $p(X)$. Este polinomio se llama *polinomio mínimo* de u sobre k.

Ahora ϕ induce un monomorfismo

$$k[X]/(p(x)) \longrightarrow K,$$

y también es conocido que resulta ser igualmente un isomorfismo, lo cual no es trivial,[4] sino que nos permite concluir que los elementos de K, que en principio son cocientes de polinomios de $k[X]$ evaluados en u, se pueden expresar de hecho como polinomios de $k[X]$ evaluados en u (y, si se quiere, de grado menor que el de $p(x)$). De aquí se sigue fácilmente que la dimensión de K como espacio vectorial sobre k es precisamente el grado de $p(X)$. Esta dimensión se llama *grado* de la extensión, y se representa por $|K : k|$.

A partir de aquí vamos a suponer que k es un cuerpo diferencial y vamos a definir derivaciones en el cuerpo $k(X)$. Para ello observamos primero que si una aplicación

[4]Véase el teorema 7.6 de mi libro de álgebra. En general, el capítulo VII contiene toda la teoría de extensiones de cuerpos que necesitamos aquí (y bastante más).

$d : k[X] \longrightarrow k[X]$ cumple sobre $K[X]$ las dos propiedades que definen a las derivaciones (que tienen sentido aunque $k[X]$ no sea un cuerpo), entonces la regla del cociente

$$\bar{d}\left(\frac{r(X)}{s(X)}\right) = \frac{d(r(X))s(X) - r(X)d(s(X))}{s(X)^2}$$

extiende d a una derivación $\bar{d}$ en el cuerpo $k(X)$. En efecto, si $r/s = f/g$, entonces $rg = sf$, luego $(dr)g + r(dg) = (ds)f + s(df)$, luego, multiplicando por sg:

$$(dr)sg^2 - (ds)sfg = s^2g(df) - rgs(dg),$$

y, usando la relación $rg = sf$,

$$(dr)sg^2 - (ds)rg^2 = s^2g(df) - s^2f(dg),$$

con lo que

$$\frac{(dr)s - s(dr)}{s^2} = \frac{(df)g - f(dg)}{g^2}.$$

Esto prueba que la definición de $\bar{d}$ no depende de la representación como fracción de un elemento de $k(X)$. Necesariamente, d ha de cumplir $d1 = 0$, por lo que

$$\bar{d}r = \bar{d}(r/1) = dr,$$

luego $\bar{d}$ extiende a d. Ahora es una simple rutina comprobar que $\bar{d}$ cumple las dos propiedades de la definición de derivación. Observemos que $\bar{d}$ es la única derivación en $k(X)$ que extiende a d, puesto que toda derivación en $k(X)$ ha de cumplir la regla del cociente.

Dicho de otro modo: para definir una derivación en $k(X)$ basta definirla en $k[X]$.

Así pues, definimos dos derivaciones D_0 y D_1 en $k(X)$ mediante las definiciones siguientes en $k[X]$:

$$D_0\left(\sum_{i=0}^n a_iX^i\right) = \sum_{i=0}^n a_i'X^i, \qquad D_1\left(\sum_{i=0}^n a_iX^i\right) = \sum_{i=0}^n ia_iX^{i-1}.$$

Una comprobación rutinaria muestra que, en efecto, D_0 y D_1 son derivaciones (sobre $k[X]$ y, por lo tanto, sobre $k(X)$). Además vemos que $D_0(\alpha) = \alpha'$, para todo $\alpha \in k$, y $D_0(X) = 0$, mientras que $D_1(\alpha) = 0$, para todo $\alpha \in k$, y $D_1(X) = 1$.

Ahora bien, si $q \in k(X)$ es un elemento arbitrario, es fácil ver que la aplicación

$$D(\alpha) = D_0(\alpha) + qD_1(\alpha)$$

es también una derivación en $k(X)$ que extiende a la derivación de k y además cumple $D(X) = q$. Con esto tenemos casi probado el teorema siguiente:

Teorema 4.1 *Si k es un cuerpo diferencial y $K = k(u)$ es una extensión simple con u trascendente sobre k, para cada $q \in K$ existe una única derivación en K que extiende a la de k y que cumple $u' = q$.*

DEMOSTRACIÓN: En efecto, si u es trascendente sobre k, sabemos que $k(u)$ es isomorfo a $k(X)$ (y el isomorfismo hace corresponder X con u), por lo que no perdemos generalidad si suponemos que $K = k(X)$. Ya hemos probado la existencia de la extensión que cumple $X' = q$, y es única porque las reglas de derivación implican inmediatamente que, para todo polinomio $q(X) \in k[X]$,

$$q(X)' = (D_0 q)(X) + (D_1 q)(X) \cdot q,$$

por lo que toda derivación en $k(X)$ que cumpla $X' = q$ está completamente determinada sobre $k[X]$, y por la regla del cociente está completamente determinada sobre $k(X)$. ∎

Ahora vamos a estudiar el caso en el que u es algebraico sobre k. Sea $p(X)$ el polinomio mínimo de u. Fijemos un polinomio $q(X) \in k[X]$ y consideremos la derivación D asociada a q. Vamos a ver que podemos elegir q para que se cumpla

$$(Dp)(u) = (D_0 p)(u) + q(u)(D_1 p)(u) = 0.$$

En efecto, observamos que $D_1 p$ es un polinomio (no nulo) de grado una unidad menos que p (aquí usamos que los cuerpos tienen característica 0), luego $(D_1 p)(u) \neq 0$ (porque, para anularse en u, el polinomio $D_1 p$ debería ser múltiplo de p, y esto es imposible), luego podemos despejar

$$q(u) = -\frac{(D_0 p)(u)}{(D_1 p)(u)},$$

y ésta es la condición para que se cumpla la ecuación. Como todo elemento de $k(u)$ (en particular el miembro derecho de la igualdad anterior) es de la forma $q(u)$, para cierto $q(X) \in k[X]$, podemos elegir $q(X)$ para que se cumpla esto, y así, hemos encontrado una derivación D en $k(X)$ que extiende a la de k y que además cumple $(Dp)(u) = 0$.

Esto nos permite definir una derivación en K mediante

$$f(u)' = (Df)(u).$$

La definición es correcta, pues si $f(u) = g(u)$, entonces $(f-g)(u) = 0$, luego $(f-g) = ph$, para cierto $h \in k[X]$, luego

$$(Df)(u) - (Dg)(u) = D(f-g)(u) = D(ph)(u) = (Dp)(u)h(u) + p(u)(Dh)(u) = 0,$$

luego $(Df)(u) = (Dg)(u)$.

El hecho de que D sea una derivación en $k(X)$ que extiende a la de k implica inmediatamente que la derivación que acabamos de definir en K cumple lo mismo. Con esto tenemos probada la mitad del teorema siguiente:

Teorema 4.2 *Si k es un cuerpo diferencial y $K = k(u)$ es una extensión simple con u algebraico sobre k, entonces existe una única derivación en K que extiende a la de k.*

DEMOSTRACIÓN: Acabamos de probar la existencia de la extensión, y la unicidad se debe a que todo elemento de K es de la forma $q(u)$, para cierto $q \in k[X]$, y

$$q(u)' = (D_0 q)(u) + (D_1 q)(u) \cdot u'.$$

Si particularizamos esta igualdad al polinomio mínimo de u obtenemos

$$0 = (D_0p)(u) + (D_1p)(u) \cdot u',$$

y ya hemos razonado que $(D_1p)(u) \neq 0$, luego necesariamente

$$u' = -\frac{(D_0p)(u)}{(D_1p)(u)},$$

con lo que la ecuación (para q arbitrario) prueba que la derivación está unívocamente determinada. ∎

Vamos a necesitar el hecho de que todo cociente de polinomios puede descomponerse en suma de *fracciones simples* (lo que se usa para calcular primitivas de funciones racionales):

Teorema 4.3 *Si K es un cuerpo, todo $z \in K(X)$ se descompone de forma única como*

$$z = f + \sum_{i=1}^{n} \sum_{j=1}^{r_i} \frac{f_{ij}}{p_i^j}$$

donde $f, f_{ij}, p_i \in K[X]$, los polinomios p_i son mónicos, irreducibles, distintos dos a dos, y f_{ij} es nulo o tiene grado menor que p_i (pero $f_{ir_i} \neq 0$).

Demostración: Sea $z = u/v$, con u, $v \in K[X]$. Podemos suponer que u y v son primos entre sí y que v es mónico. Si $v = 1$ tenemos la descomposición con $f = u$. En caso contrario consideremos un factor primo p_1 de v, de modo que $v = p_1^{r_1}\bar{v}$ y p_1 no divide a $\bar{v}$. Podemos suponer que tanto p_1 como $\bar{v}$ son mónicos. Vamos a probar que

$$\frac{u}{v} = \frac{\bar{u}}{\bar{v}} + \sum_{j=1}^{r_1} \frac{f_{1j}}{p_1^j},$$

donde $\bar{u}$ y $\bar{v}$ son primos entre sí y los polinomios f_{1j} tienen grado menor que el grado de p_1. Si obtenemos esta descomposición, podemos aplicar el mismo resultado a $\bar{u}/\bar{v}$ y así sucesivamente hasta que el denominador acabe siendo 1 (lo cual ocurrirá necesariamente tras un número finito de pasos, porque a cada paso le quitamos un factor primo). Con esto habremos llegado a una descomposición de z como la que aparece en el enunciado.

Como p_1 y $\bar{v}$ son primos entre sí, por la relación de Bezout existen polinomios c, d tales que $c\bar{v} + dp_1 = 1$. Esta igualdad implica en particular que p_1 no divide a c, y tampoco divide a u porque u y v son primos entre sí. Por lo tanto, en la división $uc = gp_1 + f_{1,r_1}$, el resto f_{1,r_1} no puede ser nulo, y tiene grado menor que el de p_1. Así pues,

$$\frac{u}{\bar{v}} = uc + \frac{du}{\bar{v}}\, p_1 = \frac{g\bar{v} + du}{\bar{v}}\, p_1 + f_{1,r_1} = \frac{u_1}{\bar{v}}\, p_1 + f_{1,r_1},$$

donde u_1 y $\bar{v}$ son primos entre sí. Aplicamos el mismo razonamiento a $u_1/\bar{v}$ para obtener la descomposición

$$\frac{u}{\bar{v}} = \left(\frac{u_2}{\bar{v}}\, p_1 + f_{1,r_1-1}\right) p_1 + f_{1,r_1} = \frac{u_2}{\bar{v}}\, p^2 + f_{1,r_1-1}p_1 + f_{1,r_1},$$

donde u_2 y $\bar{v}$ son primos entre sí (aunque ahora f_{1,r_1-1} sí puede ser 0, lo que sucederá si p_1 divide a u_1). Repetimos el proceso hasta obtener:

$$\frac{u}{\bar{v}} = \frac{\bar{u}}{\bar{v}}\, p_1^{r_1} + \sum_{j=1}^{r_1} f_{1j} p_1^{r_1-j},$$

donde cada f_{1j} es nulo o tiene grado menor que el de p_1 y $\bar{u} = u_r$ es primo con $\bar{v}$. Dividiendo entre $p_1^{r_1}$ obtenemos

$$z = \frac{u}{v} = \frac{\bar{u}}{\bar{v}} + \sum_{j=1}^{r_1} \frac{f_{1j}}{p_1^j},$$

que es la descomposición que buscábamos.

Ahora vamos a probar la unicidad. Supongamos que una misma fracción $z \in K(X)$ admite dos descomposiciones en factores simples. Pongamos que una de las descomposiciones tiene m fracciones (sin contar el polinomio inicial) y la otra n, con $m \leq n$. Razonamos por inducción sobre n. Si $n = 0$ tenemos simplemente dos polinomios, que trivialmente han de ser el mismo, pues ambos han de coincidir con z.

Consideremos una descomposición cualquiera:

$$z = f + \sum_{i=1}^{n} \sum_{j=1}^{r_i} \frac{f_{ij}}{p_i^j}$$

Al sumar todas las fracciones correspondientes a p_i, el denominador común es $p_i^{r_i}$, y el numerador es una suma en la que todos los sumandos son múltiplos de p_i menos uno ($f_{i,r_i} \neq 0$), luego tenemos que

$$z = f + \sum_{i=1}^{n} \frac{h_i}{p_i^{r_i}},$$

donde p_i no divide a h_i. Al efectuar la suma (incluyendo a f), con denominador común $p_1^{r_1} \cdots p_n^{r_n}$, el numerador es una suma de $n+1$ términos, todos los cuales son múltiplos de p_i menos uno, a saber, $p_1^{r_1} \cdots h_i \cdots p_n^{r_n}$, luego el numerador no es múltiplo de p_i. Así pues, concluimos que, si $z = u/v$ con u y v primos entre sí y v mónico, necesariamente $v = p_1^{r_1} \cdots p_n^{r_n}$ y que u no es divisible entre ninguno de los p_i.

Con esto hemos probado que, en cualquier descomposición de z en fracciones simples, los polinomios p_i son necesariamente los factores irreducibles de v, y los r_i son los exponentes con que aparecen en v.

Consideremos de nuevo las dos descomposiciones que estamos suponiendo que tiene z. Pongamos que una contiene el sumando $f_{1r_1}/p_1^{r_1}$ y la otra $g_{1r_1}/p_1^{r_1}$. Según hemos visto,

$$u = f_{1,r_1} p_2^{r_2} \cdots p_n^{r_n} + \text{ múltiplos de } p_1 \; = g_{1,r_1} p_2^{r_2} \cdots p_n^{r_n} + \text{ múltiplos de } p_1,$$

luego p_1 divide a $f_{1,r_1} - g_{1,r_1}$, lo cual sólo es posible si $f_{1,r_1} = g_{1,r_1}$, ya que ambos tienen grado menor que p_1.

