Universidad de Valladolid
Facultad de Ciencias

Trabajo Fin de Grado

Grado en Matemáticas

Integración por cuadraturas de ecuaciones diferenciales ordinarias

Autor: María Martín Manso

Tutor: José María Cano Torres

Agradecimientos

A mi familia y amigos, muy especialmente a mis padres, a mi hermano y a Juan, por sus consejos, su apoyo incondicional y confiar en mi cuando ni yo misma lo hacía.

A la memoria de los que ya no están aquí presentes, pero sé que me acompañan siempre.

A mi tutor José, por su ayuda y dedicación en este trabajo.

II

Índice general

Introducción

Una función elemental es una función formada por la composición, la suma o el producto de funciones algebraicas, exponenciales y logarítmicas. Además, utilizando la operación derivación en una de ellas, se obtienen nuevas funciones elementales.
Se puede construir de fácilmente un algoritmo para obtener la derivada de una función elemental en términos de funciones elementales. Sin embargo, el proceso inverso no se estudia en el Grado de Matemáticas, salvo casos de funciones elementales muy particulares.
En el año 1968, Risch desarrolló un algoritmo que permite decidir si una función elemental tiene una integral elemental, y calcularla en caso afirmativo. Este algoritmo es extraordinariamente complejo. De hecho, el libro de Bronstein [2] se dedica al estudio únicamente del caso de funciones elementales transcedentes, dejando para un segundo volumen, que nunca vió la luz, el caso algebraico. El objetivo de este trabajo es estudiar el teorema de Liouville, el cual forma parte de la teoría para desarrollar el algoritmo de Risch, en su versión negativa. Este nos dará una condición para saber si una función determinada tiene primitivas elementales o no.
El ejemplo más conocido por todos de función con integral no elemental, es la función de Gauss $f(x) = e^{-x^2}$. Esta función, empleada en estadística, es integrable pero, como veremos al final de este trabajo , no existe una combinación de funciones elementales que exprese su integral. De hecho, en la práctica, el valor de estas integrales se calcula con ayuda de una tabla, o con fórmulas de cuadratura numérica en algún programa de ordenador.

Dado que el cuerpo diferencial base del que partimos es el de las funciones racionales, el primer capítulo del trabajo lo dedicamos a la interpretación de éstas como funciones sobre la esfera de Riemann.

En el segundo capítulo desarrollaremos la teoría de álgebra diferencial. Entre los conceptos y resultados más importantes se encuentran aquellos que involucran anillos y cuerpos diferenciales, extensiones diferenciales y la aplicación orden. Toda esta teoría, se empleará para desarrollar el último capítulo y parte central de este trabajo, el teorema de Liouville. Aunque, a priori, parezca que vamos a dar un argumento analítico, lo cierto es que demostraremos este último teorema recurriendo a razonamientos algebraicos en el contexto de los cuerpos diferenciales. Finalmente, este teorema nos ayudará a probar que integrales como, por ejemplo,

$$\int e^{-x^2} \quad o \quad \int \frac{sen(x)}{x},$$

no pueden expresarse en términos de funciones elementales.

Capítulo 1

Funciones racionales

1.1. La esfera de Riemann

Recordamos la construcción de la esfera de Riemann y algunas de sus propiedades; para ello consideramos la esfera en $\mathbb{R}^2$,

$$S^2 = \{(x_1, x_2, x_3) \in \mathbb{R}^3 / x_1^2 + x_2^2 + x_3^2 = 1\},$$

e identificamos el plano complejo $\mathbb{C}$ con el plano $T = \{x_3 = 0\}$ mediante la correspondencia de $z = x + iy$ siendo $x, y \in \mathbb{R}$ con $(x, y, 0)$ para todo $z \in \mathbb{C}$. Sea $N = (0, 0, 1)$ el polo norte de la esfera, la proyección estereográfica desde N proporciona una aplicación biyectiva

$$\pi : S^2 \backslash N \longrightarrow \mathbb{C} \tag{1.1}$$

siendo π la composición siguiente

$$\begin{array}{rcl} \pi : S^2 \backslash N & \longrightarrow & T \cong \mathbb{C} \\ Q & \to & P \cong z \end{array} \tag{1.2}$$

donde P es un punto del plano T definido anteriormente, z el punto del plano complejo $\mathbb{C}$ homeomorfo a P y $Q \in S^2 \backslash N$, y se tiene que los puntos P,Q y N son colineales.

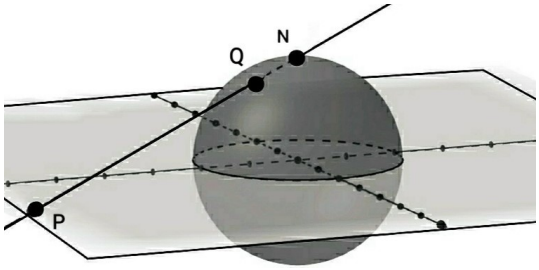

Figura 1.1: Esfera de Riemann

Proposición 1.1.1 *La aplicación π construida anteriormente es un homeomorfismo entre $S^2\backslash N$ y $\mathbb{C}$.*

Demostración:

Sea $P = (x, y, 0)$ donde $z = x + iy \in \mathbb{C}$, y sea $Q = (x_1, x_2, x_3) \in S^2\backslash N$. Como P,Q y N son colineales, se tiene que

$$\frac{x}{x_1} = \frac{y}{x_2} = \frac{1}{1 - x_3}.$$

Por lo tanto, $(x_1, x_2, x_3) \to (x, y, 0) \to x + iy$, siendo

$$x = \frac{x_1}{1 - x_3} \quad e \quad y = \frac{x_2}{1 - x_3}.$$

Calculamos ahora la aplicación inversa

$$\begin{array}{rcl} \pi^{-1} : \mathbb{C} \cong T & \longrightarrow & S^2\backslash \mathrm{N} \\ Z \cong P & \to & Q \end{array} \tag{1.3}$$

utilizando que como $Q \in S^2 \setminus N$, se cumple que $x_1^2 + x_2^2 + x_3^2 = 1$. Luego,

$$x^2 + y^2 + 1 = \frac{2 - 2x_3}{(1 - x_3)^2} = \left(\frac{x_1}{1 - x_3}\right)^2 + \left(\frac{x_2}{1 - x_3}\right)^2 + 1 = \frac{2}{1 - x_3}.$$

Por lo tanto, la aplicación π^{-1} viene dada por

$$x_1 = \frac{2x}{x^2 + y^2 + 1}, \quad x_2 = \frac{2y}{x^2 + y^2 + 1}, \quad x_3 = \frac{x^2 + y^2 - 1}{x^2 + y^2 + 1}.$$

Estas expresiones muestran que tanto π como π^{-1} son continuas, por ser cociente de funciones polinómicas cuyo denominador no se anula. Veamos que π es también biyectiva para concluir que es un homeomorfismo, comprobando que $\pi \circ \pi^{-1} = Id$ y $\pi^{-1} \circ \pi = Id$.

$$(\pi \circ \pi^{-1})(x+iy) = \pi\left(\frac{2x}{x^2+y^2+1}, \frac{2y}{x^2+y^2+1}, \frac{x^2+y^2-1}{x^2+y^2+1}\right) =$$

$$= \left(\frac{\frac{2x}{x^2+y^2+1}}{1-\frac{x^2+y^2-1}{x^2+y^2+1}}, \frac{\frac{2y}{x^2+y^2+1}}{1-\frac{x^2+y^2-1}{x^2+y^2+1}}, 0\right) =$$

$$= \left(\frac{\frac{2x}{x^2+y^2+1}}{\frac{x^2+y^2+1-(x^2+y^2-1)}{x^2+y^2+1}}, \frac{\frac{2y}{x^2+y^2+1}}{\frac{x^2+y^2+1-(x^2+y^2-1)}{x^2+y^2+1}}, 0\right) =$$

$$= (x, y, 0)\,.$$

$$(\pi^{-1} \circ \pi)(x_1, x_2, x_3) = \pi^{-1}\left(\frac{x_1}{1-x_3} + i\frac{x_2}{1-x_3}\right) =$$

$$= \left(\frac{\frac{2x_1}{1-x_3}}{\frac{x_1^2+x_2^2}{(1-x_3)^2}+1}, \frac{\frac{2x_2}{1-x_3}}{\frac{x_1^2+x_2^2}{(1-x_3)^2}+1}, \frac{\frac{x_1^2+x_2^2}{(1-x_3)^2}-1}{\frac{x_1^2+x_2^2}{(1-x_3)^2}+1}\right) =$$

$$= \left(\frac{\frac{2x_1}{1-x_3}}{\frac{x_1^2+x_2^2+(1-x_3)^2}{(1-x_3)^2}}, \frac{\frac{2x_2}{1-x_3}}{\frac{x_1^2+x_2^2+(1-x_3)^2}{(1-x_3)^2}}, \frac{\frac{x_1^2+x_2^2}{(1-x_3)^2}-1}{\frac{x_1^2+x_2^2}{(1-x_3)^2}+1}\right) =$$

$$= \left(\frac{2x_1(1-x_3)}{x_1^2+x_2^2+(1-x_3)^2}, \frac{2x_2(1-x_3)}{x_1^2+x_2^2+(1-x_3)^2}, \frac{x_1^2+x_2^2-(1-x_3)^2}{x_1^2+x_2^2+(1-x_3)^2}\right) =$$

$$= (x_1, x_2, x_3).$$

Por lo tanto, queda probado que la aplicación π definida anteriormente es un homeomorfismo. ■

En S^2 se considera la topología de subespacio de $\mathbb{R}^3$ siendo los abiertos que la definen de la forma $U = \{P \in \mathbb{R}^3 / \quad \|P - P_0\| < r\}$. Por lo que si ahora ahora denotamos $\hat{\mathbb{C}} = \mathbb{C} \cup \infty$, donde ∞ es un símbolo que representa un elemento distinto a todos los elementos de $\mathbb{C}$; extendemos

$$\pi : S^2 \backslash N \quad \longrightarrow \quad \mathbb{C} \tag{1.4}$$

a la aplicación

$$\pi : S^2 \quad \longrightarrow \quad \hat{\mathbb{C}} \tag{1.5}$$

definiendo $\pi(N) = \infty$ y utilizando esta última biyección podemos definir una topología en $\hat{\mathbb{C}}$, la topología inducida por π, definiendo sus conjuntos abiertos como la imagen por la aplicación π de los conjuntos abiertos de S^2.

Definición 1.1.1 *Un espacio topológico X es compacto si todo recubrimiento abierto de X, admite un subrecubrimiento finito.*

Teorema 1.1.1 *(Heine Borel) Un subespacio X de $\mathbb{R}^n$ es compacto si y solo si, es cerrado y acotado.*

Como consecuencia del teorema de Heine Borel, la esfera de Riemann es compacta. Luego $\hat{\mathbb{C}}$ es compacto por ser la imagen de un conjunto compacto por una aplicación continua, y por la caracterización secuencial de espacios métricos compactos, toda sucesión infinita en $\hat{\mathbb{C}}$ admite una subsucesión convergente.

Compactificación:

La topología del subespacio de $\mathbb{C}$ (inducida por su inclusión en $\hat{\mathbb{C}}$) coincide con la topología habitual. Esto muestra que $\hat{\mathbb{C}}$ es la compactificación en un punto de $\mathbb{C}$, es decir, podemos introducir cualquier espacio topológico X en un espacio compacto $X \cup \{\infty\}$ añadiendo un único punto ∞ y definiendo los conjuntos abiertos de $X \cup \{\infty\}$ como los conjuntos abiertos de X junto con aquellos subconjuntos que contienen a ∞ y tienen un complementario

compacto y cerrado en X.

Proposición 1.1.2 *Definimos los abiertos del plano complejo extendido* $\hat{\mathbb{C}}$ *como sigue:*

- *Si no contienen a* ∞ *son los abiertos de* $\mathbb{C}$.
- *Si contienen a* ∞ *se definen como la unión de* $\{\infty\}$ *con un abierto de* $\mathbb{C}$ *que contiene un conjunto de la forma* $\{z \in \mathbb{C}/ \quad \|z\| > r\}$ *para un* $r > 0$ *adecuado; es decir, son los conjuntos de la forma* $(\mathbb{C}\backslash K) \cup \infty$, *siendo* K *un subconjunto compacto de* $\mathbb{C}$.

Demostración:

Veamos la primera implicación. Para ello probaremos que todo abierto de $\hat{\mathbb{C}}$ tiene la forma dada en el enunciado.
Sea U un abierto de $\hat{\mathbb{C}}$, entonces por la definición de la topología de $\hat{\mathbb{C}}$, $\pi^{-1}(U)$ es un abierto de S^2.

- Si $\infty \notin U$ entonces $N \notin \pi^{-1}(U)$, luego $\pi^{-1}(U)$ es un abierto de $S^2\backslash N$. Así que, como $\pi|_{S^2\backslash N}$ es un homeomorfismo, se tiene que
$$\pi|_{S^2\backslash N}\left(\pi^{-1}(U)\right) = U$$
es un abierto de $\mathbb{C}$ por ser $\pi^{-1}(U)$ abierto de $S^2 \setminus N$.
- Si $\infty \in U$, entonces $\pi^{-1}(U)$ es abierto de S^2, luego existe una bola $B(N,\epsilon)$ tal que $B(N,\epsilon) \cap S^2 \subseteq \pi^{-1}(U)$. Además,
$$B(N,\epsilon) \cap S^2 = S^2\backslash(S^2 \setminus B(N,\epsilon) \cap S^2),$$
siendo $(S^2 \setminus B(N,\epsilon) \cap S^2)$ compacto por ser un cerrado y acotado de $\mathbb{R}^3$. Luego por ser π una aplicación biyectiva se tiene que
$$\begin{aligned}\pi(B(N,\epsilon) \cap S^2) &= \pi(S^2 \setminus (S^2 \setminus (B(N,\epsilon) \cap S^2))) = \\ &= \pi(S^2) \setminus \pi(S^2 \setminus (B(N,\epsilon) \cap S^2) = \\ &= \hat{\mathbb{C}} \setminus K = (\mathbb{C} \setminus K) \cup \{\infty\},\end{aligned}$$
donde K es compacto por ser imagen de un conjunto compacto por una aplicación continua. Luego $(\mathbb{C} \setminus K) \cup \{\infty\} \subseteq U$.
Además, es claro que $U \subseteq (\mathbb{C} \setminus K) \cup \{\infty\}$.

Veamos ahora la otra implicación, es decir, vamos a probar que los conjuntos que son de la forma dada en el enunciado, son abiertos del plano complejo extendido $\hat{\mathbb{C}}$.
Basta ver que para todo $p \in U$ existe un abierto U_p tal que $p \in U_p \subseteq U$

- Si $p \neq \infty$, entonces $p \in U \setminus \{\infty\}$ y $U \setminus \{\infty\}$ es un abierto de $\mathbb{C}$, luego $U \setminus \{\infty\}$ es un abierto de $\hat{\mathbb{C}}$, por ser $\mathbb{C}$ un abierto de $\hat{\mathbb{C}}$. Por tanto, existe un abierto U_p tal que $p \in U_p \subseteq U$.

- Si $p = \infty$ entonces existe un $R > 0$ tal que $\{z \in \mathbb{C} / \quad |z| > R\} \subseteq U$. Luego $\pi(B(N, \epsilon) \cap S^2) = \{z \in \mathbb{C} / \quad |z| > R\} \subseteq U$, pues $\infty \in U$. Luego $\{z \in \mathbb{C} / \quad |z| > R\} \cup \{\infty\}$ es un abierto de $\mathbb{C}$.

■

1.2. Comportamiento de las funciones en el infinito

Sea D un subconjunto de $\hat{\mathbb{C}}$ que no contiene a ∞, entonces $D \subset \mathbb{C}$ y podemos referirnos a las funciones en D como analíticas, meromorfas, con polos...Es decir, con las mismas propiedades que si sólo estuvieran definidas en $\hat{\mathbb{C}}$. Nuestro objetivo es definir conceptos similares en ∞, de modo que todos los puntos de $\hat{\mathbb{C}}$ tengan las mismas propiedades. Para ello se utiliza la transformación

$$J : \hat{\mathbb{C}} \longrightarrow \hat{\mathbb{C}} \tag{1.6}$$

Definida de la siguiente forma:

$$J(z) = \begin{cases} \frac{1}{z} & si \quad z \in (0, \infty) \\ 0 & si \quad z = \infty \\ \infty & si \quad z = 0 \end{cases}$$

Dicha J es una biyección y J^2 es la identidad, ya que la inversa de J es ella misma.

Ahora se considera P el punto $z = x + iy \in \mathbb{C}\backslash\{0\}$ con $x, y \in R$ y sea P^* el punto imagen de P por J,

$$J(z) = z^{-1} = \frac{x - iy}{z\bar{z}}.$$

Luego el punto $Q = \pi^{-1}(P)$ de S^2 tiene coordenadas

$$x_1 = \frac{2x}{z\bar{z}+1}, \quad x_2 = \frac{2y}{z\bar{z}+1}, \quad x_3 = \frac{z\bar{z}+1}{z\bar{z}+1}$$

en $\mathbb{R}^3$ y las coordenadas de $Q^* = \pi^{-1}(P^*)$ son

$$\begin{aligned} x_1^* &= \frac{2x(z\bar{z})^{-1}}{(z\bar{z})^{-1}+1} = \frac{2x}{1+z\bar{z}} = x_1, \\ x_2^* &= \frac{-2y(z\bar{z})^{-1}}{(z\bar{z})^{-1}+1} = \frac{-2y}{1+z\bar{z}} = -x_2, \\ x_3^* &= \frac{(z\bar{z})^{-1}-1}{(z\bar{z})^{-1}+1} = \frac{1-z\bar{z}}{1+z\bar{z}} = -x_3 \end{aligned}$$

Entonces J induce la transformación de S^2

$$\pi^{-1} J \pi : Q \longrightarrow Q \tag{1.7}$$

y esta es la rotación de S^2 de ángulo π sobre el eje x_1.
A partir de ahora haremos un abuso de notación y nos referiremos a la rotación

$$J : S^2 \longrightarrow S^2 \tag{1.8}$$

en lugar de $\pi^{-1} J \pi$. Es decir, identificamos S^2 con $\hat{\mathbb{C}}$ por medio de π, y consideramos J como una transformación de cada uno de estos dos espacios.