Esto significa que podemos cancelar el sumando $f_{1,r_1}/p_1^{r_1}$ de ambas descomposiciones, y así llegamos a otra fracción que admite dos descomposiciones en factores simples de longitudes $m-1$ y $n-1$. Por hipótesis de inducción, ambas tienen que ser iguales, luego las dos descomposiciones de partida también coinciden. ∎

Teorema 4.4 *Sea $F \subset L$ una extensión de cuerpos diferenciales, donde $L = F(t)$ con t trascendente sobre F, y supongamos que, para cada $p(t) \in F[t]$, también $p(t)' \in F[t]$, y que si $p(t)$ es mónico e irreducible, el grado de $p(t)'$ es menor que el de $p(t)$. Entonces, para cada $v \in L$, la descomposición en fracciones simples de v' tiene como denominadores los mismos polinomios irreducibles que aparecen en la descomposición de v, pero el exponente máximo con que cada uno de ellos aparece en v' es una unidad más que el que tiene en v. (En particular, este exponente máximo es siempre ≥ 2.)*

DEMOSTRACIÓN: Sea

$$v = f + \sum_{i=1}^{n} \sum_{j=1}^{r_i} \frac{f_{ij}}{p_i^j}$$

la descomposición de v en fracciones simples. Al derivar obtenemos

$$v' = f' + \sum_{i=1}^{n} \sum_{j=1}^{r_i} \left(\frac{f'_{ij}}{p_i^j} + \frac{-j f_{ij} p'_i}{p_i^{j+1}} \right).$$

Ahora observamos que p_i no divide ni a f_{ij} ni a p'_i, porque ambos polinomios tienen grado menor que el de p_i. Por lo tanto, en la división euclídea $-j f_{ij} p'_i = g_{ij} p_i + h_{ij}$, el resto h_{ij} es no nulo, y tenemos

$$v' = f' + \sum_{i=1}^{n} \sum_{j=1}^{r_i} \left(\frac{f'_{ij} + g_{ij}}{p_i^j} + \frac{h_{ij}}{p_i^{j+1}} \right)$$

$$= f' + \sum_{i=1}^{n} \left(\frac{f'_{i1} + g_{i1}}{p_i} + \sum_{j=2}^{r_i} \frac{f'_{ij} + g_{ij} + h_{i,j-1}}{p_i^j} + \frac{h_{i,r_i}}{p_i^{r_i+1}} \right).$$

En suma, hemos llegado a una expresión de la forma

$$v' = \bar{f} + \sum_{i=1}^{n} \sum_{j=1}^{r_i+1} \frac{\bar{f}_{ij}}{p_i^j},$$

donde $\bar{f}_{i,r_i+1} = h_{i,r_i}$ es un polinomio no nulo de grado menor que p_i. Los otros polinomios $\bar{f}_{ij}$ no tienen por qué tener grado menor que p_i, lo cual nos obliga a dividirlos entre p_i y pasar el cociente al sumando anterior. Así llegamos a la descomposición de v' en fracciones simples, pero este proceso no añade nuevos polinomios irreducibles p_i ni elimina ninguno, ya que el sumando de mayor grado sigue siendo $h_{i,r_1}/p_i^{r_i+1}$. ∎

El teorema siguiente contiene algunos hechos técnicos elementales que vamos a necesitar en la prueba del resultado principal de esta sección. Observemos que el apartado 1. implica que las hipótesis del teorema anterior se satisfacen cuando $t' \in F$. Por ejemplo, esto sucede si $L = \mathbb{C}(z)$, $F = \mathbb{C}$ y consideramos a L como cuerpo diferencial con la derivada usual, con la que $z' = 1 \in F$.

Teorema 4.5 *Sea $F \subset L$ una extensión de cuerpos diferenciales, donde $L = F(t)$ para un cierto $t \in L$ trascendente sobre F. Supongamos además que F y L tienen el mismo cuerpo de constantes.*

1. *Si $t' \in F$, para cada polinomio $f(t) \in F[t]$ de grado positivo, la derivada $f(t)'$ es un polinomio en $F[t]$ del mismo grado que $f(t)$ si el coeficiente director de $f(t)$ no es constante, y de un grado menos si es constante.*

2. *Si $t'/t \in F$, entonces, para todo $a \in F$ no nulo y todo entero no nulo n, se cumple que $(at^n)' = ht^n$, para cierto $h \in F$ no nulo y, para cada polinomio $f(t) \in F[t]$ de grado positivo, la derivada $f(t)'$ es un polinomio en $F[t]$ del mismo grado, y es un múltiplo de $f(t)$ si y sólo si $f(t)$ es un monomio.*

DEMOSTRACIÓN: Supongamos que $t' = b \in F$ y sea $n > 0$ el grado de $f(t)$. Así,

$$f(t) = a_n t^n + a_{n-1}t^{n-1} + \cdots + a_0,$$

con $a_i \in F$, $a_n \neq 0$. La derivada es

$$f(t)' = a_n' t^n + (na_n b + a_{n-1}')t^{n-1} + \cdots$$

Claramente, es un polinomio en t de grado n si $a_n' \neq 0$. Si a_n es constante, hemos de ver que $na_n b + a_{n-1}' \neq 0$. En caso contrario tendríamos que

$$(na_n t + a_{n-1})' = na_n b + a_{n-1}' = 0,$$

luego $na_n t + a_{n-1}$ sería constante y, como F y L tienen las mismas constantes, sería $na_n t + a_{n-1} \in F$, de donde $t \in F$, lo cual es imposible, porque t es trascendente sobre F.

Supongamos ahora que $t'/t = b \in F$. Entonces

$$(at^n)' = a't^n + nat^{n-1}t' = (a' + nab)t^n.$$

Hemos de probar que $a' + nab \neq 0$. En caso contrario, $(at^n)' = 0$, luego $at^n \in F$ (por ser constante) y, como $a \neq 0$, esto implica que t es algebraico sobre F, contradicción.

La parte ya probada, aplicada a cada monomio de $f(t)$, implica que $f(t)'$ es un polinomio del mismo grado que $f(t)$. Si $f(t) = at^n$ es un monomio, ya hemos visto que $f(t)' = (h/a)at^n$ es múltiplo de $f(t)$. Recíprocamente, si $f(t)'$ es un múltiplo de $f(t)$, el cociente ha de tener grado 0, luego ha de ser un elemento $c \in F$. Si $f(t)$ no es un monomio, tendrá al menos dos monomios no nulos $f(t) = a_n t^n + a_m t^m + \cdots$ y entonces, según hemos visto,

$$f(t)' = (a_n' + na_n b)t^n + (a_m' + ma_m b)t^m + \cdots,$$

con lo que, igualando coeficientes en la relación $f'(t) = cf(t)$ obtenemos que

$$\frac{a_n' + na_n b}{a_n} = \frac{a_m' + na_m b}{a_m},$$

luego

$$\frac{a_n'}{a_n} + n\frac{t'}{t} = \frac{a_m'}{a_m} + m\frac{t'}{t},$$

luego, por el teorema 2.2:

$$\left(\frac{a_n t^n}{a_m t^m}\right)' = (a_n a_m^{-1} t^n t^{-m})' = (a_n a_m^{-1} t^n t^{-m})\left(\frac{a_n'}{a_n} - \frac{a_m'}{a_m} + n\frac{t'}{t} - m\frac{t'}{t}\right) = 0.$$

Esto implica que $a_n t^n / a_m t^m \in F$, en contra nuevamente de la trascendencia de t. ∎

El teorema siguiente es una generalización debida a Ostrowski en 1946 de un teorema de Liouville de 1835.

Teorema 4.6 *Sea F un cuerpo diferencial y $\alpha \in F$. Si la ecuación $y' = \alpha$ tiene solución elemental en una extensión diferencial de F con el mismo cuerpo de constantes, entonces existen constantes $c_1, \ldots, c_m \in F$ y elementos $u_1, \ldots, u_n, v \in F$ tales que*

$$\alpha = \sum_{i=1}^{m} c_i \frac{u_i'}{u_i} + v'.$$

DEMOSTRACIÓN: Por hipótesis tenemos una cadena de cuerpos diferenciales

$$F \subset F(t_1) \subset \cdots \subset F(t_1, \ldots, t_n),$$

todos con el mismo cuerpo de constantes, que cumplen la definición 2.4 y de modo que existe un $y \in F(t_1, \ldots, t_n)$ que cumple $y' = \alpha$. Vamos a probar el teorema por inducción sobre n. Si $n = 0$ entonces α tiene la forma indicada con $v = y$, $m = 0$.

Supongamos que el teorema es cierto para $n - 1$. Entonces, aplicando el teorema con $F(t_1)$ en lugar de F, tenemos que

$$\alpha = \sum_{i=1}^{m} c_i \frac{u_i'}{u_i} + v',$$

para ciertas constantes c_i y ciertos $u_i, v \in F(t)$ (donde, por simplificar la notación, llamamos $t = t_1$). Vamos a distinguir tres casos, según que t sea algebraico sobre F, la exponencial de un elemento de F o el logaritmo de un elemento de F.

Consideramos en primer lugar el caso en que t es algebraico sobre F. Sabemos que entonces todo elemento de $F(t)$ es un polinomio de $F[X]$ evaluado en t. Sean, pues, $U_i, V \in F[X]$ tales que $u_i = U_i(t)$, $v = V(t)$.

Por otra parte, consideremos el polinomio mínimo $p(X) \in F[X]$ de t sobre F. La teoría de extensiones de cuerpos nos asegura que F tiene una clausura algebraica, en la cual $p(X)$ factoriza en la forma

$$p(X) = (X - t_1) \cdots (X - t_s),$$

donde $t_1 = t$. En lugar de trabajar en la clausura algebraica de F, podemos restringirnos al subcuerpo $L = F(t_1, \ldots, t_s)$. El teorema del elemento primitivo nos da que $L = F(u)$, para un cierto $u \in L$, que es algebraico sobre F. Más aún,[5] para cada índice j, existe un automorfismo $\sigma_j : L \longrightarrow L$ que deja invariantes a los elementos de F y cumple $\sigma_j(t_1) = t_j$.

Observemos que el hecho de que $L = F(u)$ implica también que $L = F(t)(u)$, y u también es algebraico sobre $F(t)$. Así, el teorema 4.2 nos asegura que existe una única derivación en L que extiende a la de $F(t)$. Dicha derivación extiende también a la

[5]El cuerpo L es el cuerpo de escisión sobre F del polinomio p, por lo que la extensión L/F es finita normal, y es separable porque los cuerpos tienen característica 0. Véase el teorema 7.38 de mi libro de álgebra.

derivación de F y, por el mismo teorema, es la única que lo hace. En definitiva, tenemos una cadena de extensiones de cuerpos diferenciales $F \subset F(t) \subset L$.

La aplicación en L dada por $\beta^* = \sigma_j^{-1}(\sigma_j(\beta)')$ es claramente una derivación en L que extiende a la derivación de F, luego ha de ser $\sigma_j(\beta') = \sigma_j(\beta)'$ para todo índice j y todo $\beta \in L$.

Sabemos que la igualdad

$$\alpha = \sum_{i=1}^{m} c_i \frac{U_i(t_j)'}{U_i(t_j)} + V(t_j)'$$

se cumple en L para $j = 1$, porque se cumple en $F(t) \subset L$. El hecho de que los automorfismos σ_j conserven las sumas, los productos y las derivadas, y que dejen invariantes a los elementos de F (juntamente con el hecho de que los polinomios U_i, V tienen sus coeficientes en F), implica que la igualdad es cierta para todo j.

Sumando en j y aplicando el teorema 2.2 obtenemos:

$$\alpha = \sum_{i=1}^{m} \frac{c_i}{s} \frac{(U_i(t_1) \cdots U_i(t_s))'}{U_i(t_1) \cdots U_i(t_s)} + \frac{(V(t_1) + \cdots + V(t_s))'}{s}.$$

Ahora observamos que $\bar{u}_i = U_i(t_1) \cdots U_i(t_s)$ y $\bar{v} = V(t_1) + \cdots + V(t_s)$ permanecen invariantes por los automorfismos de L que fijan a F (porque éstos permutan las raíces de $p(X)$), luego la teoría de Galois nos asegura[6] que $\bar{u}_i, \bar{v} \in F$, luego llegamos a que α tiene la forma indicada en el enunciado del teorema.

En los dos casos que nos falta considerar, es decir, que t sea una exponencial o un logaritmo de una función de F, podemos suponer además que t es trascendente sobre F, pues el caso algebraico lo hemos resuelto ya.

Ahora ya no podemos afirmar que u_i y v_i sean polinomios de $F[X]$ evaluados en t, sino cocientes de polinomios. Concretamente, si

$$u_i = \frac{F(t)}{G(t)},$$

descomponiendo F y G en factores irreducibles podemos expresar

$$u_i = F_1(t)^{n_1} \cdots F_m(t)^{n_m},$$

donde los exponentes son enteros no nulos y los polinomios $F_i(t)$ son mónicos, irreducibles, distintos dos a dos salvo quizá uno de ellos, que puede ser un elemento de F (con lo que es una unidad de $F[X]$ y, por definición, no es irreducible).