Supongamos que una función $f(z)$ está definida en $D\backslash\{\infty\}$, donde D es un entorno de ∞ en $\hat{\mathbb{C}}$, es decir $f(z)$ está definida para valores grandes de z, en valor absoluto. Si existe el límite $\lim_{z\to\infty}(f(z))$ podemos extender el dominio de f para incluir a ∞ definiendo $f(\infty)$ como el valor de dicho límite. Las propiedades que tenga f en ∞ serán las mismas que las de $f \circ J$ en 0.

Definición 1.2.1 *Se dice que z_0 es una raíz de la ecuación $f(z) = c$ con multiplicidad m_0 si la función $f(z) - c$ tiene un cero en $z = z_0$ con multiplicidad m_0, es decir, si y sólo sí $f(z_0) - c = 0$, $f'(z_0) = 0$,..., $f^{(m_0-1)}(z_0) = 0$, $f^{(m_0)}(z_0) \neq 0$.*

Observación:
Si z_0 es una raíz múltiple ($m \geq 2$) de $f(z) = c$, entonces $f'(z_0) = 0$, es decir, z_0 es un cero de $f'(z)$.

Proposición 1.2.1 *Hay un número finito de valores c para los cuales la ecuación $f(z) = c$ tiene al menos una raíz múltiple.*

Demostración:
Si la ecuación $f(z) = c$ tiene a z_0 como raíz múltiple, entonces $f'(z_0) = 0$, es decir, $z_0 \in Z(f) = \{z \in \hat{\mathbb{C}} / \quad f'(z) = 0\} = Z$, siendo $Z = \{w_1, ...w_k\}$ un conjunto finito. Luego $c = f(z_0) \in f(Z) = \{f(w_1), ..., f(w_k)\}$. Así que si $c \notin \{f(w_1), ..., f(w_k)\}$, entonces la ecuación $f(z) = c$ sólo puede tener raices simples. ■

Definición 1.2.2 *Sea D un conjunto abierto de $\hat{\mathbb{C}}$ y $f : D \to \mathbb{C}$. Se dice que f es analítica (resp. meromorfa) en D si:*

- *f es analítica (resp. meromorfa) en D, si $\infty \notin D$.*
- *$f \circ J(z) = f(1/z)$ es analítica (resp. meromorfa) en ∞, si $\infty \in D$*

Teorema 1.2.1 *Sea f una función analítica en una región R de $\hat{\mathbb{C}}$. Si f tiene ceros en un número infinito de puntos z_n en R con $z^* = \lim_{n\to\infty} z_n$ en R, entonces f es idénticamente cero en R.*

Demostración:
Si $z^* \neq \infty$, entonces $z_n \neq \infty$ para todo n suficientemente grande, por lo que omitiendo un número finito de términos podemos suponer que $z_n \in \mathbb{C}$ para todo n. Ahora $R' = R \setminus \infty$ es una región en $\mathbb{C}$, y f es analítica en R' con ceros en una secuencia infinita de puntos $z_n \in R'$ con un límite $z^* \in R'$, luego f es idénticamente cero en R'. Si $\infty \notin R$ entonces $R = R'$ y el resultado

queda demostrado. Si $\infty \in R$, entonces como f es analítico en ∞ y se anula en un entorno de ∞, tenemos que $f(\infty) = 0$, por continuidad.

Supongamos ahora que $z^* = \infty$. Omitiendo un número finito de términos, podemos suponer que $z_n \neq 0$ para todo n. Como f es analítica en la región $\hat{R} = R \setminus \{0\}$, $f \circ J$ es analítica en la región $R^* = \{z^{-1}/z \in \hat{R}\}$. Ahora $f \circ J$ tiene ceros en los puntos z_n^{-1} de R^*, y estos tienen un límite $J(z^*) = 0$ en R^*, por lo que $f \circ J$ es idénticamente cero en R^* y por tanto f es idénticamente nula en $\hat{R}$. Si $0 \notin R$ entonces $R = \hat{R}$ y el resultado queda demostrado. Si $0 \in R$ entonces $f(0) = 0$ por continuidad, por lo que f es idénticamente nula en R. ■

Hemos probado que ∞ se puede incluir en el dominio de definición de una función f, pero también se puede introducir ∞ en la imagen de f:
Si f es una función meromorfa en un punto $z_0 \in \hat{\mathbb{C}}$, con un polo en z_0, es decir f presenta una singularidad en z_0 y $\lim_{z \to z_0} f(z) = \infty$ o lo que es equivalente $J \circ f(z_0) = 0$, entonces se puede escribir $f(z_0) = \infty$.

Definición 1.2.3 *Dada f una función analítica en un punto $a \in \mathbb{C}$, con $f(a) = c \in \mathbb{C}$; si f es no constante entonces $f^{(k)}(a) \neq 0$ para algún $k \geq 1$, y al menor de dichos números enteros k se le llama multiplicidad de la solución de $f(z) = c$ en $z = a$.*
Si f es una función meromorfa en $z_0 \in \mathbb{C}$, con un polo de orden k en z_0, entonces $f(z_0) = \infty$ con multiplicidad k.
Si $z_0 = \infty$ se dice que $f(\infty) = c$ con multiplicidad k si $(f \circ J)(0) = c$ con multiplicidad k.

Proposición 1.2.2 *Una función meroforma $f : \hat{\mathbb{C}} \to \hat{\mathbb{C}}$ no constante, tiene como imagen un cierto valor $c \in \hat{\mathbb{C}}$ un número finito de veces, contando multiplicidades, es decir, la suma de las multiplicidades de las soluciones de $f(z) = c$ es finita.*

Demostración:

Demostramemos en primer lugar que si $z \in \mathbb{C}$ y $f(z) = c$, entonces existe un entorno U_z de z tal que f no toma el valor c en $U_z \backslash \{z\}$. En efecto, si

$c = \infty$, los polos de f son ceros de $J \circ f$, y como $J \circ f$ es una función meromorfa no constante, por el teorema anterior dichos ceron son aislados; si $c \neq \infty$, utilizamos el hecho de que los ceros de $f - c$ están aislados. Por ser $\hat{\mathbb{C}}$ es compacto, está recubierto por un número finito de entornos $U_{z_1}, ..., U_{z_k}$, por lo que $f^{-1}(c) = \{z_1, ..., z_k\}$ es un conjunto finito. Como f es una función meromorfa, cada solución de $f(z) = c$ tiene multiplicidad finita, luego f toma el valor c sólo un número finito de veces. ■

Definición 1.2.4 *Sea $z = z_0$ una singularidad aislada de una función $f(z)$ analítica en un anillo $A(z_0; r, R) = \{z \in \mathbb{C}; r < |z - z_0| < R\}$. Un desarrollo en serie de Laurent para f(z) es de la forma:*

$$f(z) = \sum_{k=1}^{\infty} a_{-k}(z - z_0)^{-k} + \sum_{k=0}^{\infty} a_k(z - z_0)^k.$$

El primer sumatorio se llama parte principal del desarrollo de la función en el punto z_0, y el segundo parte analítica.

Teorema 1.2.2 *Sean f y g funciones meromorfas sobre $\hat{\mathbb{C}}$ con polos en los mismos puntos de $\hat{\mathbb{C}}$, y con las mismas partes principales en estos puntos. Entonces $f(z) = g(z) + c$ para alguna constante c.*

Demostración:

La función $h = f - g$ es meromorfa, por ser diferencia de funciones meromorfas, y por tanto continua en $\hat{\mathbb{C}}$. Luego como $\hat{\mathbb{C}}$ es compacto, su imagen por h es compacta. Como las partes principales de f y g se cancelan, por ser iguales, h no tiene polos, por lo que $h(\hat{\mathbb{C}})$ es un subconjunto de $\mathbb{C}$, y al ser compacto está acotado. El teorema de Liouville muestra que por ser h una función analítica y acotada, debe ser constante en $\mathbb{C}$, y por tanto, por continuidad, $h = c$ en $\hat{\mathbb{C}}$ para alguna constante c, es decir, $f = g + c$. ■

Proposición 1.2.3 *Una función analítica en todo $\hat{\mathbb{C}}$ es constante.*

Demostración:

Es consecuencia del teorema anterior ya que dicha función tiene las mismas partes principales que una función constante. ■

Teorema 1.2.3 *Sean f y g funciones meromorfas en $\hat{\mathbb{C}}$ con ceros y polos de los mismos órdenes y en los mismos puntos de $\mathbb{C}$. Entonces $f(z) = cg(z)$ para alguna constante $c \neq 0$.*

Demostración:

Podemos suponer que f y g no son funciones idénticamente nulas. Entonces f/g y g/f son meromorfos en $\hat{\mathbb{C}}$, por ser cociente de funciones meromorfas con función denominador no nula, y ninguna de ellas tiene polos en $\mathbb{C}$, ya que como tienen polos en los mismos puntos al hacer el cociente estos desaparecen, por lo que ambas son analíticas en $\mathbb{C}$. Al menos una de ellas es finita en ∞, luego es analítica en $\hat{\mathbb{C}}$. Como en el teorema anterior, el teorema de Liouville implica que h es constante, por lo que $f = cg$ para alguna constante $c \neq 0$ ni f ni g son idénticamente nulas. ■

1.3. Funciones racionales

Definición 1.3.1 *Una función racional es una función de la forma $f(z) = p(z)/q(z)$, siendo $p(z)$ y $q(z)$ polinomios con coeficientes en $\mathbb{C}$ y $q(z)$ no idénticamente nula.*

Se puede extender la definición de función racional $f(z)$ al plano ampliado $\hat{\mathbb{C}}$, definiendo $f(z) = \lim_{z' \to z} f(z')$, para $z = \infty$ o $q(z) = 0$.

Definición 1.3.2 *Sean f, g dos polinomios con coeficientes complejos y ambos no nulos. Se dice que son coprimos si ningún polinomio de grado ≥ 1 divide simultáneamente a f y a g.*

El teorema fundamental del álgebra, establece que todo polinomio de grado mayor que cero posee una raiz. Luego se pueden descomponer p y q como producto de factores irreducibles de grado 1. Al realizar el cociente $f(z) = p(z)/q(z)$, se pueden cancelar los factores comunes del numerador y denominador, y dar como resultado una función cociente de polinomios que son coprimos. Esta función, de nuevo por el teorema fundamental del álgebra, puede expresarse como:

$$f(z) = c(z - \alpha_1)^{m_1} ... (z - \alpha_r)^{m_r} (z - \beta_1)^{-n_1} ... (z - \beta_s)^{-n_s},$$

siendo $c \in \mathbb{C}$, α_1,...,α_r raices del polinomio p con multiplicidades m_1,..m_r y β_1,...,β_s raices del polinomio q con multiplicidades n_1,...,n_s. Dichos α_1,...,α_r son ceros de la función f de multiplicidades m_1,..m_r y β_1,...,β_s son los polos de f de órdenes n_1,...,n_s.

Teorema 1.3.1 *Una función $f : \hat{\mathbb{C}} \to \hat{\mathbb{C}}$ es racional si y solo si es una función meromorfa en $\hat{\mathbb{C}}$.*

Demostración:

Si se descompone la función f como se acaba de ver (cociente de dos polinomios coprimos descompuestos en factores irreducibles), entonces f es analítica en cada $z \neq \infty$ y $z \neq \beta_j$, $j = 1, ...s$, luego f es una función analítica en $\mathbb{C} \setminus \beta_1, ..., \beta_s$. En cada β_j, $j = 1, ...s$, f tiene un polo de orden n_j, mientras que en ∞, f es analítico si $gr(p) \leq gr(q)$ y f tiene un polo de orden $gr(p) - gr(q)$, si $gr(p) > gr(q)$. Por lo tanto f es meromorfa en $\hat{\mathbb{C}}$.
Recíprocamente,sea f una función meromorfa con ceros en $\alpha_1, ..., \alpha_k$ con multiplicidades $m_1, ..., m_k$ y polos en $\beta_1, ..., \beta_s$ con órdenes $n_1, ...n_s$. En cada β_i, $f(z)$ posee una parte principal:

$$PP(f; \beta_i) = \frac{A_{i,n_i}}{(z - \beta_i)^{n_i}} + ... + \frac{A_{i,n_i}}{(z - \beta_i)} = \frac{h_i(z)}{(z - \beta_i)^{n_i}},$$

donde el grado de $h_i(z)$ es menor o igual que n_i. Además,

$$PP(f; \infty) = A_k z^k + A_{k-1} z^{k-1} + ... + A_1 z.$$

Entonces $h(z) = PP(f; \infty) + PP(f; \beta_1) + ... + PP(f; \beta_s)$ es una función racional, y por tanto meromorfa, cuyos únicos polos son $\beta_1, ...\beta_s$. Además, $PP(h; \beta_i) = PP(f; \beta_i)$ y $PP(h; \infty) = PP(f; \infty)$. Luego por el teorema 1.2.2, por ser f y h funciones meromorfas con polos en los mismos puntos y con las mismas partes principales, se tiene que $f(z) = h(z) + c$. Luego f es una función racional. ■

Definición 1.3.3 *Dada una función racional $f = p/q$, con p y q dos polinomios coprimos. Se llama grado de f al máximo de los grados de p y q.*

Teorema 1.3.2 *Una función racional $f : \hat{\mathbb{C}} \to \hat{\mathbb{C}}$ de grado $n > 0$, toma cada valor $c \in \hat{\mathbb{C}}$ exactamente n veces, contando multiplicidades.*

Demostración:

Por ser f una función racional, es de la forma $f = p/q$, donde p y q son dos polinomios coprimos. Supongamos que $c = \infty$. Para algún $z \in \mathbb{C}$ se tiene $f(z) = \infty$ si y sólo si $q(z) = 0$, y por el teorema fundamental del álgebra esta última ecuación tiene $gr(q)$ soluciones, contando multiplicidades. Si $gr(p) \leq gr(q)$, entonces dichas soluciones son los únicos polos de la función f. Si se cumple la desigualdad contraria, $gr(p) > gr(q)$ además de los polos anteriores, f posee uno en ∞ de orden $gr(p) - gr(q)$. En ambos casos, el número de soluciones de $f(z) = \infty$, contando multiplicidades, es $max(gr(p), gr(q))$ que es $gr(f)$.
Supongamos ahora que $c \neq \infty$. Como $gr(f) > 0$, f no es idénticamente igual a dicha constante. Luego existe una función racional

$$g = \frac{1}{f - c};$$

de modo que las soluciones de la ecuación $f(z) = c$ son exactamente el los polos de la función g, que por el argumento previo hay $gr(g)$ de estos. Como f es una función racional

$$g = \frac{q}{p - cq},$$

siendo q y $p - cq$ coprimos por serlo p y q, luego $gr(g) = max(gr(q), gr(p - cq)) = max(gr(q), gr(p)) = gr(f)$. ■

Definición 1.3.4 *Sea f una función meromorfa en $a \in \hat{\mathbb{C}}$ y sea $f(a) = c$. Se dice que a es un punto múltiple de f si la ecuación $f(z) = c$ tiene una solución múltiple en $z = a$; si $c \neq \infty$ esto es equivalente a $f'(a) = 0$, mientras que si $c = \infty$, es equivalente a que f tenga un polo de orden al menos dos en a.*
El resto de puntos se llaman puntos simples de f.

Proposición 1.3.1 *Sea $f : \hat{\mathbb{C}} \to \hat{\mathbb{C}}$ una función racional de grado $d > 0$. Entonces:*

1. *f sólo tiene un número finito de puntos múltiples en $\hat{\mathbb{C}}$*
2. *El cardinal del conjunto $f^{-1}(c)$ es igual a d para todos los puntos, excepto para un número finito de puntos $c \in \hat{\mathbb{C}}$, y $1 \leq \mid f^{-1}(c) \mid < d$ para el resto de puntos c.*

Demostración:

1. Como la derivada de f es racional y no idénticamente nula, f' tiene un número finito de ceros en $\hat{\mathbb{C}}$; como f tiene sólo un número finito de polos, se tiene.

2. Por el teorema anterior, si $c \in \hat{\mathbb{C}}$ entonces hay soluciones $z = a_1, ..., a_r$ de $f(z) = c$ con multiplicidades $k_1, ..., k_r$, satisfaciendo $k_1 + ... + k_r = d$. Por lo tanto $\mid f^{-1}(c) \mid = r$,por lo que $1 \leq \mid f^{-1}(c) \mid \leq d$, y se tiene $\mid f^{-1}(c) \mid = d$, a menos que haya algún $k_j \geq 2$. Como f sólo tiene un número finito de puntos múltiples, por (1), se tiene (2).

■

1.4. Integración de funciones racionales

Es conocido que cualquier función racional puede ser integrada en términos de funciones elementales. Para ello existen algoritmos, como el de Bernouilli, que detallamos a continuación.

1.4.1. Algoritmo de Bernoulli

Este método no es computacionalmente eficiente debido al costo de la factorización polinómica pero tiene importancia teórica.
Sea f una función racional, que se puede escribir como $f = P + A/D$, siendo $P, A, D \in \mathbb{R}[x]$, $mcd(A, D) = 1$ y $deg(A) < deg(D)$, haciendo la división polinómica del numerador de f entre su denominador. Sea

$$D \quad = \quad c \ \prod_{i=1}^{n}(x - a_i)^{e_i} \ \prod_{j=1}^{m}(x^2 + b_j x + c_j)^{f_j}$$

la factorización de D en términos de factores irreducibles sobre $\mathbb{R}$, donde c, a_i, b_j y c_j son valores reales, y e_i y f_j enteros positivos, para todos i,j. Realizando la descomposición en fracciones simples de f, se tiene que

$$f = P + \sum_{i=1}^{n}\sum_{k=1}^{e_i}\frac{A_{ik}}{(x - a_i)^k} + \sum_{j=1}^{m}\sum_{k=1}^{f_j}\frac{B_{jk}x + C_{jk}}{(x^2 + b_j x + c_j)^k}$$

siendo A_{ik}, B_{jk} y C_{jk} valores reales, para todos i,j y k. Luego

$$\int f = \int P + \sum_{i=1}^{n}\sum_{k=1}^{e_i} \int \frac{A_{ik}}{(x-a_i)^k} + \sum_{j=1}^{m}\sum_{k=1}^{f_j} \int \frac{B_{jk}x + C_{jk}}{(x^2+b_jx+c_j)^k}.$$

Veamos cada integral por separado: La primera no posee ningún problema ya que es una integral polinómica. La segunda,

$$\int \frac{A_{ik}}{(x-a_i)^k} = \begin{cases} \frac{A_{ik}(x-a_i)^{1-k}}{1-k} & si \quad k>1 \\ A_{i1}\log(x-a_i) & si \quad k=1 \end{cases}$$

Por último, calculamos la expresión de la tercera integral. Por ser $x^2+b_jx-a_i$ un polinomio irreducible en $\mathbb{R}[x]$ se tiene que $b_j^2 - 4c_j < 0$. Luego,

- Si $k=1$,

$$\int \frac{B_{j1}x + C_{j1}}{(x^2+b_jx+c_j)} = B_{j1}\int \frac{x + \frac{C_{j1}}{B_{j1}}}{x^2+b_jx+c_j} =$$

$$= B_{j1}\int \frac{x + \frac{b_j}{2} + \frac{C_{j1}}{B_{j1}} - \frac{b_j}{2}}{x^2+b_jx+c_j} =$$

$$= B_{j1}\int \frac{x + \frac{b_j}{2}}{x^2+b_jx+c_j} + B_{j1}\left(\frac{C_{j1}}{B_{j1}} - \frac{b_j}{2}\right)\int \frac{1}{x^2+b_jx+c_j} =$$

$$= \frac{B_{j1}}{2}\log(x^2+b_jx+c_j) + B_{j1}\left(\frac{C_{j1}}{B_{j1}} - \frac{b_j}{2}\right)\int \frac{1}{x^2+b_jx+c_j} =$$

$$= \frac{B_{j1}}{2}\log(x^2+b_jx+c_j) + \frac{1}{2}\left(2C_{j1} - b_jB_{j1}\right)\int \frac{1}{\left(x+\frac{b_j}{2}\right)^2 + c_j - \left(\frac{b_j}{2}\right)^2} =$$

$$= \frac{B_{j1}}{2}\log(x^2+b_jx+c_j) + \frac{1}{2}\left(\frac{2C_{j1}-b_jB_{j1}}{c_j+\left(\frac{b_j}{2}\right)^2}\right)\int \frac{1}{\left(\frac{2x+b_j}{\sqrt{4c_j-b_j^2}}\right)^2+1} =$$

$$= \frac{B_{j1}}{2}\log(x^2+b_jx+c_j) + \left(\frac{2C_{j1}-b_jB_{j1}}{\sqrt{4c_j+b_j^2}}\right)\int \frac{\frac{2}{\sqrt{4c_j+b_j^2}}}{\left(\frac{2x+b_j}{\sqrt{4c_j-b_j^2}}\right)^2+1} =$$

$$= \frac{B_{j1}}{2}\log(x^2+b_jx+c_j) + \frac{2C_{j1}-b_jB_{j1}}{\sqrt{4c_j-b_j^2}}\arctan\left(\frac{2x-b_j}{\sqrt{4c_j-b_j^2}}\right).$$

- Si $k>1$,

$$\int \frac{B_{jk}x+C_{jk}}{(x^2+b_jx+c_j)^k} = \frac{B_{jk}}{2}\int \frac{2x+\frac{2C_{jk}}{B_{jk}}+b_j-b_j}{(x^2+b_jx+c_j)^k} =$$

$$= \frac{B_{jk}}{2}\int \frac{2x+b_j}{(x^2+b_jx+c_j)^k} + \frac{B_{jk}}{2}\int \frac{\frac{2C_{jk}}{B_{jk}}-b_j}{(x^2+b_jx+c_j)^k} =$$

$$= \frac{B_{jk}}{2}\frac{1}{(1-k)(x^2+b_jx+c_j)^{k-1}} + \frac{1}{2}\int \frac{2C_{jk}-b_jB_{jk}}{(x^2+b_jx+c_j)^k}$$

Vamos a calcular el valor de la última integral. Pero para simplificar en las operaciones eliminamos los subíndices. Entonces,

$$\int \frac{1}{(x^2+bx+c)^k} = \int \frac{1}{\left(\left(x+\frac{b}{2}\right)^2-\frac{b^2}{4}+c\right)^k} = \int \frac{1}{\left(\left(x+\frac{b}{2}\right)^2-m^2\right)^k},$$

siendo $m^2=\frac{b^2}{4}-c$. Si hacemos el cambio de variable $mt=x+\frac{b}{2}$ con

$mdt = dx$, se tiene que la integral anterior es igual a

$$\int \frac{m\,dt}{((mt)^2+m^2)^k} = \frac{1}{m^{2k-1}}\int \frac{dt}{(t^2+1)^k} =$$

$$= \frac{1}{m^{2k-1}}\int \frac{t^2+1}{(t^2+1)^k}dt - \frac{1}{m^{2k-1}}\int \frac{t^2}{(t^2+1)^k}dt =$$

$$= \frac{1}{m^{2k-1}}\int \frac{1}{(t^2+1)^{k-1}}dt - \frac{1}{m^{2k-1}}\int \frac{t^2}{(t^2+1)^k}dt.$$

Si ahora hacemos integración por partes en la última integral considerando

$$u = t, \quad dv = \frac{2t}{(t^2+1)^k}dt, \quad du = dt, \quad v = -\frac{1}{(k-1)(t^2+1)^{k-1}},$$

nos queda que

$$\frac{1}{m^{2k-1}}\int \frac{1}{(t^2+1)^{k-1}}dt - \frac{1}{m^{2k-1}}\int \frac{t^2}{(t^2+1)^k}dt =$$

$$= \frac{1}{m^{2k-1}}\int \frac{1}{(t^2+1)^{k-1}}dt + \frac{1}{2(k-1)m^{2k-1}(t^2+1)^{k-1}} -$$

$$- \frac{1}{2(k-1)m^{2k-1}}\int \frac{1}{(t^2+1)^{k-1}}dt =$$

$$= \frac{2k-3}{2(k-1)m^{2k-1}}\int \frac{1}{(t^2+1)^{k-1}}dt + \frac{1}{2(k-1)m^{2k-1}(t^2+1)^{k-1}} =$$

$$= \frac{2k-3}{2(k-1)m}\int \frac{1}{((mt)^2+m^2)^{k-1}}dt + \frac{1}{2(k-1)m^{2k-1}(t^2+1)^{k-1}}.$$

Así que haciendo el cambio de variable inverso, es decir, $t = \frac{2x+b}{2m}$, se

tiene que

$$\int \frac{1}{(x^2+bx+c)^k} = \frac{2k-3}{2(k-1)m^2}\int \frac{1}{(x^2+bx+c)^{k-1}}dt+$$

$$+\frac{1}{4(k-1)m^2}\frac{2x-b}{(x^2+bx+c)^{k-1}}.$$

Luego volviendo a nuestra integral original y teniendo en cuenta lo anterior, llegamos a que

$$\int \frac{B_{jk}x+C_{jk}}{(x^2+b_jx+c_j)^k} = \frac{B_{jk}}{2}\frac{1}{(1-k)(x^2+b_jx+c_j)^{k-1}}+$$

$$+\frac{1}{2}\int \frac{2C_{jk}-b_jB_{jk}}{(x^2+b_jx+c_j)^k} =$$

$$= \frac{(2C_{jk}-b_jB_{jk})x+b_jC_{jk}-2c_jB_{jk}}{(k-1)(4c_j-b_j^2)(x^2+b_jx+c_j)^{k-1}}+$$

$$+\int \frac{(2k-3)(2C_{jk}-b_jB_{jk})}{(k-1)(4c_j-b_j^2)(x^2+b_jx+c_j)^{k-1}}.$$

Esta última fórmula puede usarse de manera recursiva hasta $k=1$.

1.4.2. Método de Hermite

Una variante del anterior algoritmo consiste en usar la factorización completa del denominador en $K[x]$. Este método muestra que toda función racional posee una integral de la forma

$$\int f = v + \sum_{i=1}^{n} c_i log(u_i),$$

donde $v, u_i, \ldots, u_n \in \bar{K}(x)$ y $c_1, \ldots, c_n \in \bar{K}$. En esta expresión, se llama *parte racional* de la integral a v y *parte trascendental* a la suma de logaritmos. El

método de Hermite calcula la parte racional v a partir de la factorización libre de cuadrados del denominador de la función racional f. La parte trascendente requiere de otros algoritmos de integración Consideramos entonces f una función racional, es decir, $f = P/Q$ donde $P, Q \in K(t)$ y $mcd(P, Q) = 1$.A continuación realizamos la división euclídea de P entre Q y obtenemos dos polinomios L y R tal que

$$\frac{P}{Q} = L + \frac{A}{Q}.$$

Consideramos la factorización $Q = Q_1 Q_2^2 \dots Q_n^n$, con cada Q_i mónico, libre de cuadrados, $mcd(Q_i, Q_j) = 1$ si $i \neq j$ y $gr(Q_i) > 0$. Entonces, si realizamos la descomposición en fracciones simples de A/Q, obtenemos que

$$\frac{R}{Q} = \sum_{k=1}^{n} \frac{A_k}{Q_k^k},$$

donde cada A_k son polinomios con coeficientes en K. Además, $gr(A_k) < gr(Q_k^k)$ o $A_k = 0$. Luego el problema se reduce a encontrar la integral de L, lo cual es sencillo por ser una integral polinómica, y una integral de la forma B/C^k, donde $gr(B) < gr(C^k)$ y C es libre de cuadrados. Veamos cómo esta última integral se puede reducir realizando integración por partes y haciendo uso del algoritmo de Euclides extendido para que cada sumando tenga un denominador libre de cuadrados.
Consideramos el sumando $\frac{A_k}{Q_k^k}$ siendo $k > 1$. Como Q_k es libre de cuadrados, entonces $mcd(Q_k, Q_k') = 1$. Luego utilizando el algoritmo de Euclides extendido, podemos determinar polinomios t y s de $K[x]$ tal que $tQ_k + sQ_k' = 1$. En particular, se pueden obtener dos polinomios S y T, tal que

$$SQ_k + TQ_k' = A_k,$$

donde $gr(S) < gr(Q_k) - 1$ y $gr(T) < gr(Q_i)$. Dividiendo por Q_k^k se obtiene que

$$\frac{SQ_k}{Q_k^k} + \frac{TQ_k'}{Q_k^k} = \frac{A_k}{Q_k^k}.$$

Luego,

$$\int \frac{A_k}{Q_k^k} = \int \frac{S}{Q_k^{k-1}} + \frac{TQ_k'}{Q_k^k}.$$

Ahora, aplicamos integración por partes a la integral, $\frac{TQ_k^{'}}{Q_k^k}$, considerando $u = T$ y $dv = \frac{Q_k^{'}}{Q_k^k}$ y obteniendo como resultado que

$$\int \frac{TQ_k^{'}}{Q_k^k} = \frac{-T}{(k-1)Q_k^{k-1}} + \int \frac{T'}{(k-1)Q_k^{k-1}}.$$

Con todo ello, hemos conseguido que el grado del denominador del término a integrar haya disminuido:

$$\int \frac{A_k}{Q_k^k} = \int \frac{S}{Q_k^{k-1}} + \frac{TQ_k^{'}}{Q_k^k} = \frac{-T}{(k-1)Q_k^{k-1}} + \int \frac{(k-1)S + T'}{(k-1)Q_k^{k-1}}.$$

1. Si $k - 1 = 1$, entonces
$$\int \frac{(k-1)S + T'}{(k-1)Q_k^{k-1}}$$
contribuye a la parte logarítmica de la integral original.

2. Si $k - 1 > 1$, entonces se aplica de nuevo el proceso de reducción a
$$\int \frac{(k-1)S + T'}{(k-1)Q_k^{k-1}}$$
hasta que los denominadores restantes queden libres de cuadrados.

Realizando este proceso tantas veces como sea necesario obtenemos el elemento v tal que la integral de f es de la forma

$$\int f = v + \sum_{i=1}^{n} c_i log(u_i).$$

Capítulo 2

Álgebra diferencial

2.1. Anillos y cuerpos diferenciales

Definición 2.1.1 *Sea A un anillo conmutativo con unidad. Una derivación en A es una aplicación $d : A \to A$ tal que para todo par de elementos $a, b \in A$ se cumplen las dos propiedades siguientes:*

- $d(a + b) = d(a) + d(b)$
- $d(ab) = d(a)b + ad(b)$

Usualmente se denota $a' = d(a)$ y $a'', a''', ..., a^{(n)}$ a las sucesivas derivadas.

Definición 2.1.2 *Dado A un anillo y d una derivación en A. Se llama anillo diferencial al par (A, d).*
Si además A es un cuerpo, se llama cuerpo diferencial al par (A, d).

Proposición 2.1.1 *Dado (A, d) un anillo diferencial se cumplen las siguientes propiedades:*

1. $d(0) = d(1) = 0$.
2. *Si A es un cuerpo, entonces*

$$d\left(\frac{a}{b}\right) = \frac{d(a)b - ad(b)}{b^2}.$$

En particular,

$$d\left(\frac{1}{b}\right) = -\frac{d(b)}{b^2}.$$

3. $d(a^n) = na^{n-1}d(a)$*, para todo* $a \in \mathbb{R} \setminus \{0\}$ *y todo* $n \in \mathbb{Z}$*.*

Demostración:

1. Teniendo en cuenta las propiedades de la aplicación d se tiene lo siguiente:

   - $d(0) = d(0 \cdot 0) = d(0) \cdot 0 + 0 \cdot d(0) = 0 + 0 = 0.$
   - $d(1) = d(1 \cdot 1) = d(1) \cdot 1 + 1 \cdot d(1) = d(1) + d(1)$, por lo que $d(1) = 0.$

2. Supongamos que A es un cuerpo, y sean $a, b \in A$ con $b \neq 0$, y $c = a/b$. Entonces $a = bc$, luego por las propiedades de la aplicación d,

   $$d(a) = d(bc) = d(b) \cdot c + b \cdot d(c) = \frac{a}{b} \cdot d(b) + b \cdot d\left(\frac{a}{b}\right)$$

   Luego,

   $$d\left(\frac{a}{b}\right) = \frac{1}{b}\left(d(a) - \frac{a}{b}d(b)\right) = \frac{b \cdot d(a) - a \cdot d(b)}{b^2}$$

3. Sea $a \in A$. Para probar esta propiedad, distinguimos en tres casos según el valor de n.

   - Si $n > 0$, lo probamos por inducción. Si $n = 1$, $d(a^1) = d(a) = 1 \cdot a^0 \cdot d(a)$. Supongamos como hipótesis de inducción que $d(a^n) = na^{n-1}d(a)$, para algún $n \geq 1$. Entonces,

     $$\begin{aligned} d(a^{n+1}) = d(a^n a) &= a^n d(a) + a d(a^n) = \\ &= a^n d(a) + a(na^{n-1}d(a)) = \\ &= (n+1)a^n d(a), \end{aligned}$$

     quedando probado (2) para $n \geq 1$.

   Ahora supongamos que A es un cuerpo.

- Si $n < 0$, se tiene que

$$d(a^n) = d\left(\frac{1}{a^{-n}}\right) = -\frac{d(a^{-n})}{a^{-2n}} = -\frac{-na^{-n-1}d(a)}{a^{-2n}} = na^{n-1}d(a).$$

- Si $n = 0$, entonces $d(a^0) = d(1) = 0 = 0a^{-1}d(a)$.