El teorema 2.2 nos permite sustituir el sumando $c_i u_i'/u_i$ en la descomposición que tenemos de α por m sumandos análogos correspondientes a los polinomios F_i, de modo que podemos suponer que cada $u_i = U_i(t)$ es un polinomio mónico irreducible, o bien $u_i \in F$. Además podemos suponer que todos los u_i son distintos dos a dos, ya que si hubiera dos sumandos iguales podríamos agruparlos en uno sumando los correspondientes coeficientes c_i. Obviamente, podemos suponer además que $c_i \neq 0$ para todo i.

[6] Véase el teorema 7.32 de mi libro de álgebra.

A partir de aquí vamos a distinguir los dos casos que nos quedan. Supongamos en primer lugar que t es un logaritmo de un elemento de F, es decir, que $t' = a'/a$, para cierto $a \in F$. En particular, $t' \in F$, luego el teorema anterior nos da que las derivadas de los polinomios tienen el mismo grado si el coeficiente director no es constante y una unidad menos si lo es. Tenemos que

$$v' = \alpha - \sum_{i=1}^{m} c_i \frac{u_i'}{u_i}.$$

El miembro derecho es (esencialmente) la descomposición de v' en fracciones simples. En efecto, tenemos que α, junto con los sumandos correspondientes a elementos $u_i \in F$, pueden verse como un polinomio de $F[t]$ de grado 0 (el polinomio inicial de la descomposición). Si, por el contrario, $u_i \in F[t]$ es irreducible, como su coeficiente director es 1 (constante) tenemos que $-c_i u_i'$ tiene grado menor que u_i, luego es, en efecto, una fracción simple, y tenemos que índices distintos corresponden a polinomios irreducibles distintos.

En definitiva, hemos probado que la descomposición de v' en fracciones simples tiene todos los denominadores irreducibles.

Ahora bien, el teorema 4.4 nos asegura que, en los denominadores de la descomposición de v' en fracciones simples, cada polinomio irreducible debe aparecer con exponente al menos 2. Esto es una contradicción salvo que la descomposición en fracciones simples no contenga fracciones simples, es decir, que se reduzca a un polinomio en $F[t]$.

Más concretamente, esto se traduce en que $u_i \in F$ para todo i, así como que $v \in F[t]$. Ahora bien, la igualdad nos da entonces que $v' \in F$ (es un polinomio de grado 0) y, como el grado de v' sólo puede ser una unidad menos que el grado de v, ha de ser $v(t) = ct + d$, para ciertos c, $d \in F$. Si $c \neq 0$, tenemos que la derivación reduce el grado y, según el teorema anterior, esto sólo puede ser si c es constante (luego c es una constante en cualquier caso). En definitiva, la igualdad se reduce ahora a

$$\alpha = \sum_{i=1}^{m} c_i \frac{u_i'}{u_i} + ct' + d',$$

donde ahora u_i, $d \in F$ y c es constante. Si sustituimos $t' = a'/a$, llegamos a una expresión como la que exige el enunciado.

Por último, consideramos el caso en que t es una exponencial de un elemento de F, es decir, que $t'/t = b'$, con $b \in F$. Si $p(t) \in F[t]$ es un polinomio mónico irreducible, entonces el teorema anterior nos da que $p(t)'$ es un polinomio del mismo grado, y será múltiplo de $p(t)$ si y sólo si éste un monomio, lo cual, siendo mónico e irreducible, sólo puede ser si $p(t) = t$.

Así pues, si $u_i \notin F$ y $u_i \neq t$, tenemos que u_i' no es múltiplo de u_i, luego al dividir $u_i' = g_i u_i + r_i$, se cumple que $r_i \neq 0$, y tenemos

$$c_i \frac{u_i'}{u_i} = c_i g_i + c_i \frac{r_i}{u_i}.$$

Con estas descomposiciones llegamos a la descomposición de v' en fracciones simples. (Si un $u_i = t$ entonces $u_i'/u_i = b'$ no contribuye a la descomposición en fracciones simples,

sino que este término se agrupa con el polinomio inicial.) Concluimos que, en la descomposición de v' en fracciones simples, los denominadores son los u_i que no están en F y que son distintos de t, y todos ellos aparecen con exponente máximo 1.

Notemos que ahora no se cumplen las hipótesis del teorema 4.4, puesto que ahora las derivadas de los polinomios no tienen grado menor, sino igual. No obstante, si observamos la prueba de 4.4, vemos que el único punto en el que hemos usado que el grado es menor es para asegurar que si p_i es uno de los polinomios irreducibles que aparecen en la descomposición en fracciones simples, entonces p_i no divide a p_i', y esto sigue siendo cierto en nuestro contexto salvo si $p_i = t$.

Como el argumento de 4.4 trata por separado a cada p_i, podemos concluir de todos modos que todos los polinomios distintos de t que aparezcan en la descomposición de v' en fracciones simples han de aparecer con exponente ≥ 2. Por lo tanto, podemos afirmar que $u_i \in K$ salvo quizá para un índice, para el que puede suceder $u_i = t$. Por otra parte, $v' \in F$, luego v tiene también grado 0, es decir, $v \in F$.

Si todos los u_i están en F, entonces ya tenemos la expresión buscada; si un $u_i = t$, digamos, $u_1 = t$, entonces

$$\alpha = c_1\frac{t'}{t} + \sum_{i=2}^{m} c_i\frac{u_i'}{u_i} + v' = \sum_{i=2}^{m} c_i\frac{u_i'}{u_i} + (c_1 b' + v)'$$

es la expresión buscada. ∎

Ejercicio Demostrar el recíproco del teorema anterior, es decir, que si α tiene la forma indicada, entonces existe una extensión diferencial de F en la cual α tiene una primitiva elemental. (AYUDA: Usar el teorema 4.1 para probar que existe una extensión diferencial de F en la que cada u_i tiene un logaritmo, y usar dichos logaritmos para definir la primitiva de α.)

En las secciones siguientes usaremos este teorema para mostrar ejemplos explícitos de funciones (de variable real) sin primitiva elemental. El teorema siguiente conecta el problema con las funciones de variable compleja:

Teorema 4.7 *Sea $f : [a,b] \longrightarrow \mathbb{R}$ una función elemental y sea $F : D \longrightarrow \mathbb{C}^\infty$ una extensión de f a una función meromorfa elemental sobre un dominio complejo D. Si F no admite una primitiva elemental en ningún dominio $D_1 \subset D$, entonces la integral $\int f(x)\,dx$ no es elemental.*

DEMOSTRACIÓN: Supongamos que existe una función elemental $g : [a,b] \longrightarrow \mathbb{R}$ tal que $g'(x) = f(x)$ para todo $x \in [a,b]$. Por definición de función elemental (real), tenemos que g se extiende a una función meromorfa elemental en un dominio complejo que contiene a $[a,b]$. El teorema 3.2 nos da un dominio complejo $D_1 \subset D$, que contiene a $[a,b]$, donde están definidas y son holomorfas tanto F como G. Como $G'(z) = F(z)$ para todo $z \in [a,b]$, el principio de prolongación analítica implica que esto es cierto para todo $z \in D_1$, luego F admite una primitiva elemental en D_1, en contra de lo supuesto. ∎

5 Funciones trascendentes sin primitiva elemental

Las técnicas que vamos a emplear para justificar que una función dada no tiene primitiva elemental son distintas según si la función es trascendente o algebraica. En esta sección nos ocuparemos del caso trascendente, pues el caso algebraico requiere resultados adicionales sobre la teoría de cuerpos de funciones algebraicas. Para el caso que nos ocupa nos apoyaremos en el siguiente hecho elemental:

Teorema 5.1 *Sea $D \subset \mathbb{C}$ un dominio y sea $g \in \mathbb{C}(z)$ una función no constante que no tenga polos en D. Entonces, la función $t = e^{g(z)} \in \mathcal{M}(D)$ es trascendente sobre $\mathbb{C}(z)$.*

DEMOSTRACIÓN:[7] Supongamos que t es algebraica sobre $\mathbb{C}(z)$ y sea

$$p(X) = X^n + a_1 X^{n-1} + \cdots + a_n$$

el polinomio mínimo de t sobre $\mathbb{C}(z)$, donde $a_1, \ldots, a_n \in \mathbb{C}(z)$, de modo que

$$e^{ng} + a_1 e^{(n-1)g} + \cdots + a_n = 0.$$

Derivando obtenemos

$$ng' e^{ng} + (a_1' + (n-1)a_1 g')e^{(n-1)g} + \cdots + a_n' = 0.$$

Así pues, t es también raíz del polinomio

$$q(X) = ng' X^n + (a_1' + (n-1)a_1 g')X^{(n-1)} + \cdots + a_n',$$

que tiene grado n, porque $g' \neq 0$. Como $q(X)$ tiene también sus coeficientes en $\mathbb{C}(z)$ y $p(X)$ es el polinomio mínimo de t, concluimos que $p(X)$ ha de dividir a $q(X)$. Comparando los coeficientes directores, ha de ser $q(X) = ng'p(X)$, luego, en particular, $a_n' = ng'a_n$.

Ahora bien, esta igualdad es imposible, pues, descomponiendo

$$a_n = \alpha_0(z-\alpha_1)^{n_1} \cdots (z-\alpha_r)^{n_r},$$

con $\alpha_i \in \mathbb{C}$ distintos dos a dos y $n_i \in \mathbb{Z}$ no nulos, y aplicando el teorema 2.2, vemos que la descomposición de a_n'/a_n en fracciones simples consta únicamente de sumandos de la forma $n_i/(z-\alpha_i)$, es decir, que todos los factores primos $z-\alpha_i$ aparecen con exponente 1 (y no hay polinomio inicial). Sin embargo, el teorema 4.4 nos asegura que en los denominadores de la descomposición en fracciones irreducibles de $(ng)'$ todos los polinomios irreducibles han de aparecer con exponente ≥ 2. Tenemos así una contradicción. ∎

Veamos un primer criterio práctico para reconocer el carácter no elemental de una función:

[7] Hay una prueba muy breve de este hecho: sea E el conjunto (finito y no vacío) de los polos de g sobre la esfera de Riemann $\mathbb{C}^\infty$. Entonces t es holomorfa en $\mathbb{C}^\infty \setminus E$ y tiene singularidades esenciales en los puntos de E. Si t cumpliera una ecuación polinómica en D, sería una (rama uniforme de una) función algebraica en $\mathbb{C}^\infty$, pero las funciones algebraicas no tienen singularidades esenciales. (Véase el capítulo XIV de mi libro de funciones de variable compleja.)

Teorema 5.2 *Sea $D \subset \mathbb{C}$ un dominio, sean f, $g \in \mathbb{C}(z)$ y supongamos que g no es constante y no tiene polos en D. Existe una función elemental $y \in \mathcal{M}(D)$ tal que $y' = fe^g$ si y sólo si existe $a \in \mathbb{C}(z)$ tal que $f = a' + ag'$.*

DEMOSTRACIÓN: Una implicación es inmediata: si se cumple esta condición, basta tomar $y = ae^g$. Para probar el recíproco aplicamos el teorema 4.6 al cuerpo $\mathbb{C}(z,t)$, donde $t = e^g$. Ciertamente, $\alpha = fe^g \in \mathbb{C}(z,t)$ y, si existe una función elemental $y \in \mathcal{M}(D)$ tal que $y' = \alpha$, puesto que el cuerpo de constantes de $\mathcal{M}(D)$ es $\mathbb{C}$, el mismo que el de $\mathbb{C}(z,t)$, el teorema nos asegura que

$$ft = \sum_{i=1}^{m} c_i \frac{u_i'}{u_i} + v',$$

para ciertas constantes $c_i \in \mathbb{C}$, y ciertas funciones $u_i, v \in \mathbb{C}(z,t)$.

Llamemos $F = \mathbb{C}(z)$. El teorema anterior prueba que t es trascendente sobre F. Esto nos permite expresar cada $u_i \in F(t)$ en la forma $u_i = ap_1^{r_1} \cdots p_n^{r_n}$, donde $r_i \in \mathbb{Z}$, $a \in F$ y los p_i son polinomios mónicos irreducibles distintos dos a dos. El teorema 2.2 nos permite descomponer cada sumando u_i'/u_i de modo que podemos exigir que cada u_i sea, o bien una función de F, o bien un polinomio mónico irreducible en $F[t]$. Además, podemos suponer que los u_i son distintos dos a dos.

Nos encontramos exactamente en la misma situación del último caso del teorema 4.6: tenemos que $t'/t = g'$, luego t es una exponencial de $g \in F$; podemos aplicar el teorema 4.5, según el cual si $p(t)$ es un polinomio mónico irreducible, su derivada $p(t)'$ es un polinomio del mismo grado, pero no será divisible entre $p(t)$ salvo si $p(t) = t$. Esto hace que el miembro derecho de

$$v' = ft - \sum_{i=1}^{m} c_i \frac{u_i'}{u_i}$$

sea casi la descomposición de v' en fracciones simples: si $u_i \in F[t]$ es irreducible y distinto de t, dividimos $u_i' = g_i u_i + r_i$ y el resto resulta ser no nulo, con lo que obtenemos la descomposición

$$c_i \frac{u_i'}{u_i} = c_i g_i + c_i \frac{r_i}{u_i}.$$

El último sumando es una fracción simple y el primero forma parte del polinomio inicial de la descomposición. Si $u_i = t$, el sumando correspondiente es $c_i u_i'/u_i = c_i g' \in F$, y también pertenecen a F los sumandos correspondientes a cada $u_i \in F$.

En resumen, concluimos que los denominadores de las fracciones simples de v' son todos irreducibles. Por otra parte, el teorema 4.4 nos permite concluir (gracias a las mismas observaciones hechas en la prueba de 4.6) que todos los polinomios irreducibles que aparezcan en la descomposición han de aparecer con exponente ≥ 2 salvo quizá t.