■

Definición 2.1.3 *Un A-módulo M sobre el anillo A está formado por un grupo abeliano $(M, +)$ y una operación $A \times M \to M$ tal que para toro $a, b \in A$, $n, m \in M$ se cumple:*

- $a \cdot (m + n) = a \cdot m + a \cdot n$
- $(a + b) \cdot m = a \cdot m + b \cdot m$
- $a \cdot (b \cdot m) = (a \cdot b) \cdot m$

Proposición 2.1.2 *El conjunto de todas las derivaciones en A es un A-módulo sobre A*

Demostración:

Sean d_1 y d_2 dos derivaciones en A y $c \in A$. Sea $d : A \to A$, definida como $d(a) = cd_1(a) + d_2(a)$, para algún $a \in A$. Sean $a, b \in A$. Entonces,

$$\begin{aligned} d(a + b) &= cd_1(a + b) + d_2(a + b) = \\ &= cd_1(a) + cd_1(b) + d_2(a) + d_2(b) = \\ &= d(a) + d(b), \end{aligned}$$

y

$$\begin{aligned} d(ab) = cd_1(ab) + d_2(ab) &= cad_1(b) + cbd_1(a) + ad_2(b) + bd_2(a) = \\ &= a(cd_1(b) + d_2(b)) + b(cd_1(a) + d_2(a)) = \\ &= ad(b) + bd(a). \end{aligned}$$

Luego queda probado que d es una derivación. Como la aplicación idénticamente nula en A es una derivación, queda probado que el conjunto de las derivaciones en A es un A-módulo. ■

Definición 2.1.4 *Sea (A, d) un anillo diferencial. Un ideal I de A es un ideal diferencial si $dI \subseteq I$, es decir, si para todo elemento a del ideal I, se cumple que $d(a) \in I$.*

Proposición 2.1.3 *Sean (A, d) un anillo diferencial, I un ideal diferencial en A y $\pi : A \to A/I$ la proyección canónica. Entonces d induce una derivación d^* en A/I tal que $d^* \circ \pi = \pi \circ d$.*

Demostración:

Primero definimos d^* como sigue: para $x \in A/I$ se considera $a \in A$ tal que $\pi(a) = x$ y se fija $d^*(x) = \pi(da)$. Veamos en primer lugar que la aplicación $d*$ está bien definida. Supongamos que $\pi(a) = \pi(b) = x$ para $a, b \in A$. Entonces $a - b \in I$, luego por ser I un ideal diferencial se tiene que $d(a - b) \in I$. Así que $d(a) - d(b) \in I$, y por tanto $\pi(da) = \pi(db)$, es decir, d^* está bien definido. Veamos ahora que es una derivación, para ello veamos que cumplen las propiedades de la derivación de suma y producto. Sabemos por definición de d^* que $d^* \circ \pi = \pi \circ d$. Sean $x, y \in A/I$ y $a, b \in A$ tal que $\pi(a) = x$ y $\pi(b) = y$. Entonces $\pi(a + b) = x + y$ y $\pi(ab) = xy$, y por tanto,

$$\begin{aligned} d^*(x + y) = d^*(\pi(a + b)) = \pi(d(a + b)) = \pi(da) + \pi(db) = \\ = d^*(\pi(a)) + d^*(\pi(b)) = d^*(x) + d^*(y) \end{aligned}$$

y

$$\begin{aligned} d^*(xy) = d^*(\pi(ab)) = \pi(d(ab)) = \pi(ad(b) + bd(a)) = \\ = \pi(a)\pi(d(b)) + \pi(b)\pi(d(a)) = xd^*(\pi(b)) + yd^*(\pi(a)) = \\ = xd^*(y) + yd^*(x). \end{aligned}$$

Y queda probado que d^* es una derivación en A/I. ■

2.2. Extensiones diferenciales

Definición 2.2.1 *Sean (A, d) y (B, δ) anillos diferenciales. Se dice que (B, δ) es una extensión diferencial de (A, d) si A es un subanillo de B y $\delta(a) = d(a)$ para todo $a \in A$.*

Teorema 2.2.1 *Sea (A, d) un anillo diferencial, que además es dominio de integridad y K su cuerpo de fracciones. Entonces, existe una única derivación δ en K tal que (K, δ) es una extensión diferencial de (A, d).*

Demostración:
Definimos la aplicación δ como sigue,

$$\begin{array}{rccl} \delta : K & \longrightarrow & K & \\ \dfrac{a}{b} & \to & \dfrac{b \cdot da - a \cdot db}{b^2}. & \end{array} \tag{2.1}$$

Vamos a comprobar que esta es la derivación que cumple el enunciado. Para ello veamos primero que está bien definida:
Supongamos que $a/b = x/y$, siendo $a, b, x, y \in A$. Entonces, $ay = bx$ y por lo tanto,

$$\begin{aligned} &\delta\left(\frac{a}{b}\right) - \delta\left(\frac{x}{y}\right) = \frac{b \cdot d(a) - a \cdot d(b)}{b^2} - \frac{y \cdot d(x) - x \cdot d(y)}{y^2} = \\ &= \frac{y^2 bd(a) - y^2 ad(b) - b^2 yd(x) + b^2 xd(y)}{b^2 y^2} = \\ &= \frac{(bd(y) + yd(b))(bx - ay) + abyd(y) - bxyd(b) + by(yd(a) - bd(x))}{b^2 y^2} = \\ &= \frac{d(by)(bx - ay) + by(yd(a) + ad(y) - bd(x) - xd(b))}{b^2 y^2} = \\ &= \frac{d(by)(bx - ay) + byd(ay - bx)}{b^2 y^2} = 0. \end{aligned}$$

Luego $\delta\left(\frac{a}{b}\right) = \delta\left(\frac{x}{y}\right)$ y aplicación δ está bien definida. Veamos ahora que, efectivamente, es una derivación. Para ello veamos que δ cumple las dos

propiedades que caracterizan a este tipo de aplicaciones.

$$\delta\left(\frac{a}{b}+\frac{x}{y}\right)=\delta\left(\frac{ay+bx}{by}\right)=\frac{byd(ay+bx)-(ay+bx)d(by)}{b^2y^2}=$$
$$=\frac{by^2d(a)+abyd(y)+bxyd(b)+b^2yd(x)}{b^2y^2}-$$
$$-\frac{abyd(y)+ay^2d(b)+bxyd(y)+b^2xd(y)}{b^2y^2}=$$
$$=\frac{bd(a)-ad(b)}{b^2}+\frac{yd(x)-xd(y)}{y^2}=\delta(x)+\delta(y).$$

$$\delta\left(\frac{ax}{by}\right)=\frac{byd(ax)-axd(by)}{b^2y^2}=\frac{abyd(x)+bxyd(a)-abxd(y)-axyd(b)}{b^2d^2}=$$
$$=\frac{a(yd(x)-xd(y))}{bd^2}+\frac{x(bd(a)-ad(b))}{b^2d}=\frac{a}{b}\cdot\delta\left(\frac{x}{y}\right)+\frac{x}{y}\cdot\delta\left(\frac{a}{b}\right).$$

Luego δ cumple las reglas de suma y producto, y por lo tanto, la aplicación δ es una derivación.
Veamos ahora que δ es una extensión de d. Para ello, basta observar que dado un elemento $a \in A$ arbitrario,

$$\delta(a)=\delta\left(\frac{a}{1}\right)=\frac{1d(a)-ad(1)}{1^2}=d(a)$$

Así pues, (K,δ) es una extensión diferencial de (A,d).
Por último, vamos a comprobar la unicidad de δ. Supongamos ahora que tenemos dos derivaciones δ_1 y δ_2 de K tales que (K,δ_1) y (K,δ_2) son extensiones diferenciales de (A,d). Sean $a,b \in A$ y $b \neq 0$. Entonces, utilizando la segunda propiedad de la proposición 2.1.1,

$$\delta_1\left(\frac{a}{b}\right)=\frac{b\delta_1(a)-a\delta_1(b)}{b^2}=\frac{bd(a)-ad(b)}{b^2}=\frac{b\delta_2(a)-a\delta_2(b)}{b^2}=\delta_2\left(\frac{a}{b}\right).$$

Luego $\delta_1=\delta_2$, es decir, la aplicación δ definida anteriormente es la única derivación en K tal que (K,δ) es una extensión diferencial de (A,d). ■

Definición 2.2.2 *Sean A un anillo diferencial y $A[x]$ su anillo de polinomios, siendo x una indeterminada sobre A. Para cada derivación d en A, se define la aplicación $D_d : A[x] \to A[x]$ dada por*

$$D_d\left(\sum_{i=0}^{n} a_i x^i\right) = \sum_{i=0}^{n} d(a_i)x^i$$

Proposición 2.2.1 *La aplicación D_d definida anteriormente es una derivación en $A[x]$.*

Demostración:

Sean $f, g \in A[x]$ de la forma $f = \sum_{i=0}^{n} a_i x^i$ y $g = \sum_{i=0}^{n} b_i x^i$. Veamos que se cumplen las propiedades para que D_d sea una derivación, es decir, que

$$D_d(f+g) = D_d(f) + D_d(g) \quad y \quad D_d(fg) = fD_d(g) + gD_d(f).$$

Por la definición anterior, se cumple que
$D_d(f+g) = \sum_{i=0}^{n} d(a_i+b_i)x^i = \sum_{i=0}^{n} d(a_i)x^i + \sum_{i=0}^{n} d(b_i)x^i = D_d(f) + D_d(g)$.
Además,

$$D_d(fg) = \sum_{k=0}^{2n} d\left(\sum_{i,j\geq 0, i+j=k} a_i b_j\right) x^k = \sum_{k=0}^{2n} \sum_{i,j\geq 0, i+j=k} d(a_i b_j)x^k =$$

$$= \sum_{k=0}^{2n} \sum_{i,j\geq 0, i+j=k} a_i d(b_j)x^k + \sum_{k=0}^{2n} \sum_{i,j\geq 0, i+j=k} b_j d(a_i)x^k =$$

$$= fD_d(g) + gD_d(f).$$

Luego la aplicación D_d es una derivación en $A[x]$. ■

Proposición 2.2.2 *Sea (A, d) un anillo diferencial, (B, δ) una extensión diferencial de (A, d), y x una variable indeterminada sobre A. Entonces,*

$$\delta(P(\alpha)) = D_d(P)(\alpha) + \delta(\alpha)\left(\frac{d}{dx}P\right)(\alpha)$$

para todo $\alpha \in B$ y todo polinomio $P \in A[x]$.

Demostración:

Dado $P \in A[x]$ de la forma $P = \sum_{i=0}^{n} a_i x^i$, con cada $a_i \in A$. Entonces como $\delta a_i = da_i$ para cada i y teniendo en cuenta las propiedades de derivación de productos y sumas,

$$\delta(P(\alpha)) = \delta\left(\sum_{i=0}^{n} a_i\alpha^i\right) = \sum_{i=0}^{n} \delta(a_i)\alpha^i + \delta(\alpha)\sum_{i=0}^{n} i a_i \alpha^{i-1} =$$

$$= \sum_{i=0}^{n} d(a_i)\alpha^i + \sum_{i=0}^{n} i a_i \alpha^{i-1}\delta(\alpha) =$$

$$= D_d(P)(\alpha) + \delta(\alpha)\left(\frac{d}{dx}P\right)(\alpha).$$

■

Teorema 2.2.2 *Sea (A, d) un cuerpo diferencial y sea t transcendente sobre A. Para cada $w \in A(t)$ existe una única derivación δ de $A(t)$ tal que $\delta(t) = w$ y $(A(t), \delta)$ es una extensión diferencial de (A, d).*

Demostración:

Sabemos por la proposición 2.2.1 que D_d es una derivación en $A[t]$ y por el teorema 2.2.1, que tiene una única extensión a una derivación en $A(t)$. Como d/dt es también una derivación en $A(t)$, la aplicación $\delta = D_d + w \cdot d/dt$ es una derivación en $A(t)$, por ser el conjunto de todas las derivaciones en $A(t)$ un $A(t)-$ módulo sobre $A(t)$. Tenemos que

$$\delta(t) = \left(D_d + w\frac{d}{dt}\right)(t) = D_d(t) + w\frac{d}{dt}(t) = d(1)t + w = w,$$

y para $a \in A$, que

$$\delta(a) = \left(D_d + w\frac{d}{dt}\right)(a) = D_d(a) + w\frac{d}{dt}(a) = d(a) + w \cdot 0 = d(a),$$

luego $(A(t), \delta)$ es una extensión diferencial de (A, d) que cumple lo deseado. Falta probar la unicidad de la derivación δ. Para ellos supongamos que existen

dos derivaciones δ_1 y δ_2 en $A(t)$ tal que $(A(t), \delta_1)$ y $(A(t), \delta_2)$ son extensiones diferenciales de (A, d), y tal que $\delta_1(t) = \delta_2(t) = w$. Sea $x \in A(t)$ y escribimos $x = a/b$, siendo $a, b \in A[t]$ y $b \neq 0$. Haciendo uso de la primera proposición de este capítulo en la segunda y penúltima igualdad, y aplicando la proposición anterior a a y b con $\alpha = t$,

$$\begin{aligned}\delta_1(x) = \delta_1\left(\frac{a}{b}\right) &= \frac{b\delta_1(a) - a\delta_1(b)}{b^2} = \\ &= \frac{b\left(D_d(a) + w \cdot \frac{d}{dt}(a)\right) - a\left(D_d(b) + w\frac{d}{dt}(b)\right)}{b^2} = \\ &= \frac{b\delta_2(a) - a\delta_2(b)}{b^2} = \delta_2\left(\frac{a}{b}\right) = \delta_2(x).\end{aligned}$$

Luego $\delta_1 = \delta_2$, lo que demuestra que la derivación δ es la única tal que $\delta(t) = w$ y $(A(t), \delta)$ es una extensión diferencial de (A, d). ■

Definición 2.2.3 *Un polinomio $P \in A[x]$ es separable si sus factores irreducibles, tienen todas sus raíces simples.*

Definición 2.2.4 *Un elemento algebraico de una extensión se dice que es separable si su polinomio mínimo es separable. Una extensión algebraica E de A es separable si el polinomio mínimo irreducible sobre A de todo elemento de E es separable.*

Teorema 2.2.3 *Sea (A, d) un cuerpo diferencial, y E una extensión algebraica separable de A. Entonces existe una única derivación δ en E tal que (E, δ) es una extensión diferencial de (A, d).*

Demostración:

Demostrémoslo primero para el caso particular en el que $E = A(\alpha)$ para un cierto $\alpha \in E$. Sea x una variable indeterminada sobre A y sea $P \in A[x]$ el polinomio mínimo irreducible sobre A del elemento α de E, es decir, sea P el polinomio mónico, con coeficientes de A, de menor grado tal que $P(\alpha) = 0$. Como E es una extensión algebraica separable de A, se tiene que $\left(\frac{d}{dx}P\right)(\alpha) \neq 0$. Luego si consideramos

$$w = -\frac{D_d(P)(\alpha)}{\left(\frac{d}{dx}P\right)(\alpha)} \in E,$$

como $E \simeq A[\alpha]$, existe un polinomio Q con coeficientes en A tal que $w = Q(\alpha)$. Por otro lado, sabemos que D_d es una derivación en $A[x]$, y como $\frac{d}{dx}$ lo es también en $A[x]$, se tiene que

$$\delta = D_d + Q\frac{d}{dx}$$

es una derivación en $A[x]$.
Consideramos ahora la proyección canónica $\pi : A[x] \to A[x]/(P) \simeq E$ y tenemos que

$$\begin{aligned}\pi(\delta P) &= \pi\left(D_d P + Q\frac{d}{dx}P\right) = \\ &= D_d(P)(\alpha) + Q(\alpha)\frac{d}{dx}P = \\ &= D_d(P)(\alpha) + w\frac{d}{dx}P = \\ &= D_d(P)(\alpha) - D_d(P)(\alpha) = 0\end{aligned}$$

Luego $\delta P \in Ker(\pi) = (P)$ y por tanto $Ker(\pi)$ es un ideal diferencial, lo que implica que δ induce una derivación $\delta^* : E \to E$ tal que $\pi \circ \delta = \delta^* \circ \pi$, por la proposición 2.1.3. Finalmente, para $a \in A$, tenemos que

$$\begin{aligned}\delta^*(a) = \delta^*\pi(a) = \pi\delta(a) &= \pi\left(D_d(a) + Q\frac{d}{dx}a\right) = \\ &= \pi(D_d(a)) = \pi(d(a)) = d(a),\end{aligned}$$

luego (E, δ^*) es una extensión diferencial de (A, d).
Demostrémoslo ahora en el caso general. Para ello consideramos E una extensión algebraica y separable de A, y denotamos S al conjunto de todas las extensiones diferenciales (K, δ) de (A, d) tales que $K \subseteq E$. Además, definimos el orden parcial en el conjunto S como: $(K_1, \delta_1) \leq (K_2, \delta_2)$ si (K_2, δ_2) es una extensión diferencial de (K_1, δ_1).
Como $(A, d) \in S$, S es un conjunto no vacío. Luego podemos considerar el subconjunto de S totalmente ordenado, $C = \{(K_i, \delta_i)\}$ de modo que $K = \cup_i K_i$, y definimos $\delta \in K$ como $\delta(z) = \delta_i(z)$ si $z \in K_i$. Como C es un conjunto totalmente ordenado, (K, δ) es una extensión diferencial de (A, d) que está bien definida. Además, (K, δ) es una extensión diferencial de (K_i, δ_i) para cada i, luego (K, δ) es una cota superior del conjunto C con respecto al

orden parcial $\leq$. Por lo tanto, todo subconjunto totalmente ordenado de S, tiene una cota superior en S. Luego por el lema de Zorn, existe un elemento maximal $(K_{max}, \delta_{max}) \in S$. Por la definición de S, $K_{max} \subseteq E$ y (K_{max}, δ_{max}) es una extensión diferencial de (A, d). Veamos ahora que $E \subseteq K_{max}$. Dado $z \in E$, aplicando la primera parte de la demostración, existe una derivación δ en $K_{max}(z)$ tal que $(K_{max}(z), \delta)$ es una extensión diferencial de (K_{max}, δ_{max}), luego $(K_{max}, \delta_{max}) \leq (K_{max}(z), \delta)$ en S. Esto implica que $K_{max} = K_{max}(z)$ pues (K_{max}, δ_{max}) es un elemento maximal. Por tanto, $z \in K_{max}$, luego $E = K_{max}$. Así pues, (E, δ_{max}) es una extensión diferencial de (A, d).
Por último, falta probar la unicidad de la derivación δ. Por ello, supongamos que existen dos derivaciones δ_1 y δ_2 en E tal que (E, δ_1) y (E, δ_2) son extensiones diferenciales de (A, d). Sean $z \in E$ y $P \in A[x]$ su polinomio minimal irreducible sobre A. Sabemos que por ser z un elemento de la extensión algebraica E, existe un polinomio P con coeficientes en A tal que $P(z) = 0$. Entonces, por la proposición 2.2.2, se tiene que:

$$0 = \delta_i(P(z)) = D_d(P)(z) + (\delta_i(z))\frac{dP}{dx}(z).$$

Como E es separable sobre F, $\frac{dP}{dx}(z) \neq 0$, luego

$$\delta_1(z) = -\frac{D_d(P)(z)}{\frac{dP}{dx}(z)} = \delta_2(z)$$

Como esto último se cumple para cualquier $z \in E$, $\delta_1 = \delta_2$, por lo que se concluye que existe una única derivación $\delta \in E$ tal que (E, δ) es una extensión diferenciable de (A, d). ■

Definición 2.2.5 *Dados un par de cuerpos A y K, se dice que $\sigma : A \to K$ es una inmersión, si dicha aplicación es un homomorfismo inyectivo que induce un isomorfimo de A con su imagen $\sigma(A)$.*

Definición 2.2.6 *Sea A un cuerpo y E una extensión de A. Se dice que E es una extensión normal si toda inmersión σ de E en $\bar{A}$ sobre A es un automorfismo de E.*

Teorema 2.2.4 *Sea (A, d) un cuerpo diferenciable de característica cero.*

1. *Sea F una extensión algebraica separable de A. Entonces, cualquier automorfirmo de F sobre A conmuta con d.*

2. *Sea E una extensión algebraica separable finitamente generada en A, y $T : E \to A$ y $N : E \to A$ las aplicaciones traza y norma, respectivamente, de E en A. Entonces T conmuta con D y*

$$T\left(\frac{da}{a}\right) = \frac{d(N(a))}{N(a)},$$

para todo $a \in E^*$.