La conclusión es que $u_i \in F$ para todo i salvo si $u_i = t$, así como que los denominadores de las fracciones simples de v son todos potencias de t. Por consiguiente, dicha descomposición se reduce a

$$v = \sum_{j=-r}^{n} b_j t^j,$$

donde $b_j \in F$ y $r \geq 0$ es el exponente de t en la descomposición. Aunque existiera un $u_i = t$, se cumple que

$$\sum_{i=1}^{m} c_i \frac{u_i'}{u_i} \in F,$$

es decir, que $v' - ft \in F$. Explícitamente:

$$v' - ft = \sum_{j=-r}^{n} (b_j' + jg'b_j)t^j - ft,$$

luego todos los sumandos son nulos salvo quizá el correspondiente a $j = 0$. En particular, para $j = 1$ tenemos que $b_1' + g'b_1 - f = 0$, luego basta tomar $a = b_1$ para tener la relación que buscábamos. ∎

Ejemplo *Si $g(x)$ es un polinomio de grado ≥ 2, la integral*

$$\int e^{g(x)} dx$$

no es elemental.

En efecto, por 4.7, basta probar que la función holomorfa $e^{g(z)}$ no admite una primitiva elemental en ningún dominio complejo. Si la tuviera, por el teorema anterior existiría una función $a \in \mathbb{C}(z)$ tal que $a' + ag' = 1$. Vamos a ver que esto es imposible. Expresemos la ecuación en la forma

$$\frac{a'}{a} = \frac{1}{a} - g'$$

y descompongamos en factores $a = \alpha_0(z - \alpha_1)^{r_1} \cdots (z - \alpha_n)^{r_n}$, con $\alpha_i \in \mathbb{C}$ y $r_i \in \mathbb{Z}$. El teorema 2.2 nos da que

$$\frac{a'}{a} = \sum_{i=1}^{n} \frac{r_i}{z - \alpha_i},$$

y ésta es, pues, la descomposición en fracciones simples de a'/a. Vemos que en ella aparecen todos los polinomios $z - \alpha_i$ con exponente 1. Lo mismo tiene que valer, pues, para $1/a$, pero los únicos polinomios que pueden aparecer como denominadores en su desarrollo en fracciones simples son los divisores del denominador de su expresión como cociente de polinomios primos entre sí, y éstos son los que en la factorización de a aparecen con exponente positivo.

Concluimos que todos los factores de la descomposición de a aparecen con exponente positivo (de hecho, igual a 1), con lo que a es un polinomio, pero entonces la igualdad $a' + ag' = 1$ se vuelve claramente imposible, pues el grado de g' es ≥ 1 y el de a' es menor que el de a. ∎

En particular hemos probado que la integral

$$\int e^{-x^2/2} dx,$$

que define la distribución normal, no tiene primitiva elemental.

Ejemplo El teorema de los números primos afirma que la función $\pi(x)$ definida como el número de números primos menores o iguales que x es asintóticamente igual a la *integral logarítmica:*

$$\pi(x) \sim \mathrm{Il}(x) = \int_2^x \frac{dt}{\log t}.$$

Vamos a probar que esta función tampoco es elemental. En primer lugar observamos que el cambio de variable $x = \log t$ la transforma en

$$\int \frac{e^x}{x}\, dx,$$

por lo que basta ver que esta integral no es elemental. Según el teorema 4.7, basta ver que la función meromorfa e^z/z no admite primitiva elemental, y por 5.2 basta probar que la ecuación

$$\frac{1}{z} = a + a'$$

no tiene solución $a \in \mathbb{C}(z)$. Razonando como en el ejemplo anterior, la expresamos en la forma

$$\frac{a'}{a} = \frac{1}{za} - 1$$

Nuevamente, en el desarrollo en fracciones simples del miembro izquierdo aparecen todos los polinomios $z - \alpha_i$ con exponente 1, luego, en la factorización de a, todos los polinomios $z-\alpha_i$ han de aparecer con exponente positivo salvo quizá uno (necesariamente igual a z, si es que aparece) que puede aparecer con exponente -1.

Concluimos que $a = P(z)/z$, con $P(z) \in \mathbb{C}[z]$. La ecuación original es, por lo tanto,

$$\frac{1}{z} = \frac{P(z)}{z} + \frac{P'(z)z - P(z)}{z^2},$$

o también

$$z = (z-1)P(z) + P'(z)z.$$

Comparando los grados, $P(z)$ tiene que ser constante, pero entonces la ecuación se reduce a $z = \alpha(z-1)$, y esto es imposible. ∎

Si analizamos la prueba del teorema 5.2, nos daremos cuenta de que el hecho de que la función considerada fuera precisamente $\alpha = ft$ y no otra función cualquiera de $F(t)$, sólo se usa en dos ocasiones:

La primera es al justificar que los denominadores de las fracciones simples del miembro derecho de

$$v' = \alpha - \sum_{i=1}^{m} c_i \frac{u_i'}{u_i}$$

son todos irreducibles. Pero aquí lo único que importa es que $\alpha \in F[t]$, por lo que no aporta fracciones simples al miembro derecho. Por consiguiente, este paso es válido si α es cualquier polinomio de $F[t]$. Más aún, si α es de la forma

$$\alpha = \sum_{j=-k}^{n} a_j t^j,$$

con $a_j \in F$, las únicas fracciones simples que aportará al miembro derecho tendrán denominador potencia de t, luego seguirá siendo cierto que todos los denominadores de las fracciones simples que no sean potencias de t son irreducibles y, al compararlos con la descomposición de v' calculada a partir de la de v, concluimos igualmente que $u_i \in F$ para todo i salvo quizá en un caso, que podría ser $u_i = t$. Por otra parte, v sigue siendo necesariamente de la forma

$$v = \sum_{j=-r}^{n} b_j t^j,$$

y se ha de cumplir que $v' - \alpha \in F$. En este punto es donde, por segunda y última vez, se usa la expresión concreta de α. En el caso general obtenemos la condición

$$\sum_{j=-r}^{n} (b_j' + jg'b_j - a_j)t^j \in F,$$

lo que se traduce en que, para todo $j \neq 0$, han de existir funciones $b_j \in F$ tales que

$$a_j = b_j' + jg'b_j.$$

Obviamente, estas condiciones son triviales si $a_j = 0$, pues basta tomar $b_j = 0$. Con esto hemos probado la siguiente generalización del teorema 5.2:

Teorema 5.3 *Sea $D \subset \mathbb{C}$ un dominio, sea $g \in \mathbb{C}(z)$ y supongamos que g no es constante y no tiene polos en D. Sea $t = e^g \in \mathcal{M}(D)$, sea $\alpha \in \mathbb{C}(z)(t)$ una función de la forma*

$$\alpha = \sum_{j=-k}^{n} a_j t^j,$$

donde $a_j \in \mathbb{C}(z)$. Si existe una función elemental $y \in \mathcal{M}(D)$ tal que $y' = \alpha$, entonces, para cada $j \neq 0$, existe una función $b_j \in \mathbb{C}(z)$ tal que

$$a_j = b_j' + jg'b_j.$$

Ejemplo *La integral*

$$\int \frac{\operatorname{sen} x}{x}\, dx$$

no es elemental.

Basta probar que la función meromorfa $(\operatorname{sen} z)/z$ no tiene primitiva elemental en ningún dominio complejo. En primer lugar realizamos un cambio de variable: si existiera una función elemental $G(z)$ tal que $G'(z) = (\operatorname{sen} z)/z$ (en un dominio complejo cualquiera), entonces la función $F(z) = -2iG(iz)$ también sería elemental en dicho dominio, y su derivada sería

$$F'(z) = 2G'(iz) = 2\,\frac{\operatorname{sen} iz}{iz} = \frac{e^z - e^{-z}}{z}.$$

Basta probar, pues, que esta última función no admite una primitiva elemental.

Vamos a aplicar el teorema 5.3. Si llamamos $t = e^z$, vemos que

$$\alpha = \frac{t - t^{-1}}{z} = -\frac{1}{z}t^{-1} + \frac{1}{z}\,t.$$

Por consiguiente, si α tiene una primitiva elemental, existen funciones b_1, $b_{-1} \in \mathbb{C}(z)$ tales que

$$b_1' + b_1 = \frac{1}{z}, \qquad b_{-1}' - b_{-1} = -\frac{1}{z}.$$

Basta probar que la primera ecuación es imposible, pero eso ya lo hemos visto en el ejemplo anterior (donde la incógnita se llamaba a). ∎

Ejemplo *Si $f(x)$ es un polinomio de grado ≥ 2, las integrales*

$$\int \operatorname{sen} f(x)\,dx, \quad y \quad \int \cos f(x)\,dx$$

no son elementales.

En efecto, basta probar que las funciones holomorfas

$$\operatorname{sen} f(z) = \frac{e^{if(z)} - e^{-if(z)}}{2i} \quad \text{y} \quad \cos f(z) = \frac{e^{if(z)} + e^{-if(z)}}{2}$$

no tienen primitiva elemental en ningún dominio complejo. Si la tuvieran, multiplicando la primitiva por $2i$ o por 2, respectivamente, obtendríamos una primitiva elemental de las funciones $\alpha = e^{g(z)} \pm e^{-g(z)}$, donde llamamos $g(z) = if(z)$. Basta probar, pues, que estas funciones no tienen primitiva elemental.

Para aplicar el teorema 5.3 llamamos $t = e^{g(z)}$ y observamos que $\alpha = t \pm t^{-1}$ tiene la forma adecuada. La condición necesaria para $j = 1$ es que exista $b_1 \in \mathbb{C}(z)$ tal que

$$b_1' + g' b_1 = 1,$$

pero ya hemos demostrado que esta ecuación no tiene solución al estudiar la integrabilidad de $e^{g(z)}$. ∎

Ejercicio Probar que la integral $\int e^{e^x}\,dx$ no es elemental (AYUDA: Considerar el cambio de variable $t = e^x$.)

Ejercicio Probar que la integral $\int \log\log x\,dx$ no es elemental. (AYUDA: Integrar por partes.)

Ejercicio Probar que la integral $\int e^x \log x\,dx$ no es elemental.

6 Cuerpos de funciones algebraicas

Recogemos en esta sección los preliminares necesarios para la sección siguiente, en la que presentaremos ejemplos de funciones algebraicas sin primitiva elemental. Concretamente, necesitaremos algunos hechos básicos de la teoría de cuerpos de funciones algebraicas que enunciaremos sin demostración.[8]

[8] Todo lo que necesitamos se encuentra en mi libro de *Geometría algebraica,* al que harán referencia las citas entre corchetes. Una alternativa al enfoque algebraico que vamos a seguir sería considerar formas diferenciales en superficies de Riemann. Indicaremos (sin pruebas) las conexiones entre ambos puntos de vista.

Recordemos que un *cuerpo de funciones algebraicas* sobre un cuerpo de constantes k es una extensión finita del cuerpo de funciones racionales $k(z)$. Aquí vamos a restringirnos al caso en el que el cuerpo de constantes es $k = \mathbb{C}$. El hecho de que sea algebraicamente cerrado y de característica 0 simplifica bastante la teoría general.

En general, una *valoración* en un cuerpo F (definición [5.10]) es una aplicación suprayectiva $v : F^* \longrightarrow \mathbb{Z}$ que cumple las propiedades siguientes:

$$v(\alpha\beta) = v(\alpha) + v(\beta), \qquad v(\alpha + \beta) \geq \min\{v(\alpha), v(\beta)\}.$$

Si adoptamos el convenio de que $v(0) = +\infty$, entonces las propiedades anteriores se cumplen trivialmente si $\alpha = 0$ o $\beta = 0$.

Si F es un cuerpo de funciones algebraicas sobre $\mathbb{C}$, se llaman *divisores primos* (definición [6.5]) de F a las valoraciones en F que se anulan sobre $\mathbb{C}^*$. La *superficie de Riemann* de F se define como el conjunto Σ_F de todos los divisores primos de F. Aunque, por definición, los divisores primos son valoraciones, los representaremos con letras góticas, como $\mathfrak{p}$, cuando pensemos en ellos como puntos de Σ_F y con la notación $v_\mathfrak{p}$ cuando pensemos en ellos como valoraciones.[9] De este modo, diremos que $v_\mathfrak{p} : F^* \longrightarrow \mathbb{Z}$ es la valoración asociada al divisor $\mathfrak{p}$, aunque técnicamente $v_\mathfrak{p} = \mathfrak{p}$. A los divisores primos de F los llamaremos también *puntos* de la superficie Σ_F.

Si $f \in F^*$, diremos que f tiene un *cero* de orden n en el punto $\mathfrak{p} \in \Sigma_F$ si $v_\mathfrak{p}(f) = n > 0$, y que tiene un *polo* de orden n en $\mathfrak{p}$ si $v_\mathfrak{p}(f) = -n < 0$. Según el teorema [6.22] las funciones de F^* que no tienen ni ceros ni polos en Σ_F son exactamente las constantes[10] (no nulas).

Por ejemplo ([6.14]), si $F = \mathbb{C}(z)$, podemos identificar Σ_F con la esfera de Riemann $\mathbb{C}^\infty = \mathbb{C} \cup \{\infty\}$. Concretamente, para cada $\alpha \in \mathbb{C}$, la valoración v_α es la determinada por que, para todo $p(z) \in \mathbb{C}[z]$, se cumple que $v_\alpha(p(z))$ es la multiplicidad con la que $z - \alpha$ divide a $p(z)$ (o, equivalentemente, el orden de α como cero de $p(z)$). La valoración asociada a ∞ viene dada por $v_\infty(p(z)) = -\operatorname{grad} p(z)$.

Si F es un cuerpo de funciones algebraicas arbitrario, podemos definir una aplicación $\phi : \Sigma_F \longrightarrow \mathbb{C}^\infty$ del modo siguiente (teorema [6.10]): si $\mathfrak{p} \in \Sigma_F$, la restricción de $v_\mathfrak{p}$ a $\mathbb{C}(z)$ no es necesariamente un divisor primo de $\mathbb{C}(z)$ porque ya no tiene por qué ser suprayectiva. No obstante, existe un número natural $e \geq 1$ tal que $v_\mathfrak{p}|_{\mathbb{C}(z)}/e$ es una valoración en $\mathbb{C}(z)$. Equivalentemente, existe un (único) $p \in \mathbb{C}^\infty$ tal que $v_\mathfrak{p}|_{\mathbb{C}(z)} = ev_p$. (Se dice entonces que $\mathfrak{p}$ *divide* a p.) La aplicación ϕ viene dada por $\phi(\mathfrak{p}) = p$. El número e se llama *índice de ramificación* de $\mathfrak{p}$.

Cada divisor primo $\mathfrak{p}$ de un cuerpo de funciones algebraicas F define un *valor absoluto* (definición [5.1]) en F mediante $|\alpha|_\mathfrak{p} = 1/2^{v_\mathfrak{p}(\alpha)}$, entendiendo que $|0|_\mathfrak{p} = 0$. Este valor absoluto determina una métrica en F que no es completa, pero podemos construir la *compleción* de F, que es un cuerpo $F_\mathfrak{p}$ al cual se extiende de forma única la valoración $v_\mathfrak{p}$,

[9] La razón de esta notación es que puede probarse (teorema [6.23]) que Σ_F admite una estructura natural de superficie de Riemann compacta tal que F se identifica con su cuerpo de funciones meromorfas. Si pensamos en $f \in F$ como función meromorfa sobre Σ_F, entonces $v_\mathfrak{p}(f)$ es el orden del cero (o del polo, si es negativo) de la función f en el punto $\mathfrak{p}$, en el sentido de la teoría de funciones de variable compleja. No vamos a necesitar este hecho.

[10] Nótese que, como $\mathbb{C}$ es algebraicamente cerrado, $\mathbb{C}$ es también el cuerpo exacto de constantes de F, en el sentido de la definición [6.21].

de modo que, con la métrica inducida por esta extensión, es completo, y contiene a F como subcuerpo denso.

La estructura de $F_\mathfrak{p}$ es muy simple, ya que se trata de un cuerpo de series formales de potencias. Concretamente (teorema [6.42]), si $\pi \in F_\mathfrak{p}$ cumple que $v_\mathfrak{p}(\pi) = 1$ (y se dice entonces que π es un *primo* de $F_\mathfrak{p}$), entonces $F_\mathfrak{p} = \mathbb{C}((\pi))$, lo que significa que los elementos $f \in F_\mathfrak{p}$ son las series formales de potencias[11]

$$f = \sum_{-\infty \ll n} a_n \pi^n, \qquad \text{con } a_n \in \mathbb{C},$$

donde $-\infty \ll n$ significa que n toma valores desde un cierto entero n_0 hasta $+\infty$. Se cumple entonces que $v_\mathfrak{p}(f)$ es el menor entero n tal que $a_n \neq 0$.

En particular, si $p \in \mathbb{C}^\infty$ es un primo finito, de modo que existe un $\alpha \in \mathbb{C}$ tal que $v_p(z - \alpha) = 1$, la compleción $\mathbb{C}(z)_p$ está formada por las series de potencias

$$f = \sum_{-\infty \ll n} a_n (z - \alpha)^n, \qquad \text{con } a_n \in \mathbb{C},$$

y si $p = \infty$ basta cambiar $z - \alpha$ por $1/z$.

Si F es un cuerpo de funciones algebraicas arbitrario, $\mathfrak{p} \in \Sigma_F$ y $p \in \mathbb{C}^\infty$ es el divisor primo de $\mathbb{C}(z)$ divisible entre $\mathfrak{p}$, podemos identificar la compleción $\mathbb{C}(z)_p$ con la clausura de $\mathbb{C}(z)$ en $F_\mathfrak{p}$, de modo que tenemos una extensión de cuerpos $\mathbb{C}(z)_p \subset F_\mathfrak{p}$. Las valoraciones v_p y $v_\mathfrak{p}$ se extienden a $\mathbb{C}(z)_p$ y $F_\mathfrak{p}$ respectivamente, y las extensiones siguen satisfaciendo la relación $v_\mathfrak{p}|_{\mathbb{C}(z)_p} = e v_p$, con el mismo índice de ramificación. Más aún, el teorema [5.32] afirma[12] que el índice de ramificación coincide con el grado de la extensión de las compleciones, es decir:

$$e = |F_\mathfrak{p} : \mathbb{C}(z)_p|.$$

Esta relación es útil a la hora de calcular índices de ramificación. Observemos también que si $F = \mathbb{C}(z)(\alpha)$, entonces $F \subset \mathbb{C}(z)_p(\alpha) \subset F_\mathfrak{p}$. El teorema [5.27] implica que $\mathbb{C}(z)_p(\alpha)$ es completo respecto a la métrica inducida desde $F_\mathfrak{p}$, luego es cerrado en $F_\mathfrak{p}$ y, como F es denso, ha de ser $F_\mathfrak{p} = \mathbb{C}(z)_p(\alpha)$. Como $\mathbb{C}(z) \subset \mathbb{C}(z)_p$, el polinomio mínimo de α sobre $\mathbb{C}(z)_p$ divide al polinomio mínimo sobre $\mathbb{C}(z)$, luego $e = |F_\mathfrak{p} : \mathbb{C}(z)_p|$ es menor o igual que el grado $|F : \mathbb{C}(z)|$.

Veamos un ejemplo de aplicación de estos hechos:

Teorema 6.1 *Sea $F = \mathbb{C}(z, \sqrt{\alpha})$, para cierto $\alpha \in \mathbb{C}(z)$ no nulo. Si $\mathfrak{p} \in \Sigma_F$ y $p \in \mathbb{C}^\infty$ es el primo al que divide, entonces su índice de ramificación es $e = 1$ si $v_p(\alpha)$ es par y es $e = 2$ si $v_p(\alpha)$ es impar.*

Demostración: Llamemos $y = \sqrt{\alpha}$, donde esta notación ha de entenderse simplemente como que y es un elemento de una extensión de $\mathbb{C}(z)$ que cumple $y^2 = \alpha$. Entonces

[11] Si, concretamente, tomamos $\pi \in F$, el hecho de que $v_\mathfrak{p}(\pi) = 1$ equivale a que, viendo a π como función meromorfa en Σ_F, es localmente inyectiva en un entorno de $\mathfrak{p}$, por lo que puede tomarse como carta de la superficie de Riemann, y entonces el desarrollo en serie de potencias no es más que el desarrollo en serie de Laurent de f respecto de la carta π.

[12] Notemos que como, en nuestro caso, el cuerpo de constantes $\mathbb{C}$ es algebraicamente cerrado, el grado de inercia que aparece en el teorema [5.32] es $f = 1$.

$2v_\mathfrak{p}(y) = v_\mathfrak{p}(\alpha) = ev_p(\alpha)$. Como F tiene grado ≤ 2 sobre $\mathbb{C}(z)$, sabemos que $e = 1, 2$ y, si $v_p(\alpha)$ es impar, ha de ser necesariamente $e = 2$.

Supongamos ahora que $v_p(\alpha) = 2k$ y sea $\pi \in \mathbb{C}(z)$ tal que $v_p(\pi) = 1$. Entonces $\alpha = \epsilon\pi^{2k}$, donde $\epsilon = \alpha\pi^{-2k}$ cumple $v_p(\epsilon) = 0$. Llamemos $w = \pi^{-k}y$. Así, $w^2 = \epsilon$, y podemos expresar esto con la notación $w = \sqrt{\epsilon}$. Es claro que $F = \mathbb{C}(z, \sqrt{\epsilon})$, luego $F_\mathfrak{p} = \mathbb{C}(z)_p(\sqrt{\epsilon})$. Basta probar que $\sqrt{\epsilon} \in \mathbb{C}(z)_p$, pues entonces el índice de ramificación de $\mathfrak{p}$ será $e = |F_\mathfrak{p} : \mathbb{C}(z)_p| = 1$.

El hecho de que $v_p(\epsilon) = 0$ se traduce en que

$$\epsilon = \sum_{n=0}^{\infty} a_n \pi^n,$$

donde $a_n \in \mathbb{C}$, $a_0 \neq 0$. Sólo hemos de probar que existe otra serie de potencias

$$\eta = \sum_{n=0}^{\infty} b_n \pi^n \in \mathbb{C}(z)_p$$

tal que $\eta^2 = \epsilon$. Teniendo en cuenta la definición del producto de dos series de potencias, b_0 ha de cumplir que $b_0^2 = a_0$, luego podemos tomar como $b_0 \neq 0$ cualquiera de las dos raíces cuadradas (en $\mathbb{C}$) de a_0. A su vez, b_1 ha de cumplir la ecuación

$$b_0 b_1 + b_1 b_0 = a_1,$$

luego basta tomar $b_1 = a_1/2b_0$. Similarmente, b_2 ha de cumplir la ecuación

$$b_2 b_0 + b_1 b_1 + b_2 b_0 = a_2,$$

lo que se cumple con $b_2 = (a_2 - b_1^2)/(2b_0)$. Es fácil ver que, en general, b_n puede definirse recurrentemente sin más que despejar en una ecuación que no requiere sino dividir entre $2b_0 \neq 0$. Por consiguiente, existe la serie $\eta \in \mathbb{C}(z)_p$ que, por construcción, cumple $\eta^2 = \epsilon$, como había que probar.[13] ∎

Sea F un cuerpo de funciones algebraicas y $\mathfrak{p} \in \Sigma_F$. Para cada $f \in F_\mathfrak{p}$, que será de la forma

$$f = \sum_{-\infty \ll n} a_n \pi^n, \qquad \text{con } a_n \in \mathbb{C},$$

podemos definir ([8.1])

$$\frac{df}{d\pi} = \sum_{-\infty \ll n} n a_n \pi^{n-1},$$

de modo que $d/d\pi$ resulta ser una derivación en $F_\mathfrak{p}$. Las constantes para esta derivación (los elementos con derivada nula) son claramente los elementos de $\mathbb{C}$. Más en general, si $g \in F_\mathfrak{p}$ no es constante, podemos definir ([8.4]) una derivación d/dg en $F_\mathfrak{p}$ mediante

$$\frac{df}{dg} = \frac{\dfrac{df}{d\pi}}{\dfrac{dg}{d\pi}}.$$

[13] Notemos que $\mathbb{C}(z)_p$ está formado por *todas* las series de potencias de π con coeficientes en $\mathbb{C}$. No hay que probar que la serie η converja en ningún punto del plano complejo.

Se comprueba que d/dg es independiente de la elección del primo π. La derivación d/dz cumple $dz/dz = 1$, de donde se sigue que extiende a la derivación usual en $\mathbb{C}(z)$, luego, por el teorema 4.2, su restricción a F ha de ser la única derivación de F que extiende a la derivación usual de $\mathbb{C}(z)$.

Las *formas diferenciales* en $F_\mathfrak{p}$ se definen mediante la construcción adecuada para que, finalmente, resulten ser expresiones de la forma $\omega = f\,dg$, con f, $g \in F_\mathfrak{p}$, de modo que, si g_1 y g_2 no son constantes, la igualdad $f_1\,dg_1 = f_2\,dg_2$ equivale a que

$$f_1 = f_2\,\frac{dg_2}{dg_1}.$$

Convenimos además que $f\,dg = 0$ cuando g es constante (y sucede entonces que $g \in F_\mathfrak{p}$ es constante si y sólo si $dg = 0$). El conjunto de todas las formas diferenciales sobre $F_\mathfrak{p}$ tiene una estructura natural de espacio vectorial de dimensión 1 sobre $F_\mathfrak{p}$.

Esta relación hace que si $\omega = f\,dg \neq 0$ y π es un primo en $F_\mathfrak{p}$, el elemento

$$f\,\frac{dg}{d\pi} \in F_\mathfrak{p}$$

sea independiente de la elección de f y g y además sucede que

$$v_\mathfrak{p}(\omega) = v_\mathfrak{p}\Big(f\,\frac{dg}{d\pi}\Big)$$

es independiente de la elección de π.

Si $f \in F_\mathfrak{p}$ y $\pi \in F_\mathfrak{p}$ es primo, el *residuo* de f respecto de π se define ([8.6]) como el coeficiente $\mathrm{Res}_\pi(f) = a_{-1}$ del desarrollo de f en serie de potencias de π. El *residuo* de una forma diferencial $\omega = f\,dg$ es

$$\mathrm{Res}_\mathfrak{p}\,\omega = \mathrm{Res}_\pi(f\,\frac{dg}{d\pi}).$$

Se comprueba fácilmente que no depende de la representación de ω en términos de las funciones f y g, y el teorema [8.7] prueba que tampoco depende de la elección de π. Claramente, $\mathrm{Res}_\mathfrak{p}$ es una aplicación $\mathbb{C}$-lineal.