Demostración:

1. Sea F una extensión algebraica separable de A. Entonces, por el teorema 2.2.3, la derivación d se extiende de forma única a una derivación de F, es decir, existe una única derivación δ de modo que (F, δ) es una extensión diferencial de (A, d). Consideramos también σ un automorfismo de F sobre A, es decir, un automorfismo de F que deja fijo A y $d_\sigma = \sigma^{-1} \circ d \circ \sigma$. Como σ es una automorfismo, y por tanto un isomorfismo, se tiene que d_σ es una derivación en F por serlo d. Además, σ es la aplicación identidad en A, luego $dx = d_\sigma x$, para todo $x \in A$. Por lo tanto, por la unicidad de la derivación vista en el teorema 2.2.3, se tiene que $d = d_\sigma$, lo que implica que $\sigma \circ d = \sigma \circ d_\sigma = d \circ \sigma$, quedando probado que el automorfismo σ conmuta con la derivación d.

2. Sea E una extensión algebraica separable finitamente generada de A, y sean $T : E \to A$ y $N : E \to A$ las aplicaciones traza y norma, respectivamente, de E en A. Sean $\bar{E}$ la clausura algebraica de E y $\sigma_1, ..., \sigma_n$ las inmersiones de E en $\bar{E}$ sobre A, es decir, los distintos homomorfismos inyectivos de E en $\bar{E}$ que inducen un isomorfismo de E en $\sigma(E)$ y que dejan fijos los elementos de A. Entonces la composición de todas las inmersiones, es decir, $F = (\sigma_1(E))...(\sigma_n(E))$ es una extensión de A. De hecho, es una extensión separable, por encontrarnos en característica cero. Por el teorema 2.2.3, la derivación d se extiende de manera única a una derivación en F de modo que (F, d) es una extensión diferencial de (A, d). Sea $a \in E$. Por el primer apartado de este teorema, tenemos

que $d(\sigma_i(a)) = \sigma_i(d(a))$, luego

$$d(T(a)) = d\left(\sum_{i=1}^{n} \sigma_i(a)\right) = \sum_{i=1}^{n} d(\sigma_i(a)) =$$
$$= \sum_{i=1}^{n} \sigma_i(d(a)) = T(d(a)),$$

Luego $d \circ T = T \circ d$, lo que prueba que la aplicación traza T conmuta con la derivación d.
Además,

$$\frac{d(N(a))}{N(a)} = \frac{d\left(\prod_i \sigma_i(a)\right)}{\prod_i \sigma_i(a)} = \sum_i \frac{d(\sigma_i(a))}{\sigma_i(a)} =$$
$$= \sum_i \frac{\sigma_i(d(a))}{\sigma_i(a)} = \sum_i \sigma_i\left(\frac{d(a)}{a}\right) =$$
$$= T\left(\frac{d(a)}{a}\right),$$

donde la cuarta igualdad es cierta por ser σ_i es un isomorfismo.

■

2.3. Monomios, y polinomios especiales y normales

Sean k un cuerpo diferencial de característica cero con derivación d, K una extensión diferencial de k, t un elemento de K y D la derivación en K.

Definición 2.3.1 *Un elemento t de K es un monomio sobre k, si se cumplen las siguientes propiedades.*

1. *El elemento t es trascendente sobre k.*
2. *$D(t) \in k[t]$.*

En el resto de la sección t será un monomio sobre k.

Notación: En lo que resta de sección, denotaremos

- $\delta(t)$ al grado de $D(t)$, es decir, al grado de t al aplicarle la derivación D.
- $\lambda(t)$ al coeficiente líder de $D(t)$.

Definición 2.3.2 *Se dice que t es lineal si $\delta(t) \leq 1$, y no lineal si ocurre la desigualdad contraria.*

Proposición 2.3.1 *Sea t un monomio sobre k y sea un polinomio $p \in k[t]$. Entonces se cumple que*

1. $gr(D(p)) \leq gr(p) + max(0, \delta(t) - 1)$
2. *Si t es no lineal y $gr(p) > 0$, entonces se cumple la igualdad en (1), y el coeficiente líder de $D(p)$ es $gr(p)l(p)\lambda(t)$, siendo $l(p)$ el coeficiente lider de p.*

Demostración:

Si $p = 0$, entonces $D(p) = 0$ y por tanto se cumple (1). Además, (2) es cierto teniendo en cuenta que el grado del polinomio idénticamente cero es $-\infty$. Por lo tanto supongamos que $p \neq 0$ y que $gr(p) = n$ y veamos que se cumplen (1) y (2).

1. Sabemos por la proposición 2.2.2 que

$$D(p) = D_d(p) + D(t)\left(\frac{dp}{dt}\right).$$

   - Si $n = 0$, entonces $dp/dt = 0$ y por tanto $D(p) = D_d(p)$, es decir, $gr(D(p)) = gr(D_d(p)) \leq n \leq n + max(0, \delta(t) - 1)$.
   - Si $n > 0$, entonces $gr(dp/dt) = n - 1$, lo que implica que

$$gr\left(D(t)\frac{dp}{dt}\right) = \delta(t) + n - 1.$$

   Por lo tanto, como $gr(D_d(p)) \leq n$ entonces

$$\begin{aligned} gr(D(p)) &\leq max\left(gr(D_d(p)), gr\left(D(t)\frac{dp}{dt}\right)\right) \leq \\ &\leq max(n, \delta(t) + n - 1) = \\ &= n + max(0, \delta(t) - 1). \end{aligned}$$

2. Supongamos que t es no lineal y $n = gr(p) > 0$. Entonces $\delta(t) > 1$ y

$$gr\left(D(t)\frac{dp}{dt}\right) = \delta(t) + n - 1 > 1 - n - 1 = n \geq gr(D_d(p)).$$

Luego al ser la desigualdad anterior estricta, se tiene que

$$gr(D(p)) = gr\left(D(t)\frac{dp}{dt}\right) = \delta(t) + n - 1.$$

Además, el coeficiente líder de dp/dt es el producto del coeficiente líder $l(p)$ del polinomio p por n, $l(p)n$. Luego el coeficiente líder de $D(p)$ es $\lambda(t)l(p)n = \lambda(t)l(p)gr(p)$.

■

Definición 2.3.3 *Se dice que $p \in k[t]$ es normal respecto a D si $mcd(p, Dp) = 1$. Decimos que p es especial con respecto a D si $mcd(p, Dp) = p$, es decir, si $p|Dp$.*

Notación:
Al conjunto formado por polinomios especiales se le denota como S. Además, si dichos polinomios son mónicos e irreducibles, el conjunto se denotará S^{Irr}.

Proposición 2.3.2 *Sean $p_1, ..., p_m \in k[t]$ tales que todos los p_i son primos entre sí, es decir, $mcd(p_i, p_j) = 1$ para $i \neq j$. Consideramos el polinomio p formado por el producto de potencias enteras de los polinomios p_i, esto es, $p = \prod_{i=1}^{m} p_i^{e_i}$ siendo $e_i \in \mathbb{Z}^+$. Entonces se cumple la siguiente igualdad:*

$$mcd(p, D(p)) = \left(\prod_{i=1}^{m} p_i^{e_i - 1}\right) \prod_{i=1}^{m} mcd(p_i, D(p_i)).$$

Demostración:
Sean $a, b \in k[t]$ y supongamos que $mcd(a, b) = 1$. Entonces,

$$\begin{aligned} mcd(ab, D(ab)) &= mcd(a, D(ab))mcd(b, D(ab)) = \\ &= mcd(a, aD(b) + bD(a))mcd(b, aD(b) + bD(a)) = \\ &= mcd(a, bD(a))mcd(b, aD(b)) = \\ &= mcd(a, D(a))mcd(b, D(b)), \end{aligned}$$

donde se ha utilizado que a y b son coprimos. Supongamos ahora como hipótesis de inducción que esto es cierto para $p_1^{e_1}, ..., p_{m-1}^{e_{m-1}}$ donde $mcd(p_i, p_j) = 1$ para $i \neq j$ y veamos que se cumple para $p_1^{e_1}, ..., p_m^{e_m} = p$:

$$
\begin{aligned}
mcd(p, Dp) &= mcd(p_1^{e_1} \dots p_m^{e_m}, D(p_1^{e_1} \dots p_m^{e_m})) = \\
&= mcd(p_1^{e_1} \dots p_{m-1}^{e_{m-1}}, D(p_1^{e_1} \dots p_m^{e_m})) \cdot mcd(p_m^{e_m}, D(p_1^{e_1} \dots p_m^{e_m})) = \\
&= mcd(p_1^{e_1} \dots p_{m-1}^{e_{m-1}}, p_m^{e_m} D(p_1^{e_1} \dots p_{m-1}^{e_{m-1}}) + p_1^{e_1} \dots p_{m-1}^{e_{m-1}} D(p_m^{e_m})) \cdot \\
&\quad \cdot mcd(p_m^{e_m}, D(p_1^{e_1} \dots p_m^{e_m})) = \\
&= mcd(p_1^{e_1} \dots p_{m-1}^{e_{m-1}}, p_m^{e_m} D(p_1^{e_1} \dots p_{m-1}^{e_{m-1}})) \cdot \\
&\quad \cdot mcd(p_m^{e_m}, D(p_1^{e_1} \dots p_m^{e_m})) = \\
&= mcd(p_1^{e_1} \dots p_{m-1}^{e_{m-1}}, p_m^{e_m} D(p_1^{e_1} \dots p_{m-1}^{e_{m-1}})) \cdot \\
&\quad \cdot mcd(p_m^{e_m}, p_m^{e_m} D(p_1^{e_1} \dots p_{m-1}^{e_{m-1}}) + p_1^{e_1} \dots p_{m-1}^{e_{m-1}} D(p_m^{e_m})) = \\
&= mcd(p_1^{e_1} \dots p_{m-1}^{e_{m-1}}, p_m^{e_m} D(p_1^{e_1} \dots p_{m-1}^{e_{m-1}})) \cdot \\
&\quad \cdot mcd(p_m^{e_m}, p_1^{e_1} \dots p_{m-1}^{e_{m-1}} D(p_m^{e_m})) = \\
&= mcd(p_1^{e_1} \dots p_{m-1}^{e_{m-1}}, p_m^{e_m} D(p_1^{e_1} \dots p_{m-1}^{e_{m-1}})) \cdot \\
&\quad \cdot mcd(p_m^{e_m}, D(p_m^{e_m})) = \\
&= mcd(p_1^{e_1}, D(p_1^{e_1})) \dots mcd(p_m^{e_m}, D(p_m^{e_m})),
\end{aligned}
$$

donde se ha tenido en cuenta que los polinomios p_i son coprimos y en la última igualdad se ha aplicado la hipótesis de inducción. Por tanto, se tiene que

$$mcd(p, D(p)) = \prod_{i=1}^{m} mcd(p_i^{e_i}, D(p_i^{e_i})).$$

Además,

$$\begin{aligned} mcd(p_i^{e_i}, D(p_i^{e_i})) &= mcd(p_i^{e_i}, e_i p_i^{e_i-1} D(p_i)) = \\ &= p_i^{e_i-1} mcd(p_i, e_i D(p_i)) = \\ &= p_i^{e_i-1} mcd(p_i, D(p_i)). \end{aligned}$$

Luego,

$$mcd(p, D(p)) = \left(\prod_{i=1}^{m} p_i^{e_i-1} \right) \prod_{i=1}^{m} mcd(p_i, D(p_i)).$$

■

Corolario 2.3.1 *Si $p \in k[t]$ es un polinomio normal, entonces es libre de cuadrados.*

Demostración:

Este corolario es consecuencia directa de la proposición anterior. Consideramos p como el producto de potencias enteras de polinomios $p_i \in k[t]$. Entonces, por la proposición anterior y por ser p un polinomio normal, se cumple que

$$1 = mcd(p, D(p)) = \left(\prod_{i=1}^{m} p_i^{e_i-1} \right) \prod_{i=1}^{m} mcd(p_i, D(p_i)).$$

Luego necesariamente debe ocurrir que los enteros $e_i = 1$, ya que de no ser así, entonces $mcd(p, D(p)) \neq 1$ contradiciendo que p es un polinomio normal. ■

Teorema 2.3.1

1. *Cualquier producto finito de polinomios normales y relativamente primos dos a dos es normal. Además, cualquier factor de un polinomio normal es normal.*

2. *El producto finito de polinomios especiales, es un polinomio especial.*

3. *Dado p un polinomio especial no nulo y q un factor de p, entonces q es un polinomio especial.*

Demostración:

1. Sean $p_1, ..., p_m \in k[t]$ polinomios normales tales que $mcd(p_i, p_j) = 1$ para $i \neq j$, y sea p el polinomio formado por un producto finito de ellos, $p = \prod_{i=1}^{n} p_i$. Veamos que p es un polinomio normal. Por la proposición 2.3.2, tenemos que

$$mcd(p, d(p)) = \left(\prod_{i=1}^{m} p_i^0\right) \prod_{i=1}^{m} mcd(p_i, D(p_i)).$$

   Además, se cumple que $mcd(p_i, D(p_i)) = 1$ por ser cada p_i un polinomio normal. Luego $mcd(p, d(p)) = 1$, es decir, p es un polinomio normal.
   Veamos ahora que cualquier factor de un polinomio normal es normal. Para ello consideramos p un polinomio normal y $q \in k[t]$ un factor de p. Entonces existe un polinomio $h \in k[t]$ tal que $p = qh$. Como p es un polinomio libre de cuadrados por el corolario 2.3.1 , se tiene que $mcd(q, h) = 1$, por lo que, de nuevo por la proposición 2.3.2, $1 = mcd(p, D(p)) = mcd(q, D(q))mcd(h, D(h))$. Luego $mcd(q, D(q)) = 1$, es decir, q es un factor normal.

2. Vamos a razonar por inducción. Comenzamos con dos polinomios, es decir, sean p_1 y p_2 dos polinomios especiales. Entonces $D(p_1) = p_1 q_1$ y $D(p_2) = p_2 q_2$ siendo $q_1, q_2 \in k[t]$. Por lo tanto,

$$D(p_1 p_2) = p_1 Dp_2 + p_2 Dp_1 = p_1 p_2 q_2 + p_2 p_1 q_1 = p_1 p_2 (q_1 + q_2).$$

   Luego $mcd(p_1 p_2, D(p_1 p_2)) = p_1 p_2$, es decir, $p_1 p_2$ es un polinomio especial. Supongamos como hipótesis de inducción que dados $p_1, ..., p_{n-1}$ polinomios especiales, entonces $\prod_{i=1}^{n-1} p_i$ es especial. Consideramos $p_1, ..., p_n$ polinomios especiales. Veamos que el producto de todos ellos, $\prod_{i=1}^{n} p_i$, es especial. Como $p_1, ..., p_n \in S$, entonces $D(p_1) = p_1 q_1, ..., Dp_n = p_n q_n \in S$. (Cabe recordar que denotamos S al conjunto de los polinomios especiales).
   Entonces,

$$\begin{aligned} D(p_1 ... p_n) &= D(p_1) p_2 \dots p_n + \dots + p_1 \dots p_{n-1} D(p_n) = \\ &= q_1 p_1 \dots p_n + \dots + q_n p_1 \dots p_n = \\ &= p_1 \dots p_n (q_1 + \dots + q_n), \end{aligned}$$

   luego $\prod_{i=1}^{n} p_i \in S$.