Si f, $g \in F$, definimos la *forma diferencial* $\omega = f\,dg$ como el elemento del producto de todos los espacios de formas diferenciales de todas las compleciones $F_\mathfrak{p}$ cuya componente $\mathfrak{p}$-ésima $\omega_\mathfrak{p}$ es la forma diferencial $f\,dg$ sobre $F_\mathfrak{p}$ que resulta de considerar a f y g como elementos de $F_\mathfrak{p}$. El conjunto de todas las formas diferenciales en F es un F-espacio vectorial de dimensión 1. Definimos

$$v_\mathfrak{p}(\omega) = v_\mathfrak{p}(\omega_\mathfrak{p}), \qquad \mathrm{Res}_\mathfrak{p}\,\omega = \mathrm{Res}_\mathfrak{p}\,\omega_\mathfrak{p},$$

de modo que $\mathrm{Res}_\mathfrak{p}$ es también una aplicación $\mathbb{C}$-lineal. Los órdenes $v_\mathfrak{p}(\omega)$ nos permiten hablar de ceros y polos de una forma diferencial en la superficie de Riemann Σ_F.

7 Funciones algebraicas sin primitiva elemental

Consideremos un cuerpo de funciones algebraicas $K = \mathbb{C}(z,t)$, donde t es algebraico sobre $\mathbb{C}(z)$, considerado como cuerpo diferencial con la única derivación que extiende a la derivación usual en $\mathbb{C}(z)$. Si el polinomio mínimo de t sobre $\mathbb{C}(z)$ es

$$p(T) = \textstyle\sum_{j=0}^{n} c_j T^j,$$

con $c_j \in \mathbb{C}(z)$, $c_n \neq 0$, en la prueba del teorema 2.5 hemos visto que

$$t' = -\frac{\displaystyle\sum_{j=0}^{n} c_j' t^j}{\displaystyle\sum_{j=1}^{n} j c_j t^{j-1}} \in \mathbb{C}(z,t).$$

Así pues, la derivada de una función algebraica (sobre $\mathbb{C}(z)$) es algebraica. Recíprocamente, una condición necesaria para que una función tenga una primitiva algebraica es que ella misma sea algebraica. Vamos a probar que, en tal caso, la primitiva está en la misma extensión algebraica de $\mathbb{C}(z)$ que la función dada:

Teorema 7.1 *Sea $F = \mathbb{C}(z,u)$ una extensión algebraica de $\mathbb{C}(z)$ y supongamos que u tiene una primitiva t algebraica sobre $\mathbb{C}(z)$. Entonces $t \in F$.*

DEMOSTRACIÓN: Si t es algebraica sobre $\mathbb{C}(z)$, en particular es algebraica sobre F. Consideramos su polinomio mínimo sobre F, que nos da una ecuación de la forma

$$\sum_{j=0}^{n} c_j t^j = 0,$$

para ciertos $c_j \in F$, con $c_n = 1$. Derivando obtenemos la relación

$$\sum_{j=1}^{n} j c_j u t^{j-1} + \sum_{j=0}^{n-1} c_j' t^j = 0.$$

Tal y como hemos observado antes de este teorema, $c_j' \in \mathbb{C}(z, c_j) \subset F$, luego tenemos una ecuación polinómica en t de grado $\leq n-1$ con coeficientes en F. Por la minimalidad de n, ha de ser idénticamente nula. En particular es nulo el coeficiente de t^{n-1}:

$$nu + c_{n-1}' = nt' + c_{n-1}' = 0.$$

De aquí se sigue que $nt + c_{n-1} \in \mathbb{C}$, luego $t \in \mathbb{C}(c_{n-1}) \subset F$. ∎

Obviamente, si una función algebraica tiene primitiva algebraica, ésta es elemental, luego una condición necesaria para que una función algebraica no tenga primitiva elemental es que sus primitivas sean trascendentes. El teorema anterior nos servirá para probar que así sucede en los casos particulares que consideraremos.

Teorema 7.2 *Si $P(z)$, $Q(z) \in \mathbb{C}[z]$ son polinomios tales que $Q(z)$ tiene raíces simples,* $\operatorname{grad} Q(z) > 1$ *y* $\operatorname{grad} P(z) < \operatorname{grad} Q(z) - 1$*, entonces la función*

$$\frac{P(z)}{\sqrt{Q(z)}}$$

no tiene primitiva algebraica.

DEMOSTRACIÓN: Llamemos $y = \sqrt{Q(z)}$, que ha de entenderse como un elemento de una extensión algebraica de $\mathbb{C}(z)$ tal que $y^2 = Q(z)$. Así la adjunción a $\mathbb{C}(z)$ de la función del enunciado es $\mathbb{C}(z, y)$. Por el teorema 7.1, si dicha función tuviera una primitiva algebraica, estaría en $\mathbb{C}(z, y)$, luego sería de la forma $a + by$, con a, $b \in \mathbb{C}(z)$ (donde usamos que el polinomio mínimo de y sobre $\mathbb{C}(z)$ tiene grado 2). Tenemos, pues, que

$$\frac{P}{y} = a' + b'y + by' = a' + b'y + \frac{bQ'}{2y}.$$

Reordenando:

$$a'y = P - b'Q - \frac{bQ'}{2}.$$

En esta expresión, el miembro derecho está en $\mathbb{C}(z)$, mientras que el miembro izquierdo sólo puede estarlo si $a' = 0$. Dividiendo la expresión entre bQ se convierte en

$$\frac{b'}{b} = \frac{P}{bQ} - \frac{Q'}{2Q}.$$

Si $b = \alpha_0(z - \alpha_1)^{r_1} \cdots (z - \alpha_n)^{r_n}$, con $r_i \in \mathbb{Z}$ y $Q = \beta_0(z - \beta_1) \cdots (z - \beta_m)$, entonces

$$\sum_i \frac{r_i}{z - \alpha_i} = \frac{P}{bQ} - \sum_j \frac{1/2}{z - \beta_j}.$$

El miembro izquierdo es la descomposición en factores simples del miembro derecho. Si un r_i es negativo, entonces α_i ha de coincidir con un β_j o, de lo contrario, $z - \alpha_i$ no aparecería como denominador en la descomposición en factores simples de P/bQ ni tampoco en la de todo el miembro derecho. Como Q tiene raíces simples, $z - \beta_j$ aparece en P/bQ con exponente ≥ 0, luego sigue sin aparecer como denominador en la descomposición en factores simples de este término, luego en la descomposición del miembro derecho aparece con numerador $-1/2$, mientras que en el miembro izquierdo aparece con numerador $r_i \in \mathbb{Z}$. Esta contradicción muestra que todos los r_i son positivos, luego b es un polinomio. Volvemos a la relación

$$P - b'Q - \frac{bQ'}{2} = 0.$$

El grado de P es menor que $m - 1$, mientras que los otros dos términos tienen grado $m + d - 1$, donde $d = \operatorname{grad} b$. Por lo tanto, el coeficiente director del miembro izquierdo es

$$-d\alpha_0\beta_0 - \frac{m\alpha_0\beta_0}{2} = 0,$$

lo cual nos lleva a que $d + m/2 = 0$, y esto es imposible, pues m y d son números naturales no nulos. ∎

Si una función algebraica α tiene primitiva algebraica, el teorema 7.1 nos da que ésta es una función $v \in \mathbb{C}(z,\alpha)$, luego la expresión que proporciona el teorema de Liouville 4.6 se reduce a $\alpha = v'$ (con $m = 0$). Recíprocamente, si α admite una expresión del tipo dado en el teorema 4.6 con $m = 0$, entonces sus primitivas son algebraicas (pues son funciones $v \in \mathbb{C}(z,\alpha)$ salvo una constante). Así pues, si α tiene una primitiva elemental trascendente, la expresión dada por el teorema de Liouville ha de tener $m \geq 1$.

Teorema 7.3 *Sea $F = \mathbb{C}(z,\alpha)$ una extensión algebraica de $\mathbb{C}(z)$ y supongamos que α admite una primitiva elemental trascendente. Si $m \geq 1$ es el mínimo natural tal que α admite una expresión de la forma*

$$\alpha = \sum_{i=1}^{m} c_i \frac{u_i'}{u_i} + v',$$

con $c_1, \ldots, c_m \in \mathbb{C}$ no nulos y $u_1, \ldots, u_m, v \in F$, entonces las constantes c_i son linealmente independientes sobre $\mathbb{Q}$.

Demostración: Supongamos que $c_1 = s_2c_2 + \cdots + s_mc_m$, con $s_i \in \mathbb{Q}$. Si $s_i = p_i/q_i$, con $p_i, q_i \in \mathbb{Z}$, tomamos $\bar{u}_i$ en una extensión algebraica[14] de F tal que[15] $\bar{u}_i^{q_i} = u_1^{p_i}$. Derivando obtenemos inmediatamente que

$$\frac{\bar{u}_i'}{\bar{u}_i} = s_i \frac{u_1'}{u_1}.$$

Por consiguiente, al sustituir c_1 como combinación lineal de las otras constantes, la expresión de α se convierte en

$$\alpha = \sum_{i=2}^{m} c_i \left(\frac{\bar{u}_i'}{\bar{u}_i} + \frac{u_i'}{u_i} \right) + v' = \sum_{i=2}^{m} c_i \frac{(\bar{u}_i u_i)'}{\bar{u}_i u_i} + v'.$$

Esta expresión no contradice la minimalidad de m porque las funciones $w_i = \bar{u}_i u_i$ no están en F, sino en una extensión finita L, que podemos suponer de Galois. Sea $G(L/F)$ el grupo de Galois de la extensión, es decir, el grupo de todos los automorfismos de L que fijan a F. Para cada $\sigma \in G(L/F)$ tenemos que

$$\alpha = \sigma(\alpha) = \sum_{i=2}^{m} c_i \frac{\sigma(w_i)'}{\sigma(w_i)} + v',$$

donde hemos usado que $\sigma(w_i)' = \sigma(w_i')$ debido a que la aplicación $x \mapsto \sigma(x')$ es una derivación en L que extiende a la de F y la extensión ha de ser única. Sumando para todo σ y aplicando el teorema 2.2 concluimos que

$$n\alpha = \sum_{i=2}^{m} c_i \frac{\mathrm{N}(w_i)'}{\mathrm{N}(w_i)} + nv',$$

[14]No necesitamos considerar a $\bar{u}_i$ como una función meromorfa, sino que el teorema 4.2 nos permite trabajar con el cuerpo $F(\bar{u}_2, \ldots, \bar{u}_m)$ considerado como un cuerpo diferencial en sentido abstracto.

[15]Podemos expresar esto en la forma $\bar{u}_i = u_1^{s_i}$, pero hay que tener presente que $\bar{u}_i$ no está unívocamente determinado por u_i y s_i.

donde la *norma* $\mathrm{N}(w_i)$ es el producto de todos los conjugados $\sigma(w_i)$, y es necesariamente[16] un elemento de F. Despejando α obtenemos una nueva expresión que —ahora sí— contradice la minimalidad de m. ∎

Con esto estamos en condiciones de probar el criterio que usaremos en la práctica para reconocer el carácter no elemental de la primitiva de una función algebraica:

Teorema 7.4 *Si $F = \mathbb{C}(z, \alpha)$ es una extensión finita de $\mathbb{C}(z)$ y α admite una primitiva elemental trascendente sobre $\mathbb{C}(z)$, entonces, la forma diferencial $\alpha\, dz$ tiene al menos un residuo no nulo.*

Demostración: Por el teorema 7.3 sabemos que

$$\alpha = \sum_{i=1}^{m} c_i \frac{u_i'}{u_i} + v',$$

para ciertas funciones u_i, $v \in F$ y ciertas constantes c_i independientes sobre $\mathbb{Q}$. Entonces, recordando que la derivación en F coincide con d/dz, resulta que

$$\alpha\, dz = \sum_{i=1}^{m} c_i \frac{du_i}{u_i} + dv,$$

luego, para cada divisor primo $\mathfrak{p}$ de F, se cumple que

$$\mathrm{Res}_{\mathfrak{p}}(\alpha\, dz) = \sum_{i=1}^{m} c_i \,\mathrm{Res}_{\mathfrak{p}}\Big(\frac{du_i}{u_i}\Big),$$

donde hemos usado que la diferencial exacta dv tiene residuos nulos, pues, si $v_{\mathfrak{p}}(\pi) = 1$, entonces

$$\mathrm{Res}_{\mathfrak{p}}(dv) = \mathrm{Res}_{\pi}\Big(\frac{dv}{d\pi}\Big) = 0,$$

ya que la derivada de una serie de potencias tiene nulo el coeficiente de índice -1. Por otra parte, se cumple que

$$\mathrm{Res}_{\mathfrak{p}}\Big(\frac{du_i}{u_i}\Big) = v_{\mathfrak{p}}(u_i).$$

En efecto, si $v_{\mathfrak{p}}(u_i) = n$, entonces podemos expresar $u_i = \epsilon\pi^n$, donde $\epsilon = u/\pi^n \in F_{\mathfrak{p}}$ cumple $v_{\mathfrak{p}}(\epsilon) = 0$, lo cual significa que el primer coeficiente no nulo de su serie de potencias es el de índice $i = 0$. Entonces,

$$\frac{1}{u_i}\frac{du_i}{d\pi} = \frac{1}{\epsilon}\frac{d\epsilon}{d\pi} + \frac{n}{\pi}.$$

Como

$$v_{\mathfrak{p}}\Big(\frac{1}{\epsilon}\frac{d\epsilon}{d\pi}\Big) = -v_{\mathfrak{p}}(\epsilon) + v_{\mathfrak{p}}\Big(\frac{d\epsilon}{d\pi}\Big) \geq 0,$$

[16] Véase la definición 8.44 de mi libro de Álgebra y las observaciones posteriores.

el desarrollo en serie de este término tiene nulos todos los coeficientes de índice negativo, luego

$$\mathrm{Res}_{\mathfrak{p}}\Big(\frac{du_i}{u_i}\Big) = \mathrm{Res}_{\pi}\Big(\frac{1}{u_i}\frac{du_i}{d\pi}\Big) = n = v_{\mathfrak{p}}(u_i).$$

En particular, los residuos son enteros. Tomemos, por ejemplo, u_1. Como no es constante, ha de haber un punto $\mathfrak{p} \in \Sigma_F$ tal que $v_{\mathfrak{p}}(u_1) \neq 0$, con lo que $\mathrm{Res}_{\mathfrak{p}}(\alpha\, dz)$ es combinación lineal de las constantes c_i con coeficientes enteros y, al menos uno de ellos, no nulo. La independencia lineal de los c_i implica que $\mathrm{Res}_{\mathfrak{p}}(\alpha\, dz) \neq 0$. ∎

Así pues, para probar que una función algebraica α no tiene primitiva elemental, basta ver que sus primitivas son trascendentes y que la forma diferencial $\alpha\, dz$ tiene todos sus residuos nulos.

Ejemplo *Supongamos que $P(x)$, $Q(x) \in \mathbb{R}[x]$ cumplen que $Q(x)$ tiene sólo raíces simples,* $\operatorname{grad} Q(x) = m \geq 3$ *y* $\operatorname{grad} P(x) < m/2 - 1$. *Entonces, la integral*

$$\int \frac{P(x)}{\sqrt{Q(x)}}\, dx$$

no es elemental.

Llamemos $y = \sqrt{Q(z)} \in F = \mathbb{C}(z, y)$. Basta probar que $P(z)/y$ no tiene primitiva (compleja) elemental. Sus primitivas son trascendentes por el teorema 7.2, luego, según el teorema 7.4, basta probar que los residuos de la forma diferencial $\omega = (P(z)/y)\, dz$ son nulos. Por la linealidad de los residuos, no perdemos generalidad si suponemos que $P(z) = z^r$, donde $0 \leq r \leq m/2 - 1$.

Tomemos $\mathfrak{p} \in \Sigma_F$ y sea $\pi \in F$ tal que $v_{\mathfrak{p}}(\pi) = 1$. Como $y^2 = Q(z)$, tenemos que

$$2v_{\mathfrak{p}}(y) = v_{\mathfrak{p}}(Q(z)).$$

Supongamos en primer lugar que $\mathfrak{p}$ divide a un primo finito de $\mathbb{C}(z)$, es decir, que existe un $\alpha \in \mathbb{C}$ tal que $v_{\mathfrak{p}}(z - \alpha) = e$, donde e es el índice de ramificación de $\mathfrak{p}$, que ha de ser $e = 1$ o $e = 2$.

Entonces $v_{\mathfrak{p}}(P(z)) \geq 0$, $v_{\mathfrak{p}}(Q(z)) \geq 0$, $v_{\mathfrak{p}}(z) \geq 0$. Si $Q(\alpha) \neq 0$, se cumple que $v_{\mathfrak{p}}(Q(z)) = 0$, luego también $v_{\mathfrak{p}}(y) = 0$. Por consiguiente,

$$v_{\mathfrak{p}}(\omega) = v_{\mathfrak{p}}\Big(\frac{P(z)}{y}\frac{dz}{d\pi}\Big) \geq 0,$$

pues z tiene un desarrollo en serie de potencias de π sin coeficientes de índice negativo, y lo mismo vale para su derivada. Esto implica, en particular, que $\mathrm{Res}_{\mathfrak{p}}\, \omega = 0$.

Supongamos ahora que $Q(\alpha) = 0$. Como las raíces de Q son simples, ha de ser $v_{\mathfrak{p}}(Q(z)) = e = 2v_{\mathfrak{p}}(y)$. Por lo tanto, $e = 2$ y $v_{\mathfrak{p}}(y) = 1$. Podemos calcular el residuo en $\mathfrak{p}$ tomando $\pi = y$. Observemos que $z - \alpha = \epsilon\pi^2$, con $v_{\mathfrak{p}}(\epsilon) = 0$. Por lo tanto,

$$\frac{dz}{d\pi} = \frac{d(z-\alpha)}{d\pi} = \frac{d\epsilon}{d\pi}\pi^2 + 2\epsilon\pi,$$

luego

$$v_{\mathfrak{p}}(\omega) = v_{\mathfrak{p}}\left(\frac{P(z)}{y}\frac{dz}{d\pi}\right) = v_{\mathfrak{p}}(z^r) + v_{\mathfrak{p}}\left(\frac{d\epsilon}{d\pi}\pi + 2\epsilon\right) \geq 0$$

y concluimos igualmente que el residuo es nulo. Falta considerar el caso en que $\mathfrak{p}$ divide al primo infinito de $\mathbb{C}(z)$. Como $v_p(Q(z)) = -m$, el teorema 6.1 nos da que el índice de ramificación es $e = 2$ si m es impar y $e = 1$ si m es par.

Supongamos en primer lugar que m es impar, de modo que $v_\mathfrak{p}(z) = -2$, $v_\mathfrak{p}(y) = -m$. Entonces $z = \epsilon\pi^{-2}$, $y = \eta\pi^{-m}$, donde $v_\mathfrak{p}(\epsilon) = v_\mathfrak{p}(\eta) = 0$. Así,

$$\frac{P(z)}{y}\frac{dz}{d\pi} = \frac{\epsilon^r\pi^{-2r}}{\eta\pi^{-m}}\left(\frac{d\epsilon}{d\pi}\pi^{-2} - 2\epsilon\pi^{-3}\right) = \frac{\epsilon^r}{\eta}\left(\frac{d\epsilon}{d\pi}\pi^{m-2r-2} - 2\epsilon\pi^{m-2r-3}\right).$$

La hipótesis $r < m/2 - 1$ implica que $m - 2r - 2 > 0$, $m - 2r - 3 \geq 0$, luego $v_\mathfrak{p}(\omega) \geq 0$ y el residuo es nulo.

Por último, supongamos que m es par, con lo que $e = 1$, $v_\mathfrak{p}(y) = -m/2$. Podemos tomar $\pi = 1/z$, con lo que $z = \pi^{-1}$ y

$$\frac{P(z)}{y}\frac{dz}{d\pi} = \frac{\pi^{-r}}{\eta\pi^{-m/2}}(-\pi^{-2}) = -\eta^{-1}\pi^{m/2-r-2}.$$

Nuevamente concluimos $v_\mathfrak{p}(\omega) \geq 0$ y el residuo es nulo. ∎

Conviene observar que la hipótesis sobre el grado de $P(x)$ sólo la hemos usado para probar que los residuos en los primos infinitos son nulos.[17] Los residuos en los primos finitos son nulos para cualquier $P(x)$.

Con esto casi tenemos probado el carácter no elemental de una integral famosa. Respecto a un sistema de referencia adecuado, toda elipse admite una ecuación de la forma

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1, \qquad a \geq b > 0.$$

El número $0 \leq k < 1$ dado por $k^2 = (a^2 - b^2)/a^2$ es la *excentricidad* de la elipse. Aplicando una homotecia podemos suponer que el semieje mayor es $a = 1$, con lo que la excentricidad es $k = \sqrt{1 - b^2}$. Para calcular el elemento de longitud despejamos $y(x) = b\sqrt{1 - x^2}$, con lo que

$$ds = \sqrt{1 + y'(x)^2}\,dx = \sqrt{\frac{1 - k^2x^2}{1 - x^2}}\,dx = \frac{1 - k^2x^2}{\sqrt{(1 - x^2)(1 - k^2x^2)}}\,dx.$$

Consecuentemente, la longitud del arco de elipse comprendido entre $x = 0$ y $x = x_1 \leq 1$ es

$$s(x_1) = \int_0^{x_1} \frac{1 - k^2x^2}{\sqrt{(1 - x^2)(1 - k^2x^2)}}\,dx.$$

Esta integral es la que ha dado lugar a que se llame *integrales elípticas* a las integrales de funciones racionales de una raíz cuadrada de un polinomio de grado 3 o 4 (el grado 4 se puede reducir a grado 3 mediante un cambio de variable).

[17] En realidad, lo que hemos probado es que el integrando es una forma diferencial *de primera clase,* es decir, que no tiene polos, lo cual es más fuerte que el mero hecho de tener residuos nulos.

Ejemplo Si $0 < k < 1$, la integral

$$\int \frac{1-k^2x^2}{\sqrt{(1-x^2)(1-k^2x^2)}}\,dx$$

no es elemental.

El teorema 7.2 nos garantiza que la primitiva no es algebraica. Sólo hemos de probar que el integrando tiene residuos nulos. Podemos descomponer la integral como combinación lineal de dos:

$$I_1 = \int \frac{dx}{\sqrt{(1-x^2)(1-k^2x^2)}}, \qquad I_2 = \int \frac{x^2}{\sqrt{(1-x^2)(1-k^2x^2)}}\,dx.$$

La primera tiene residuos nulos —y, por consiguiente, no es elemental— por el ejemplo anterior, luego basta probar que la segunda tiene también residuos nulos. La segunda no cumple la condición del ejemplo anterior sobre el grado del numerador, pero hemos visto que eso no impide probar que el integrando tiene residuos nulos en todos los divisores primos finitos.

Llamemos, pues $y = \sqrt{(1-z^2)(1-k^2z^2)}$, sea $F = \mathbb{C}(z,y)$, tomemos un primo infinito $\mathfrak{p} \in \Sigma_F$ y veamos que la forma diferencial $\omega = z^2\,dz/y$ tiene residuo nulo en $\mathfrak{p}$. Como el grado del radicando es par, el teorema 6.1 implica que el índice de ramificación es $e = 1$, por lo que $\pi = 1/z$ cumple $v_\mathfrak{p}(\pi) = 1$. Vamos a seguir la prueba de 6.1, para lo cual expresamos

$$(1-z^2)(1-k^2z^2) = \pi^{-4}(\pi^2-1)(\pi^2-k^2)$$

y llamamos $\epsilon = (\pi^2-1)(\pi^2-k^2) = k^2 - (1+k^2)\pi^2 + \pi^4$. Así, $y = \pi^{-2}\sqrt{\epsilon}$ y

$$\frac{z^2}{y}\frac{dz}{d\pi} = \frac{\pi^{-2}}{\pi^{-2}\sqrt{\epsilon}}(-\pi^{-2}) = -\frac{1}{\sqrt{\epsilon}\,\pi^2}.$$

Ahora sólo necesitamos calcular el desarrollo en serie de $1/\sqrt{\epsilon}$. En primer lugar calculamos el de $\sqrt{\epsilon}$. Su primer coeficiente ha de cumplir $a_0^2 = k^2$, luego $a_0 = \pm k$. El siguiente ha de cumplir $a_0a_1 + a_1a_0 = 0$, luego ha de ser $a_1 = 0$, y podemos detenernos aquí: concluimos que $\sqrt{\epsilon} = \pm k + \eta\pi^2$, donde $v_\mathfrak{p}(\eta) \geq 0$.

El primer coeficiente de $1/\sqrt{\epsilon}$ ha de cumplir $b_0(\pm k) = 1$, luego ha de ser $b_0 = \pm 1/k$. El segundo ha de cumplir $b_0a_1 + b_1a_0 = 0$, luego $b_1 = 0$. Por consiguiente,

$$\frac{1}{\sqrt{\epsilon}} = \pm\frac{1}{k} + \delta\pi^2, \qquad \text{donde } v_\mathfrak{p}(\delta) \geq 0.$$

En total:

$$-\frac{1}{\sqrt{\epsilon}\,\pi^2} = \pm\frac{1}{k\pi^2} + \delta,$$

luego ω tiene un polo de orden 2 en $\mathfrak{p}$, pero su residuo es nulo. ∎

Para terminar con las integrales elípticas, veamos uno de los casos más sencillos posibles:

Ejemplo *La integral*

$$\int \sqrt{x^3-1}\,dx$$

no es elemental.

En efecto, empezaremos probando, más en general, que si $P(z)$ es un polinomio de grado > 1 con raíces simples, entonces $y = \sqrt{P(z)}$ no tiene una primitiva algebraica. En caso contrario, el teorema 7.1 implica que sería de la forma $a + by$, para ciertos a, $b \in \mathbb{C}(z)$. Por lo tanto,

$$y = a' + b'y + \frac{bP'}{2y},$$

luego

$$P = a'y + b'P + \frac{bP'}{2}.$$

Como todos los términos están en $\mathbb{C}(z)$ salvo y, es necesario que $a' = 0$. La ecuación se reduce a

$$\frac{b'}{b} = \frac{1}{b} - \frac{1}{2}\frac{P'}{P}.$$

Pongamos que $b = \alpha_0(z-\alpha_1)^{r_1}\cdots(z-\alpha_m)^{r_m}$, $P = \beta_0(z-\beta_1)\cdots(z-\beta_n)$. Entonces

$$\sum_i \frac{r_i}{z-\alpha_i} = \frac{1}{b} - \frac{1}{2}\sum_j \frac{1}{z-\beta_j}.$$

Si $r_i < 0$, entonces α_i ha de ser un β_j o, de lo contrario, no aparecería en la descomposición en fracciones simples del miembro derecho, pero, aun así, en el miembro izquierdo aparece con numerador r_i y en el miembro izquierdo con numerador $-1/2$, lo cual es imposible. Así pues, todos los r_i son positivos y $b \in \mathbb{C}[z]$.