3. Sean p un polinomio especial no nulo, $r \in k[t]$ un factor irreducible de p, y n el exponente máximo tal que $r^n|p$. Entonces, $n \geq 1$ ya que $r|p$ y $p = r^n h$ para algún $h \in k[t]$ de modo que $mcd(r, h) = 1$. Luego por la proposición 2.3.2 y por ser $p \in S \setminus \{0\}$,

$$\begin{aligned} r^n h = p = mcd(p, D(p)) = mcd(r^n h, D(r^n h)) = \\ = r^{n-1} mcd(r, D(r)) mcd(h, D(h)) \end{aligned}$$

Por lo tanto, $rh = mcd(r, D(r))mcd(h, D(h))$. Luego por ser h y r coprimos sebe ocurrir que $mcd(h, D(h)) = h$ y $mcd(r, D(r)) = r$. Por lo tanto, r es un polinomio especial. Así pues, queda probado que todo factor irreducible de p es especial. Sea ahora $q \in k[t]$ un factor de p. Si $q \in k$, entonces q es un polinomio especial ya que $k \subset S$. En otro caso, q es un producto finito y no vacío de factores irreducibles de p. Por lo tanto, por el apartado (2) de este mismo teorema y el razonamiento previo, q es un polinomio especial.

■

Proposición 2.3.3 *Sea p un polinomio no nulo de $k[t]$. Se cumple que p es un polinomio especial con respecto a la derivación D, si y sólo si para todas las raíces α de p en la clausura algebraica de k, $D(\alpha)$ coincide con el valor obtenido al realizar $D(t)$ y evaluar el resultado obtenido en α.*

Demostración:

Sea p un polinomio no nulo de $k[t]$. Consideramos la descomposición en factores irreducibles de p sobre la clausura algebraica de k,

$$p = l \prod_{i=1}^{n} (t - \alpha_i)^{e_i},$$

donde l es el coeficiente líder del polinomio p y cada e_i es positivo. Entonces, por la proposición 2.3.2,

$$mcd(p, D(p)) = l \left(\prod_{i=1}^{m} (t - \alpha_i)^{e_i - 1} \right) \prod_{i=1}^{m} mcd(t - \alpha_i, D(t - \alpha_i)).$$

Luego para que p sea un polinomio especial, es necesario y suficiente que $mcd(t-\alpha_i, D(t-\alpha_i)) = t-\alpha_i$ para cada i. Y esto ocurre si y sólo si $t-\alpha_i$ divide a $D(t-\alpha_i) = D(t) - D(\alpha_i)$ en la clausura algebraica de k. Luego p es especial si y sólo si, al evaluar el polinomio obtenido al realizar la derivada D de t en cada raíz α_i del polinomio p, obtenemos $D(\alpha_i)$. ■

Proposición 2.3.4 *Si $c \in Const_D(k(t))$, es decir, si $D(c) = 0$, entonces tanto el numerador como el denominador de c son especiales. Además, si $c \neq 0$ y t es no lineal, entonces el numerador y el denominador de c tienen el mismo grado.*

Demostración:

Sea $c \in Const_D(k(t))$ de modo que $c = a/b$ donde $a, b \in k[t]$, $b \neq 0$ y $mcd(a,b) = 1$. Entonces,

$$0 = D(c) = \frac{bD(a) - aD(b)}{b^2},$$

lo que implica que $bD(a) = aD(b)$. Por lo tanto, como a y b son primos entre sí, se tiene que $a|Da$ y $b|Db$, es decir, $mcd(a, D(a)) = a$ y $mcd(b, D(b)) = b$. Luego a y b son especiales.

Para probar la segunda parte de la proposición vamos a razonar por reducción al absurdo. Supongamos entonces que $c \neq 0$, t es no lineal y $gr(a) \neq gr(b)$. Como $1/c \in Const_D(k(t))$, ya que $D(1/c) = \frac{1}{c^2}D(c) = 0$ por ser $D(c) = 0$, entonces podemos suponer sin pérdida de generalidad que $gr(a) > gr(b)$. Realizando la división euclídea de a entre b, se tiene que $c = p + e/b$ donde $p, e \in k[t]$, $gr(p) = gr(a) - gr(b) > 0$ y $gr(e) < gr(b)$ o $e = 0$. Entonces,

$$0 = Dc = D\left(p + \frac{e}{b}\right) = D(p) + D\left(\frac{e}{b}\right) = D(p) + \frac{bD(e) - eD(b)}{b^2}. \quad (2.2)$$

Realizando ahora la división euclidea de $bD(e) - eD(b)$ entre b^2, se tiene que existen $q, r \in k[t]$ tales que

$$\frac{bD(e) - eD(b)}{b^2} = q + \frac{r}{b^2},$$

donde $gr(r) < gr(b^2)$. Como t es no lineal, por hipótesis, $\delta(t) > 1$. Además, por la proposición 2.3.1, $gr(D(p)) = gr(p) + \delta(t) - 1$, luego $gr(D(p)) > 0$. Por lo tanto $D(p) \neq 0$. Así que, debe ser $e \neq 0$, ya que si fuese $e = 0$ entonces,

por la ecuación 2.2, sería $D(p) = 0$. Luego como $gr(b) > gr(e)$ se tiene que $gr(b) \geq 0$. Todo esto implica que

$$gr(eD(b)) = gr(e) + gr(D(b)) = gr(e) + gr(b) + \delta(t) - 1$$

y por tanto $gr(eD(b)) < 2gr(b) + \delta(t) - 1$.
Por otro lado tenemos que, o bien $e \in k$, en cuyo caso $gr(bD(e)) \leq gr(b)$, o bien $e \notin k$, en cuyo caso $gr(bD(e)) = gr(b) + gr(e) + \delta(t) - 1$. Luego en ambos casos

$$gr(bD(e)) < 2gr(b) + \delta(t) - 1.$$

Por lo tanto, $gr(bD(e) - eD(b)) < 2gr(b) + \delta(t) - 1$, lo que implica que

$$\begin{aligned} gr(q) &= gr(bD(e) - eD(b)) - 2gr(b) < \\ &< 2gr(b) + \delta(t) - 1 - 2gr(b) = \\ &= \delta(t) - 1 < gr(D(p)), \end{aligned}$$

contradiciendo que

$$0 = D(p) + q + \frac{r}{b^2}. \tag{2.3}$$

Como $gr(q) < gr(D(p))$ entonces $gr(q + D(p)) = gr(D(p))$. Si se tuviera la igualdad 2.3, entonces multiplicando por b^2 a ambos lados de la igualdad, obtendríamos que $-r = (q + D(p))b^2$. Tomando grados en esta última igualdad y teniendo en cuenta que $gr(q + D(p)) = gr(D(p))$,

$$gr(r) = gr(D(p)) + 2gr(b) \geq 0.$$

Pero se tenía que $gr(r) < gr(b^2) = 2gr(b)$, lo cual es absurdo. Luego queda probado que $gr(a) = gr(b)$. ■

Por último damos unas definiciones que nos serán de utilidad en las secciones posteriores.

Definición 2.3.4 *Se dice que $u \in k$ es una derivada logarítmica de un $k-$radical si existe un $v \in k^*$ y un entero no nulo e de modo que $eu = Dv/v$.*

Ejemplo:
Consideramos $k = \mathbb{Q}(x)$ con derivación $D = d/dx$, y sea $u = 1/(2x) \in k$. Como $2u = D(x)/x$, entonces u es la derivada logarítmica de un $\mathbb{Q}(x)$-radical. De hecho, u es la derivada logarítmica de $\sqrt{x}$.

Definición 2.3.5 *Se dice que $q \in k[t]$ es especial de primer tipo con respecto a la derivación D si q es un polinomio especial y para toda raíz r de q en una extensión algebraicamente cerrada de k, $p_r(r)$ no es una derivada logarítmica de un $k(r)-$radical, donde*

$$p_r = \frac{D(t) - D(r)}{t - r} \in k(r)[t].$$

Notación: Se denota S_1 al conjunto de todos los polinomios especiales de primer tipo, y S_1^{Irr} al subconjunto del anterior tal que sus polinomios sean, además, mónicos e irreducibles.

Proposición 2.3.5 *Sea E una extensión algebraica de k, y un elemento $u \in k$. Si u no es una derivada logarítmica de un $k-$radical, entonces tampoco lo es de un $E-$radical.*

Demostración:

Consideramos un elemento $u \in k$ de modo que no sea la derivada logarítmica de un $k-$radical. Vamos a razonar por reducción al absurdo. Para ello supongamos que u es la derivada logarítmica de un radical sobre E, es decir, existe un elemento $v \in E^*$ y un entero no nulo e de modo que $eu = D(v)/v$. Como E es una extensión algebraica de k, podemos considerar el polinomio mínimo p de v con coeficientes en k. Este es mónico e irreducible, por lo que podemos suponer que es de la forma $p = b_0x + b_1x^1 + ... + b_{n-1}x^{n-1} + x^n$, siendo $b_j \in k$ para todo $j = 0, \ldots, n-1$ y $b_j \neq 0$ para al menos uno de dichos j por ser p irreducible. Entonces $p(v) = 0$ y por tanto $D(p(v)) = 0$. Además,

$$\begin{aligned} D(p(v)) &= \sum_{j=1}^{n-1}(D(b_j)v^j + jb_jv^{j-1}D(v)) + nv^{n-1}D(v) = \\ &= \sum_{j=1}^{n-1}(D(b_j)v^j + jb_jv^jeu) + nv^neu = \\ &= \sum_{j=1}^{n-1}(D(b_j) + jb_jeu)v^j + nv^neu = q(v), \end{aligned}$$

siendo $q(x) = \sum_{j=1}^{n-1}(D(b_j) + jb_jeu)x^j + nx^neu$ un polinomio en $k[x]$. Luego $q(v) = 0$ y como p es un polinomio mínimo de v con coeficientes en k, se

tiene que p divide al polinomio q. Entonces, debe cumplirse que $q = neup$ para igualar los coeficientes líderes. Por lo tanto, $D(b_j) + jb_jeu = neub_j$ para todo j desde 1 hasta $n-1$. Por lo tanto,

$$\frac{D(b_j)}{b_j} = neu - jeu = eu(n-1),$$

es decir, u es la derivada logarítmica de un $k-$radical, por definición, lo que contradice nuestra hipótesis. Luego queda probada la proposición. ■

2.4. Aplicación orden

Dado K un dominio de factorización única, K^* su grupo de unidades, F su cuerpo de fracciones y $a \in K$ tal que $a \neq 0$ y $a \notin K^*$.

Definición 2.4.1 *El orden en a es la aplicación* $v_a : K \to \mathbb{Z} \bigcup \{\infty\}$ *dada por:*

1. $v_a(0) = +\infty$.
2. $v_a(x) = max\{n \in \mathbb{N} \quad tal \quad que \quad a^n | x\}$, *si* $x \in K \setminus \{0\}$.

Proposición 2.4.1 *Sean dos elementos* $x, y \in K$. *Entonces se cumplen las siguientes propiedades:*

1. $v_a(xy) \geq v_a(x) + v_a(y)$, *y se da la igualdad si y sólo si a es irreducible.*
2. $v_a(x+y) \geq min(v_a(x), v_a(y))$, *dándose la igualdad si y sólo si* $v_a(x) \neq v_a(y)$.
3. *Si* $x|y$, *entonces* $v_a(x) \leq v_a(y)$.
4. $v_a(mcd(x,y)) = min(v_a(x), v_a(y))$.

Demostración:

Todos los puntos son triviales si $x = 0$ o $y = 0$. Así que supongamos que $x \neq 0$ e $y \neq 0$. Sea $n = v_a(x)$ y $m = v_a(y)$. Entonces $x = ba^n$ e $y = ca^m$, para algún $b, c \in K$ tal que a no divide a b ni c.

1. Tenemos que $xy = bca^{n+m}$, luego $v_a(xy) \geq n + m$. Supongamos que a es irreducible. Entonces, como a no divide ni a b ni a c se tiene que $a \nmid bc$. Luego $a^{n+m+1} \nmid xy$. Por lo tanto $v_a(xy) = n + m$.

2. Podemos suponer sin pérdida de generalidad que $n \leq m$. Tenemos que $x + y = ba^n + ca^m = a^n(b + ca^{m-n})$, luego $v_a(x + y) \geq n = min(n, m)$. Ahora supongamos que $n \neq m$, es decir, $m - n > 0$. Entonces, $a|ca^{m-n}$. Esto implica que $a \nmid (b + ca^{m-n})$ ya que en caso de hacerlo, como a divide a ca^{m-n}, entonces a dividiría a b. Pero esto no ocurre, por hipótesis. Luego $v_a(x + y) = n$.

3. Supongamos que $x|y$. Entonces, $y = xz$ para algún $z \in K$. Luego $v_a(y) = v_a(x) + v_a(z)$, por el primer apartado de esta proposición. Por tanto $v_a(y) \geq v_a(x)$.

4. Sea $g = mcd(x, y)$. Entonces $g|x$ y $g|y$, luego $v_a(g) \leq v_a(x)$ y $v_a(g) \leq v_a(y)$, por el apartado anterior. Por tanto $v_a(g) \leq min(v_a(x), v_a(y))$. Por otro lado, sea $z = a^{min(v_a(x), v_a(y))} \in D$. Entonces $z|x$ y $z|y$, luego $z|g$. Por tanto, $v_a(g) \geq v_a(z) = min(v_a(x), v_a(y))$ por (3). Luego juntando ambas desigualdades, $v_a(g) = min(v_a(x), v_a(y))$.

■

Proposición 2.4.2 *Sea $u \in K^*$ y $x \in K$. Entonces, se verifica que*

1. $v_a(ux) = v_a(x) = v_{ua}(x)$

2. $v_a(u) = 0$

Demostración:

1. Si $x = 0$, entonces $v_a(ux) = v_a(x) = v_{au}(x) = +\infty$. Así que supongamos que $x \neq 0$. Entonces, $a^{v_a(x)}|x$. Luego $a^{v_a(x)}|ux$ y por tanto, $v_a(x) \leq v_a(ux)$. Como esta desigualdad es cierta para cualquier unidad, y u^{-1} es una unidad en K, se tiene que $v_a(ux) \leq v_a(u^{-1}ux) = v_a(x)$. Por tanto, $v_a(x) = v_a(ux)$.
   De manera similar, si $a^{v_a(x)}|x$ entonces, $(ua)^{v_a(x)}|x$, ya que $u^{v_a(x)}$ es una unidad. Luego $v_a(x) \leq v_{au}(x)$. Además, si aplicamos dicha desigualdad a ua y u^{-1} se tiene que $v_{ua}(x) \leq v_{u^{-1}ua}(x) = v_a(x)$. Luego, $v_a(x) = v_{ua}(x)$.

2. Por el apartado anterior, sabemos que $v_a(u) = v_a(u^2)$. Pero $v_a(u^2) \geq 2v_a(u)$ por la proposición 2.4.1. Luego, o bien $v_a(u) = 0$ o bien $v_a(u) = +\infty$. Pero $u \neq 0$. Así que, debe ser $v_a(u) = 0$.

■

Definición 2.4.2 *Sea $x \in F^*$, siendo x de la forma $x = y/z$, donde $y, z \in K$ no tienen factores comunes y $z \neq 0$. Se define $v_a(x) = v_a(y) - v_a(z)$.*

Teorema 2.4.1 *Sean $x, y \in F$ y supongamos que a es irreducible en K. Entonces, se verifican las siguientes propiedades:*

1. *$v_a(xy) = v_a(x) + v_a(y)$.*
2. *si $x \neq 0$, $v_a(x^m) = mv_a(x)$ para todo $m \in \mathbb{Z}$.*
3. *$v_a(x + y) \geq min(v_a(x), v_a(y))$, dándose la igualdad si $v_a(x) \neq v_a(y)$.*

Demostración:

Consideramos dos elementos $x, y \in F$ y escribimos $x = b/c$ e $y = d/e$, donde $b, c, d, e \in K$, b y c no tienen factores comunes, d y e tampoco los tienen, $c \neq 0$ y $e \neq 0$.
Como a es irreducible, por la proposición 2.4.1 se tiene que $v_a(fg) = v_a(f) + v_a(g)$ para algún $f, g \in K$. Veamos que se cumplen las propiedades del enunciado.

1. Consideramos $h = mcd(bd, ce)$, $f = bd/h$ y $g = ce/h$. Tenemos que $f, g, h \in K$, f y g no tienen factores comunes, y $xy = bd/ce = f/g$, luego

$$\begin{aligned} v_a(xy) = v_a(f) - v_a(g) = v_a(f) + v_a(h) - (v_a(g) + v_a(h)) = \\ = v_a(fh) - v_a(gh) = v_a(bd) - v_a(ce) = \\ = (v_a(b) - v_a(c)) + (v_a(d) - v_a(e)) = v_a(x) + v_a(y) \end{aligned}$$

2. $x^0 = 1$ es una unidad en K, luego $v_a(1) = 0$ por la proposición 2.4.2. Para el caso en el que $m \geq 0$ lo probamos por inducción, suponiendo como hipótesis que para algún $m \geq 0$ se cumple la desigualdad. Entonces,

$$\begin{aligned} v_a(x^{m+1}) = v_a(x^m x) = v_a(x^m) + v_a(x) = \\ = mv_a(x) + v_a(x) = (m+1)v_a(x), \end{aligned}$$

   lo que prueba la igualdad para $m + 1$. Luego queda probado el punto (2) para valores positivos de m. Para $m < 0$ tenemos que $0 = v_a(1) = v_a(x^m x^{-m}) = v_a(x^m) - mv_a(x)$. Luego $v_a(x^m) = mv_a(x^m)$.