La igualdad $b'P + bP'/2 - P = 0$ exige que b tenga grado 1, pues de lo contrario el coeficiente director sería $\alpha_0\beta_0 d + n\alpha_0\beta_0/2$, que no puede ser 0. Pero, en tal caso, la descomposición en fracciones simples se reduce a

$$\frac{1}{z-\alpha_1} = \frac{1/\alpha_0}{z-\alpha_1} - \frac{1}{2}\sum_j \frac{1}{z-\beta_j},$$

y esto fuerza a que $\operatorname{grad} P = 1$, en contra de lo supuesto.

También podemos probar en general que la forma diferencial $y\,dz$ tiene residuos nulos en los primos finitos. En efecto, si $\mathfrak{p}$ es un divisor primo finito, entonces $v_\mathfrak{p}(y) \geq 0$, $v_\mathfrak{p}(z) \geq 0$, luego también

$$v_\mathfrak{p}(\omega) = v_\mathfrak{p}\Big(y\frac{dz}{d\pi}\Big) \geq 0,$$

y el residuo de ω en $\mathfrak{p}$ es nulo. Tomemos ahora un primo infinito $\mathfrak{p}$ y consideremos ya, concretamente, $y = \sqrt{z^3-1}$. Como

$$2v_\mathfrak{p}(y) = v_\mathfrak{p}(z^3-1) = ev_\infty(z^3-1) = -3e,$$

ha de ser $e = 2$ y $v_\mathfrak{p}(y) = -3$. En particular, $v_\mathfrak{p}(z) = -2$. Por consiguiente, podemos tomar $\pi = z/y$. Así,

$$\frac{d\pi}{dz} = \frac{y - z\frac{3z^2}{2y}}{z^3 - 1} = \frac{-z^3 - 2}{2y(z^3 - 1)},$$

luego

$$y\frac{dz}{d\pi} = -\frac{2(z^3 - 1)^2}{z^3 + 2} \in \mathbb{C}(z).$$

Vemos que

$$v_\infty\Big(y\frac{dz}{d\pi}\Big) = -3,$$

luego

$$y\frac{dz}{d\pi} = \alpha_{-3}z^3 + \alpha_{-2}z^2 + \alpha_{-1}z + \epsilon,$$

donde $v_\infty(\epsilon) \geq 0$ (y también $v_\mathfrak{p}(\epsilon) \geq 0$). Ahora observamos que

$$\pi^2 z = \frac{z^3}{z^3 - 1} = 1 + \frac{1}{z^3 - 1} = 1 + \eta\pi^6,$$

donde $v_\mathfrak{p}(\eta) = 0$. Por consiguiente,

$$z = \pi^{-2} + \eta\pi^4, \quad z^2 = \pi^{-4} + 2\eta\pi^2 + \cdots, \quad z^3 = \pi^{-6} + 3\eta + \cdots$$

y así llegamos a que

$$y\frac{dz}{d\pi} = \alpha_{-3}\pi^{-6} + \alpha_{-2}\pi^{-4} + \alpha_{-1}\pi^{-2} + \alpha_0 + \alpha_1\pi + \cdots$$

tiene residuo nulo. ∎

Terminamos con un resultado debido a Chebyshev que proporciona una condición necesaria y suficiente para que una integral binomia sea elemental:

Ejemplo *La integral binomia*

$$\int x^k(b + ax^h)^q\,dx,$$

donde a, $b \in \mathbb{R}$, h, k, $q \in \mathbb{Q}$ son todos no nulos, es elemental si y sólo si al menos uno de los tres números

$$q, \quad \frac{k+1}{h}, \quad \frac{k+1}{h} + q$$

es entero.

Probaremos únicamente que la condición es necesaria, pues la suficiencia consiste en calcular la integral mediante los cambios de variable oportunos (los llamados cambios de Chebyshev), que pueden encontrarse en cualquier libro de cálculo de primitivas. En primer lugar observamos que el cambio de variable $t = x^h$ reduce el problema al caso $h = 1$. En efecto, la integral se convierte en

$$\frac{1}{h}\int t^{\frac{k+1}{h}-1}(a + bt)^q\,dt,$$

luego, llamando $p = (k+1)/h - 1$, basta probar que una integral de la forma

$$\int t^p (a+bt)^q \, dt,$$

donde $a, b \in \mathbb{R}$, p, $q \in \mathbb{Q}$ son no nulos y p, q, $p+q$ no son enteros, no tiene primitiva elemental.

Pongamos que $p = r/t$, $q = s/t$ y tomemos, en una clausura algebraica de $\mathbb{C}(z)$, elementos cualesquiera u, v tales que $u^t = z^r$, $v^t = (a+bt)^s$. Podemos llamarlos simplemente $u = z^p$, $v = (a+bz)^q$, teniendo en cuenta que no están unívocamente determinados. Lo que importa es que cualquier extensión holomorfa del integrando a un dominio complejo es de la forma $y = z^p(a+bz)^q \in F = \mathbb{C}(z, y)$, luego basta probar que y no tiene primitiva elemental en el sentido complejo.

Empezamos probando que si I es una primitiva de y, entonces no es algebraica. Si lo fuera, el teorema 7.1 implica que $I \in F$, luego sería de la forma

$$I = a_0 + a_1 y + \cdots + a_m y^m,$$

para ciertos $a_i \in \mathbb{C}(z)$, donde podemos tomar m menor que el grado del polinomio mínimo de y sobre $\mathbb{C}(z)$. Ahora observamos que

$$y' = pz^{p-1}(a+bz)^q + qbz^p(a+bz)^{q-1} = y\Big(\frac{p}{z} + \frac{qb}{a+bz}\Big)$$

luego $y'/y \in \mathbb{C}(z)$, y también

$$(a_i y^i)' = a_i' y^i + i a_i y^{i-1} y' = \Big(a_i' + i a_i \frac{y'}{y}\Big) y^i = b_i y^i,$$

donde $b_i \in \mathbb{C}(z)$. Por consiguiente, al derivar la expresión para I obtenemos

$$y = b_0 + b_1 y + \cdots + b_m y^m.$$

Como m es menor que el grado del polinomio mínimo de y, el polinomio que resulta de igualar a 0 la ecuación anterior ha de ser idénticamente nulo. En particular, $b_1 = 1$, lo cual, explícitamente, es la igualdad

$$a_1' + a_1\Big(\frac{p}{z} + \frac{qb}{a+bz}\Big) = 1.$$

Equivalentemente:

$$\frac{a_1'}{a_1} = \frac{1}{a_1} - \frac{p}{z} - \frac{q}{z + a/b}.$$

Pongamos que $a_1 = \alpha_0(z-\alpha_1)^{r_1} \cdots (z-\alpha_m)^{r_m}$. Entonces

$$\sum_i \frac{r_i}{z-\alpha_i} = \frac{1}{a_1} - \frac{p}{z} - \frac{q}{z+a/b}.$$

Vemos que, si $r_i < 0$, entonces α_i ha de ser 0 o bien $-a/b$, pues en caso contrario no aparecería en la descomposición en fracciones simples del miembro derecho, pero, aun

así, tenemos una contradicción, pues si, por ejemplo, $\alpha_i = 0$ con $r_i < 0$, el numerador del término correspondiente en la descomposición del miembro derecho es $-p \notin \mathbb{Z}$, y en la izquierda es $r_i \in \mathbb{Z}$. Lo mismo sucede si $\alpha_i = -a/b$. Así pues, a_1 es un polinomio. Si llamamos $d = \operatorname{grad} a_1$ y suponemos que $d > 1$, entonces, en la identidad

$$a_1' z(z + a/b) + pa_1(z + a/b) + qa_1 z - z(z + a/b) = 0,$$

el coeficiente director es

$$d\alpha_0 + p\alpha_0 + q\alpha_0 = 0,$$

de donde se sigue que $p + q = -d \in \mathbb{Z}$, contradicción, luego ha de ser $d = 1$. Así pues, tenemos la igualdad de descomposiciones en fracciones simples

$$\frac{1 - \alpha_0}{z - \alpha_1} = -\frac{p}{z} - \frac{q}{z + a/b},$$

que claramente es imposible, pues los dos denominadores del miembro derecho son distintos entre sí.

Ahora nos falta probar que la forma diferencial $\omega = y\,dz$ tiene residuos nulos. Tomemos un divisor primo $\mathfrak{p} \in \Sigma_F$ y sea $p_0 \in \mathbb{C}^\infty$ el primo al que divide. Si p_0 es finito y distinto de 0 y de $-a/b$, entonces $v_\mathfrak{p}(z) = v_\mathfrak{p}(a + bz) = 0$. La relación

$$y^t = z^r(a + bz)^s$$

nos da que $v_\mathfrak{p}(y) = 0$, de donde se sigue que

$$v_\mathfrak{p}(\omega) = v_\mathfrak{p}\Big(y\frac{dz}{d\pi}\Big) \geq 0,$$

luego el residuo es nulo.

Supongamos ahora que $p_0 = 0$, de modo que $v_\mathfrak{p}(z) = e > 0$ y $v_\mathfrak{p}(a + bz) = 0$. Necesitamos calcular el índice de ramificación e. Razonaremos como en la prueba del teorema 6.1. Sea $K = \mathbb{C}(z)_{p_0}$ la compleción de $\mathbb{C}(z)$ respecto de p_0. Sabemos que $F_\mathfrak{p} = K(y)$ y que $e = |F_\mathfrak{p} : K|$.

Se cumple que $\epsilon = (a + bz)^q \in K$. En efecto, si[18]

$$(a + bz)^s = a_0 + a_1 z + a_2 z^2 + \cdots$$

donde $a_0 = a^s \neq 0$, podemos definir una serie $S = b_0 + b_1 z + b_2 z^2 + \cdots$ tal que $S^t = (a + bz)^s$. Ha de ser $b_0^t = a_0$, con lo que tenemos t elecciones posibles para $b_0 \neq 0$ (que nos darán las t raíces t-ésimas de $(a + bz)^s$). Supuesto que hayamos definido $b_0, \ldots, b_{n-1}$, la condición que define a b_n es

$$\sum_{i_1 + \cdots + i_t = n} b_{i_1} \cdots b_{i_t} = a_n,$$

y b_n sólo aparece en t monomios de la forma $b_0^{t-1} b_n$, luego podemos despejar b_n dividiendo entre $t b_0^{t-1} \neq 0$. Una de las t series construidas de esta forma[19] ha de ser $(a + bz)^q \in K$.

[18] Notemos que puede ser $s < 0$, y entonces la serie es infinita.

[19] Alternativamente, podríamos haber aplicado el lema de Hensel.

Por consiguiente, $F_\mathfrak{p} = K(z^p)$. Pongamos que $p = r'/t'$, con r' y t' primos entre sí. Así, si $w = z^p$, se cumple que $w^{t'} = z^{r'}$. Tomemos enteros u y v tales que $ur' + vt' = 1$. Así, $\pi = w^u z^v \in F_\mathfrak{p}$ cumple que $\pi^{t'} = w^{t'u} z^{t'v} = z^{r'u+t'v} = z$. Como $e = v_\mathfrak{p}(z) = t' v_\mathfrak{p}(\pi)$, vemos que

$$t' \le e = |F_\mathfrak{p} : K| \le t',$$

donde la última desigualdad se debe a que z^p es raíz del polinomio $T^{t'} - z^{r'}$. Concluimos que $e = t'$, con lo que $v_\mathfrak{p}(\pi) = 1$. La relación $w^{t'} = z^{r'} = \pi^{r't'}$ implica que $w = \eta\pi^{r'}$, para cierta constante $\eta \in \mathbb{C}$ (una raíz de la unidad).

Ya tenemos todo lo necesario para calcular el residuo de ω en $\mathfrak{p}$:

$$y\,\frac{dz}{d\pi} = \eta\pi^{r'}\epsilon\, t'\pi^{t'-1} = \eta t'\pi^{r'+t'-1}(b_0 + b_1\pi^{t'} + b_2\pi^{2t'} + \cdots)$$

Para que esta serie pudiera tener residuo no nulo, tendría que haber un número natural k tal que $r' + t' - 1 + kt' = -1$, pero entonces $(1+k)t' = -r'$, luego t' divide a r' y p sería entero. Concluimos que $\operatorname{Res}_\mathfrak{p} \omega = 0$.

Si $p_0 = -a/b$, llamamos $t = a + bz \in \mathbb{C}(z)$, con lo que $\mathbb{C}(z) = \mathbb{C}(t)$ y ω puede expresarse en la forma

$$\omega = b^{-1}(-ab^{-1} + b^{-1}t)^p\, t^q\, dt.$$

Esta expresión es (salvo la constante b^{-1}) análoga a la original (para otros valores de a y b) y, tras el cambio de variable, el divisor primo de $\mathbb{C}(t)$ divisible entre $\mathfrak{p}$ pasa a ser p_0, luego $\operatorname{Res}_\mathfrak{p} \omega = 0$ por el caso ya probado.

Si $p_0 = \infty$ podemos hacer lo mismo. Ahora llamamos $t = 1/z$, con lo que

$$\omega = z^p(a + bz)^q\, dz = -t^{-p-q-2}(at + b)^q\, dt,$$

y concluimos que $\operatorname{Res}_\mathfrak{p} \omega = 0$ aplicando el caso ya probado. ∎

Referencias

Ritt, J.F., *Integration in Finite Terms. Liouville's Theory of Elementary Methods*, Columbia University Press, 1948.

Rosenlicht, M. *Integration in Finite Terms,* Amer. Math. Monthly, Vol. 79, No 9, (1972) pp. 963–972.