3. $x + y = (be + cd)(ce)^{-1}$. Aunque $be + cd$ y ce pueden tener factores comunes, tenemos que

$$v_a(x + y) = v_a(be + cd) + v_a((ce)^{-1}) = v_a(be + cd) - v_a(ce),$$

   por los apartados anteriores de este mismo teorema. Podemos suponer sin pérdida de generalidad que $v_a(x) \leq v_a(y)$, lo que implica que $v_a(b) - v_a(c) \leq v_a(d) - v_a(e)$. Luego $v_a(b) + v_a(e) \leq v_a(d) + v_a(c)$. Así pues, $v_a(be) \leq v_a(ce)$. Luego $v_a(be + cd) \geq v_a(be)$ por la proposición 2.4.1. Por lo tanto

$$v_a(x+y) \geq v_a(be) - v_a(ce) = v_a(b) - v_a(c) = v_a(x) = min(v_a(x), v_a(y)).$$

   Veamos ahora la segunda parte de este apartado, es decir, veamos que se da la igualdad si $v_a(x) \neq v_a(y)$. Para ello supongamos que $v_a(x) < v_a(y)$. Entonces, $v_a(be) < v_a(dc)$ como en el caso anterior. Luego, $v_a(be+cd) = v_a(be)$, por la proposición 2.4.1. Por tanto, $v_a(x+y) = v_a(be) - v_a(ce) = v_a(x) = min(v_a(x), v_a(y))$.

■

Definición 2.4.3 *Una aplicación que cumple las tres propiedades del anterior teorema se llama valoración.*

Teorema 2.4.2 *Sea F un cuerpo, E una extensión algebraica y separable de F y x una variable indeterminada en E. Sea $p \in F[x]$ un polinomio irreducible sobre F. Entonces, para cualquier factor irreducible $q \in E[x]$ de $p \in E[x]$, y cualquier $f \in F(x)$ se cumple que, $v_p(f) = v_q(f)$.*

Demostración:

Consideramos $q \in E[x]$ un factor irreducible de p en $E[x]$. Luego, existe un polinomio $r \in E[x]$ tal que $p = qr$. Sea $h \in F[x]$ y $n = v_p(h) \geq 0$. Entonces $p^n|h$. Es decir, existe un elemento $s \in F[x]$ tal que $h = p^n s$. Luego, por ser $p = qr$, se tiene que $h = q^n r^n s$. Además, sabemos que $p^{n+1} \nmid h$ ya que n es el mayor número natural tal que p^n divide a h. Luego p no puede dividir a s. Por tanto $mcd(p, s) = 1$, ya que tampoco puede ocurrir que s divida a p puesto que p es irreducible en $F[x]$. Luego, por la identidad de Bezout, existen $a, b \in F[x]$ tal que $1 = ap + bs$. Y como $p = qr$, se cumple que $1 = arq + bs$. Luego, de nuevo por la identidad de Bezout, $mcd(q, s) = 1$. Supongamos ahora que $q^m|h$, para aun cierto $m > n$. Entonces, existe un elemento $t \in E[x]$, tal que $h = p^n s = q^n r^n s = q^m t$. Luego $r^n s = q^{m-n} t$ y por tanto, q divide a $r^n s$ en $E[x]$. Pero sabemos que q es irreducible y $mcd(q, s) = 1$, entonces $q|r^n$. Por lo tanto $n > 0$ ya que en caso contrario q sería una unidad. En particular $q|r$, luego $q^2|p$. Esto contradice p era un polinomio libre de cuadrados en $E[x]$ por ser esta última una extensión algebraica y separable de F. Luego $q^m \nmid h$ siendo $m > n$. Por lo tanto, $v_q(h) = n$. Para concluir consideramos $f \in F[x]$ y escribimos $f = a/b$, siendo $a, b \in F[x]$ y $b \neq 0$. Entonces,

$$v_p(f) = v_p\left(\frac{a}{b}\right) = v_p(a) - v_p(b) = v_q(a) - v_q(b) = v_q\left(\frac{a}{b}\right) = v_q(f),$$

donde en la tercera igualdad se ha empleado el razonamiento anterior. ■

2.4.1. Aplicación orden en infinito

Definición 2.4.4 *Sea K un dominio de integridad. Se llama orden en infinito a la aplicación $v_\infty : K(x) \to \mathbb{Z} \cup \{+\infty\}$ dada por $v_\infty(0) = +\infty$ y*

$v_\infty(b/c) = gr(c) - gr(b)$, *para* $b, c \in K[x] \setminus \{0\}$.

A continuación, vamos a probar que la aplicación orden en infinito es una valoración.

Proposición 2.4.3 *Sean dos elementos* $f, g \in K(x)$. *Entonces, se cumplen las siguientes propiedades:*

1. $v_\infty(fg) = v_\infty(f) + v_\infty(g)$.
2. *Si* $f \neq 0$ *entonces* $v_\infty(f^m) = mv_\infty(f)$, *para todo entero* m.
3. $v_\infty(f+g) \geq min(v_\infty(f), v_\infty(g))$. *Además, se da la igualdad si y sólo si* $v_\infty(f) \neq v_\infty(g)$.

Demostración:
Consideramos dos elementos $f, g \in K(x)$. Escribimos $f = b/c$ y $g = d/e$, donde b, c, d, e son polinomios de $K[t]$ con c y e no nulos. Veamos que se cumplen las propiedades del enunciado.

1. Al hacer el producto de f por g, obtenemos que $fg = bd/ce$. Luego,

$$\begin{aligned} v_\infty(fg) &= gr(ce) - gr(bd) = \\ &= gr(c) + gr(e) - gr(b) - gr(d) = \\ &= (gr(c) - gr(b)) + (gr(e) - gr(d)) = \\ &= v_\infty(f) + v_\infty(g). \end{aligned}$$

2. Consideramos ahora $f \neq 0$. Veamos que para cualquier entero m se cumple que $v_\infty(f^m) = mv_\infty(f)$. Vamos a probarlo por inducción. Para $m = 1$ es trivial. Luego supongamos como hipótesis de inducción que la igualdad es cierta para un entero $m - 1 > 0$ y veamos que es cierto para m. Entonces,

$$\begin{aligned} v_\infty(f^m) = v_\infty(f^{m-1}f) = v_\infty(f^{m-1}) + v_\infty(f) = \\ = (m-1)v_\infty(f) + v_\infty(f) = mv_\infty(f), \end{aligned}$$

donde se ha aplicado el primer apartado de la proposición en la segunda igualdad y la hipótesis de inducción en la tercera.

3. Consideramos la suma de f y g,

$$f+g=\frac{b}{c}+\frac{d}{e}=\frac{be+cd}{ec}.$$

Luego, $v_\infty(f+g)=gr(ec)-gr(be+cd)$. Supongamos, sin pérdida de generalidad, que $v_\infty(f)\leq v_\infty(g)$. Entonces, $gr(c)-gr(b)\leq gr(e)-gr(d)$, o lo que es equivalente, $gr(c)+gr(d)\leq gr(e)+gr(b)$. Luego, $gr(cd)\leq gr(eb)$, es decir, $gr(be+cd)\leq gr(eb)$. Por lo tanto,

$$\begin{aligned}v_\infty(f+g)&\geq gr(ec)-gr(eb)=gr(c)-gr(b)=\\&=v_\infty(f)=min(v_\infty(f),v_\infty(g)).\end{aligned}$$

Además, si $v_\infty(f)\neq v_\infty(g)$, es decir, si $v_\infty(f)<v_\infty(g)$, entonces $gr(cd)<gr(eb)$. Luego $gr(be+cd)=gr(eb)$. Por lo tanto,

$$\begin{aligned}v_\infty(f+g)&=gr(ec)-gr(be+cd)=gr(ec)-gr(eb)=\\&=gr(c)-gr(b)=v_\infty(f)=min(v_\infty(f),v_\infty(g)).\end{aligned}$$

El razonamiento es análogo si fuese $v_\infty(g)\leq v_\infty(f)$.

■

Teorema 2.4.3 *Sea K un anillo diferencial con derivación D y t un monomio sobre K. Dado $f\in K(t)\setminus\{0\}$. Entonces,*

$$v_\infty(Df)\geq v_\infty(f)-max(0,\delta(t)-1).$$

Además, si t es lineal y $v_\infty(f)=0$, entonces la desigualdad anterior es estricta.

Demostración:

Consideramos $f=a/b\in K(t)\setminus\{0\}$, donde $a,b\in K[t]$, b es no nulo y $mcd(a,b)=1$. Entonces,

$$D(f)=\frac{bD(a)-aD(b)}{b^2}.$$

Luego,

$$v_\infty(D(f))=gr(b^2)-gr(bD(a)-aD(b))=2gr(b)-gr(bD(a)-aD(b)).$$

Sabemos por la proposición 2.3.1 que $gr(D(a)) \leq gr(a) + max(0, \delta(t) - 1)$ y $gr(D(b)) \leq gr(b) + max(0, \delta(t) - 1)$. Por lo tanto,

$$gr(bD(a) - aD(b)) \leq gr(a) + gr(b) + max(0, \delta(t) - 1).$$

Luego,

$$\begin{aligned} v_\infty(D(f)) &\geq 2gr(b) + gr(a) + gr(b) + max(0, \delta(t) - 1) = \\ &= gr(b) - gr(a) - max(0, \delta(t) - 1) = \\ &= v_\infty(f) - max(0, \delta(t) - 1). \end{aligned}$$

Además, si t es lineal, entonces $\delta(t) \leq 1$. Así que, si $v_\infty(f) = 0$ se tiene la desigualdad estricta. ■

2.4.2. Localizaciones

Consideramos de nuevo K un dominio de factorización única, K^* su grupo de unidades, F su cuerpo de fracciones y a un elemento de K tal que $a \neq 0$ y $a \notin K^*$.

Definición 2.4.5 *Llamaremos localización de a en K al conjunto*

$$\Theta_a = \cap_{p|a}\{x \in F / \quad v_p(x) \geq 0\},$$

donde los elementos p son los factores de a en K.

Proposición 2.4.4 *El conjunto localización de a en K verifica las siguientes propiedades:*

1. *Θ_a es un subanillo de F que contiene a K.*
2. *Si $x \in \Theta_a$, entonces $v_a(x) \geq 0$.*
3. *Se cumple que $x \in a\Theta_a$ si y sólo sí, $v_a(x) \geq 1$, donde $a\Theta_a$ es el ideal generado por a en Θ_a.*
4. *Si a es irreducible, entonces $x \in \Theta_a$ si y sólo sí $v_a(x) \geq 0$.*
5. *Si a es irreducible, entonces $xa^{-v_a(x)} \in \Theta_a$ para todo $x \in F^*$.*
6. *Si δ es una derivación en K, entonces $\delta\Theta_a \subseteq \Theta_a$.*

Demostración:

1. Sea $p \in K$ un factor irreducible de a, y consideramos $x, y \in \Theta_a$. Entonces, por definición de localización, se tiene que $v_p(x) \geq 0$ y $v_p(y) \geq 0$. Sabemos por la proposición 2.4.2 que $v_p(-y) = v_p(y)$. Luego por el teorema 2.4.1, se tiene que $v_p(x-y) \geq 0$ y $v_p(xy) \geq 0$. Y como esto es cierto para cualquier factor irreducible p de a, por la definición anterior, se tiene que $x - y \in \Theta_a$ y $xy \in \Theta_a$.
   Consideramos ahora un elemento $c \in K$. Entonces, $v_p(c) \geq 0$ para todo factor irreducible p de a, luego $K \subseteq \Theta_a$. En particular, $0, 1 \in \Theta_a$. Así que, queda probado que Θ_a es un subanillo de F que contiene al dominio de factorización única K.

2. Sea $x \in \Theta_a$ de modo que $x = b/c$ donde $b, c \in K$ no tienen factores comunes. Sea $p \in K$ un factor irreducible de a. Entonces $v_p(x) \geq 0$, por ser $x \in \Theta_a$. Luego $v_p(b) - v_p(c) \geq 0$. Además, no puede ocurrir al mismo tiempo que $v_p(b) \neq 0$ y $v_p(c) \neq 0$, ya que de hacerlo, entonces por definición de $v_p(x)$ se tendría que $p|b$ y $p|c$, contradiciendo que b y c no tienen factores comunes. Asimismo $v_p(b)$ y $v_p(c)$ son valores no negativos por ser $b, c \in K$. Luego debe ser $v_p(c) = 0$. Por lo tanto, $p \nmid c$, luego $a \nmid c$, por ser p cualquier factor irreducible de a. Como consecuencia de esto último $v_a(c) = 0$. Luego, $v_a(x) = v_a(b) - v_a(c) = v_a(b) \geq 0$.

3. Para probarlo veremos ambas implicaciones por separado.

   - Sea $x \in a\Theta_a$, entonces existe algún elemento $y \in \Theta_a$ tal que $x = ay$. Consideramos y de la forma $y = b/c$ donde $b, c \in K$ no tienen factores comunes. Siguiendo el mismo razonamiento que en la demostración del apartado anterior, se tiene que $p \nmid c$ para ningún factor irreducible p de a. Por lo tanto a y c no tienen ningún factor en común. Por hipótesis, b y c tampoco lo tienen. Luego, c y ab no tienen ningún factor irreducible en común. Así que, por la definición 2.4.2,

$$v_a(x) = v_a(ay) = v_a\left(\frac{ab}{c}\right) = v_a(ab) - v_a(c).$$

Pero de nuevo siguiendo el mismo razonamiento del segundo apartado de esta misma proposición, se tiene que $v_a(c) = 0$, luego $v_a(x) = v_a(ab) \geq v_a(a) + v_a(b) \geq 1$ siendo la primera desigualdad cierta por la proposición 2.4.1 y la segunda teniendo en cuenta que $v_a(a) = 1$ y $v_a(b) \geq 0$.

- Ahora vamos a probar la segunda implicación. Sea $x \in F^*$ de modo que $v_a(x) \geq 1$. Escribimos $x = b/c$, donde $b, c \in K$ no tienen factores comunes. De nuevo, por el razonamiento seguido en la prueba de (2), o bien $v_a(b) = 0$ o bien $v_a(c) = 0$. Además, $v_a(x) = v_a(b) - v_a(c) \geq 1$. Luego $v_a(c) = 0$ y $v_a(b) \geq 1$ Por lo tanto, a divide a b, es decir, $b = ad$ para un cierto $d \in K$. Sea ahora $p \in K$ un factor irreducible de a. Entonces, $p|b$ ya que $p|a$. Por lo tanto, $p \nmid c$ por no tener c y b factores comunes. Luego

$$v_p(d/c) = v_p(d) - v_p(c) = v_p(d) \geq 0.$$

Como esto es cierto para cualquier factor irreducible p de a, se tiene que $d/c \in \Theta_a$. Luego,

$$x = \frac{b}{c} = a\frac{d}{c} \in a\Theta_a.$$

4. - Sea $x \in \Theta_a$, entonces por el segundo apartado de esta misma proposición, se tiene que $v_a(x) \geq 0$.
   - Recíprocamente, supongamos que a es irreducible y consideramos $x \in F$ de modo que $v_a(x) \geq 0$. Sea p un factor irreducible de a en K. Entonces $p = ua$, para un cierto $u \in K^*$. Luego por la proposición 2.4.2, $v_p(x) = v_{ua}(x) = v_a(x)$. Por lo tanto, $v_p(x) \geq 0$. Es decir, $x \in \Theta_a$.

5. Supongamos que a es irreducible, y sea $x \in F^*$. Entonces,

$$\begin{aligned} v_a(xa^{-v_a(x)}) &= v_a(x) + v_a(a^{-v_a(x)}) = \\ &= v_a(x) + (-v_a(x))v_a(a) = \\ &= v_a(x) - v_a(x) = 0. \end{aligned}$$

Luego, por el apartado anterior, $xa^{-v_a(x)}$.

6. Sea δ una derivación en K. Entonces, por el teorema 2.2.1 , δ puede extenderse de forma única a una derivación en F. Sea $x \in \Theta_a$ y escribimos $x = b/c$, donde $b, c \in K$ no tienen factores comunes y $c \neq 0$. Sea $p \in K$ un factor irreducible de a. Entonces, $v_p(x) = v_p(b) - v_p(c) \geq 0$ ya que $x \in \Theta_a$. Luego, $v_p(c) = 0$, por el mismo razonamiento usado en el apartado (2). Esto implica que

$$\begin{aligned} v_p(\delta x) = v_p\left(\delta\left(\frac{b}{c}\right)\right) = v_p\left(\frac{c\delta(b) - b\delta(c)}{c^2}\right) = \\ = v_p(c\delta(b) - b\delta(c)) - v_p(c^2) = \\ = v_p(c\delta(b) - b\delta(c)) - 2v_p(c) = \\ = v_p(c\delta(b) - b\delta(c)) \geq 0 \end{aligned}$$

Como esto es cierto para cualquier factor irreducible a, se tiene que $\delta(x) \in \Theta_a$, luego $\delta(\Theta_a) \subset \Theta_a$.

■

Consideramos ahora que K es un dominio de ideales principales e I un ideal propio de K. En la definición que viene a continuación vamos a construir una extensión de la proyección canónica $\pi_I : K \to K/I$ a una localización Θ_a, donde a es un generador del ideal I.

Definición 2.4.6 *Sean K un dominio de ideales principales e I un ideal propio no nulo de K, es decir, $I \neq K$ e $I \neq (0)$, y $a \in K$ un generador del ideal I, es decir, $I = (a)$. Se define el valor de a como la aplicación $\pi_a : \Theta_a \to K/I$ como:*
Sea $x \in \Theta_a$ de modo que $x = b/c$ donde $b, c \in K$ no tienen factores comunes. Se define $\pi_a(x)$ como $\pi_I(bd)$ donde $d, e \in K$ son tal que $cd + ae = 1$ y π_I es la proyección canónica de K en K/I.

Proposición 2.4.5 *La aplicación π_a definida anteriormente está bien definida y es una extensión de π_I.*

Demostración:

Vamos a probar en primer lugar que la aplicación está bien definida, es decir, que siempre existen los valores d y e, y que el valor de la aplicación en

un punto x, $\pi_a(x)$ no depende de la elección de los elementos b, c, d y e.
En primer lugar, por ser I un ideal propio no nulo, se tiene que $a \neq 0$ por ser $I \neq (0)$, y $a \notin K^*$ por ser $I \neq K$. Luego, el cuerpo localización de a, Θ_a, está definido. Consideramos x un elemento de dicho conjunto y escribimos $x = b/c$, donde $b, c \in K$ no tienen factores en común. Consideramos p un factor irreducible de a, entonces por ser $x \in \Theta_a$ debe ser $v_p(x) = v_p(b) - v_p(c) \geq 0$. Pero, o bien $v_p(b) = 0$ o bien $v_p(c)$, ya que por hipótesis b y c no tienen factores en común. Luego ha de ser $v_p(c) = 0$, es decir, p no divide a c. Por ser esto cierto para cualquier factor irreducible p de a, entonces $mcd(a, c) = 1$. Luego por la Identidad de Bezout, existen dos elementos $d, e \in K$ tal que $ae + cd = 1$. Ya tenemos probado que siempre existen los valores d y e de la definición. Veamos ahora que el valor de $\pi_a(x)$ no depende de ellos. Para ello, supongamos que también existen dos elementos $f, g \in K$ tal que $ae + cd = ag + cf = 1$. Entonces, $a(e - g) = c(f - d)$. Y dado un factor irreducible p de a,

$$v_p(c) + v_p(f - d) = v_p(c(f - d)) = v_p(a(e - g)) = v_p(a) + v_p(e - g) \geq v_p(a).$$

Pero habíamos probado que $v_p(c) = 0$, por lo que debe ser $v_p(f - d) \geq v_p(a)$. Es decir, si denotamos $m = v_p(f - d)$ y $n = v_p(a)$, entonces $m \geq n$ y p^m divide a $(f - d)$ y p^n divide a a. Luego a divide a $(f - d)$, es decir, $f - d \in I$. Por lo tanto, $\pi_I(f - d) = 0$. Y por ser π_I un homomorfismo de anillos, se tiene que $\pi_I(bf) = \pi_I(bd)$, es decir, el valor de $\pi_a(x)$ no depende de la elección de d y e.
Veamos ahora que dicho valor tampoco depende de b y c. Supongamos entonces que $x = b/c = b'/c'$, donde $b, c, b', c' \in K$, y ni b y c , ni b' y c' tienen factores en común. Entonces existe un elemento $u \in K^*$ tal que $b = ub'$ y $c = uc'$. Si consideramos la igualdad $ae + cd = 1$, entonces $ae + uc'd = 1$. Y tomando $d' = ud$ se tiene que $ae + c'd' = 1$. Además, $bd = ub'd = b'd'$. Por lo tanto, el valor de $\pi_a(x)$ tampoco depende de la elección de b y c. Y concluimos que la aplicación π_a está bien definida.
Veamos por último que π_a es una extensión de π_I, es decir, veamos que para todo elemento b de K, $\pi_a(b) = \pi_I(b)$. Sea $b \in K$, entonces lo podemos escribir como $b = b/c$ con $c = 1$. Luego tomando $d = 1$ y $e = 0$, se tiene que $cd + ae = 1$. Por lo tanto $\pi_a(b) = \pi_I(bd) = \pi_I(b)$. ■

Teorema 2.4.4 *Sea K un dominio de ideales principales, I un ideal propio no nulo de K y $a \in K$ un generador del ideal I. Entonces,*

1. *$ker(\pi_a) = a\Theta_a$.*

2. *π_a es un homomorfismo sobreyectivo de anillos de Θ_a en K/I, por lo tanto un isomorfismo de anillos entre $\Theta_a/a\Theta_a$ y K/I (un isomorfismo de cuerpos si I es maximal).*

3. *Si δ es una derivación de K y $\delta I \subset I$, entonces $\delta^* \circ \pi_a = \pi_a \circ \delta$ siendo δ^* la derivación inducida en K/I.*

Demostración:

1. Consideramos $x \in \Theta_a$ y escribimos $x = b/c$, donde $b, c \in K$ no tienen factores comunes. Veamos que se cumple la igualdad deseada comprobando ambas contenciones.

   - Sea $x \in a\Theta_a$, veamos que $x \in ker(\pi_a)$, es decir, comprobemos que $\pi_a(x) = 0$.
     Como $x \in a\Theta_a$, por la proposición 2.4.4 se tiene que $v_a(x) \geq 1$, es decir, $v_a(x) = v_a(b) - v_a(c) > 0$. Por lo tanto $v_a(b) > v_a(c) \geq 0$, luego $a|b$, es decir, $b \in I$ y en particular, $bd \in I$. Como consecuencia de esto último y por la definición de la aplicación valor en a se concluye que $\pi_a(x) = \pi_I(bd) = 0$, es decir, $x \in ker(\pi_a)$.
   - Supongamos ahora que $x \in ker(\pi_a)$ y veamos que $x \in a\Theta_a$. Como $x \in ker(\pi_a)$, entonces $\pi_I(bd) = \pi_a(x) = 0$. Por lo tanto, $bd \in I$. Luego, el elemento a divide a bd por ser a el generador del ideal I. Pero por ser $cd + ae = 1$, por la Identidad de Bezout se tiene que $mcd(a, d) = 1$. Luego $a \nmid d$ y por tanto, debe ocurrir que a divida a b. Así pues, $v_a(b) \geq 0$. Además, siguiendo este mismo razonamiento se tiene que $mcd(a, c) = 1$, luego a no divide a c y por tanto, $v_a(c) = 0$. Por lo que se concluye que $v_a(x) = v_a(b) - v_a(c) > 0$. Luego por la proposición 2.4.4, $x \in \Theta_a$.

2. Sabemos que por ser π_I la proyección canónica entonces es una aplicación sobreyectiva. Además, también sabemos que π_a una extensión de π_I. Luego π_a es una aplicación sobreyectiva. Además, $\pi_a(1) = \pi_I(1) = 1$, por el primer apartado de este teorema. Veamos que π_a es un homomorfismo de anillos:

Consideramos $x, x' \in \Theta_a$ de modo que $x = b/c$, $x' = b'/c'$ donde $b, c, b', c' \in K$, y ni b y c, ni b' y c' tienen factores comunes. Veamos que

$$\pi_a(xx') = \pi_a(x)\pi_a(x') \quad y \quad \pi_a(x + x') = \pi_a(x) + \pi_a(x').$$

- $xx' = b''/c''$, donde $b'', c'' \in D$ no tienen factores en común. Entonces, $bb' = gb''$ y $cc' = gc''$ siendo $g \in D$. Sean $d, e, d', e' \in D$, tal que $cd + ae = 1$ y $c'd' + ae' = 1$. Multiplicando estas dos últimas ecuaciones se tiene que

$$\begin{aligned}(cd + ae)(c'd' + ae') &= cc'dd' + cade' + aec'd' + aaee' = \\ &= cc'dd' + a(cde' + ec'd' + aee').\end{aligned}$$

  Luego si $h = cde' + ec'd' + aee'$ y teniendo en cuenta que $cc' = gc''$, se tiene que $c''(gdd') + ah = 1$. Teniendo en cuenta que π_I es un homomorfismo de anillos llegamos a

$$\begin{aligned}\pi_a(xx') = \pi_a\left(\frac{b''}{c''}\right) &= \pi_I(b''gdd') = \\ &= \pi_I(bb'dd') = \pi_I(bd)\pi_I(b'd') = \\ &= \pi_a(x)\pi_a(x').\end{aligned}$$

- Sea ahora $x + x' = b''/c''$ donde $b'', c'' \in K$ no tienen factores comunes. Entonces,

$$x + x' = \frac{b}{c} + \frac{b'}{c'} = \frac{bc' + b'c}{cc'} = \frac{b''}{c''}$$

  y por tanto $bc' + b'c = gb''$ y $cc' = gc''$ para algún $g \in K$. Sea $d, e, d', e' \in K$ tal que $cd + ae = 1$ y $c'd' + ae' = 1$. Del mismo modo que en el punto anterior, multiplicando entre sí ambas ecuaciones se llega a $c''(gdd') + ah = 1$ para un cierto $h \in K$. Luego, haciendo uso de la definición 2.4.6 y por ser π_I un homomorfismo de anillos se tiene que

$$\begin{aligned}\pi_a(x + x') = \pi_a\left(\frac{b''}{c''}\right) &= \pi_I(b''gdd') = \\ &= \pi_I((bc' + b'c)dd') = \\ &= \pi_I(bd)\pi_I(c'd') + \pi_I(b'd')\pi_I(cd) = \\ &= \pi_a(x)\pi_I(c'd') + \pi_a(x')\pi_I(cd).\end{aligned}$$

Como $a \in I$ y $1 = cd + ae$, entonces,

$$1 = \pi_I(1) = \pi_I(cd) + \pi_I(ae) = \pi_I(cd),$$

y de manera similar $\pi_I(c'd') = 1$. Luego $\pi_a(x+x') = \pi_a(x)+\pi_a(x')$.

Y queda probado que $\pi_a(x)$ es un homomorfismo de anillos sobreyectivo. Teniendo en cuenta esto último, y como $ker(\pi_a) = a\Theta_a$ por el primer apartado de este mismo teorema, entonces π_a es un isomorfismo de anillos entre $\Theta_a/a\Theta_a$ y K/I. Además, si I es un ideal maximal, entonces K/I es un cuerpo, y por tanto π_a será un isomorfismo de cuerpos.

3. Sea δ una derivación en K y supongamos que $\delta I \subset I$. Entonces, la derivación inducida δ^* en K/I satisface que $\delta^* \circ \pi_I = \pi_I \circ \delta$ por la proposición 2.1.3. Además, por la proposición 2.4.4 se tiene que $\delta\Theta_a \subset \Theta_a$, por lo que $\pi_a \circ \delta$ está definida en Θ_a. Sea $x = b/c \in \Theta_a$ donde $b, c \in K$ no tienen factores comunes. Entonces $mcd(a, c) = 1$ como se vio en el primer apartado de este mismo teorema. Por la identidad de Bezout, se cumple que $1 = ad + ce$ para algún $d, e \in K$. Luego,

$$1 = \pi_a(1) = \pi_a(a)\pi_a(d) + \pi_a(c)\pi_a(e) = \pi_a(c)\pi_a(e).$$

Por lo tanto, $\pi_a(c)$ es una unidad en K/I. Además, $b = cx$, luego $\pi_a(b) = \pi_a(cx) = \pi_a(c)\pi_a(x)$ y aplicando δ^* a esta igualdad llegamos a lo siguiente:

$$\delta^*\pi_a(b) = \delta^*(\pi_a(c)\pi_a(x)) = \pi_a(c)\delta^*(\pi_a(x)) + \pi_a(x)\delta^*(\pi_a(c)). \quad (2.4)$$

Por otro lado, si aplicamos la derivación δ a $b = cx$ entonces $\delta(b) = c\delta(x) + x\delta(c)$. Además, si a esto último se le aplica π_a tenemos que:

$$\pi_a(\delta(b)) = \pi_a(c)\pi_a(\delta(x)) + \pi_a(x)\pi_a(\delta(c)). \quad (2.5)$$

Pero

$$\pi_a(\delta(b)) = \pi_I(\delta(b)) = \delta^*(\pi_I(b)) = \delta^*(\pi_a(b))$$

y

$$\pi_a(\delta(c)) = \delta^*(\pi_a(c))$$

de manera similar. Luego la ecuación 2.5 se convierte en

$$\delta^*(\pi_a(b)) = \pi_a(c)\pi_a(\delta(x)) + \pi_a(x)\delta^*(\pi_a(c)). \quad (2.6)$$

Igualando 2.4 y 2.6, se tiene que

$$\pi_a(c)\delta^*(\pi_a(x)) = \pi_a(c)\pi_a(\delta(x)).$$

Por último, como $\pi_a(c)$ es invertible en K/I por ser un elemento unidad, llegamos a que $\delta^* \circ \pi_a = \pi_a \circ \delta$.

■

2.4.3. Residuos

En esta sección estudiaremos el concepto de residuo en polinomios normales. Se considera K un cuerpo diferencial de característica cero con derivada D y t un monomio sobre K.

Definición 2.4.7 *Consideramos $p \in K[t] \setminus K$ un polinomio normal y el conjunto*

$$R_p = \{f \in K(t) \quad tal \quad que \quad pf \in \Theta_p\}.$$

Se llama residuo en p a la aplicación

$$\begin{array}{rcl} res_p : R_p & \longrightarrow & K[t]/(p) \\ f & \to & res_p(f) = \pi_p\left(f\dfrac{p}{D(p)}\right) \end{array} \tag{2.7}$$

Teorema 2.4.5 *Sea $p \in K[t] \setminus K$ un polinomio normal. Entonces R_p es un espacio vectorial sobre K, $ker(res_p) = \Theta_p$ y res_p es un isomorfismo de $K-$espacios vectoriales entre R_p/Θ_p y $K[t]/(p)$.*

Demostración:

Veamos en primer lugar que R_p cumple las propiedades de ser un $K-$espacio vectorial. Como $0, p \in \Theta_p$, entonces $0, 1 \in R_p$. Sean $f, g \in R_p$ y $c \in K \subseteq \Theta_p$, veamos que $cf + g \in R_p$. Como $f, g \in R_p$, entonces $pf, pg \in \Theta_p$ y por ser Θ_p un anillo se tiene que $cpf + pg = p(cf + g) \in \Theta_p$. Luego $cf + g \in R_p$ y por lo tanto, R_p es $K-$ espacio vectorial.
Veamos ahora que $ker(res_p) = \Theta_p$, para ello veremos que se cumplen ambas contenciones. Supongamos que $f \in \Theta_p$. Sabemos que $1/D(p) \in \Theta_p$ ya que

dado $q \in K[t]$ cualquier factor irreducible de p se tiene que $q \nmid D(p)$ por ser p un polinomio normal, luego $1/D(p) \in \Theta_q$. Como esto es cierto para cualquier factor irreducible de p, se tiene que $1/D(p) \in \Theta_p$. Por lo tanto $f/D(p) \in \Theta_p$, luego $pf/D(p) \in p\Theta_p$ y en consecuencia $res_p(f) = \pi_p(pf/D(p)) = 0$ ya que vimos en el teorema 2.4.4 que $ker(\pi_p) = p\Theta_p$. Luego $\Theta_p \subsetneq Ker(res_p)$. Recíprocamente, sea $f \in Ker(res_p)$. Entonces, $res_p(f) = \pi_p(fp/D(p)) = 0$. Luego por el teorema 2.4.4, $fp/D(p) \in p\Theta_p$, es decir, $f/D(p) \in \Theta_p$. Luego $f \in \Theta_p$ ya que $D(p) \in \Theta_p$ y $f = fD(p)/D(p)$. Por lo tanto, queda probado que $\Theta_p = Ker(res_p)$.
Por último veamos que res_p es un isomorfismo de $K-$espacios vectoriales entre R_p/Θ_p y $K[t]/(p)$. Sabemos que π_p es un homomorfismo de anillos. Luego dados $f, g \in R_p$ y $c \in K$, se tiene que

$$\begin{aligned} res_p(cf+g) &= \pi_p\left(\frac{(cf+g)p}{D(p)}\right) = \\ &= \pi_p\left(\frac{cfp}{D(p)}\right) + \pi_p\left(\frac{gp}{D(p)}\right) = \\ &= \pi_p(c)\pi_p\left(f\frac{p}{D(p)}\right) + \pi_p\left(g\frac{p}{D(p)}\right) = \\ &= \pi_p(c)res_p(f) + res_p(g). \end{aligned}$$

Como $c \in K$, $\pi_p(c) = c$. Luego, $res_p(cf+g) = \cdot res_p(f) + res_p(g)$ en $K[t]/(p)$, quedando probado que res_p es un homomorfismo de $K-$ espacios vectoriales. Nos falta ver que es una biyección. Sabemos que π_p es una aplicación sobreyectiva por el teorema 2.4.4. Así que dado $w \in K[t]/(p)$, existe $g \in \Theta_p$ tal que $\pi_p(g) = w\pi_p(D(p))$. Consideramos ahora $f = g/p$, entonces $fp = g \in \Theta_p$, luego $f \in R_p$ y

$$res_p(f) = \pi_p\left(f\frac{p}{D(p)}\right) = \frac{\pi_p(g)}{\pi_p(D(p))} = \frac{\pi_p(fp)}{\pi_p(D(p))} = w.$$

Luego la aplicación res_p es sobreyectiva. Además, por ser $ker(res_p) = \Theta_p$ podemos concluir que res_p es un isomorfismo de $K-$espacios vectoriales entre R_p/Θ_p y $K[t]/(p)$. ■

Definición 2.4.8 *Se dice que $f \in k(t)$ es reducible con respecto a la derivación D si su denominador es especial con respecto a D.*

Se dice que f es simple con respecto a D si su denominador es normal con respecto a dicha derivación.

Teorema 2.4.6 *Sea $f \in K(t) \setminus \{0\}$ y $p \in K[t]$ un polinomio irreducible.*

1. *Si p es un polinomio normal, entonces se cumple que*

   - $v_p(D(f)) = v_p(f) - 1$ *si* $v_p(f) \neq 0$.
   - $v_p(D(f)) \geq 0$ *si* $v_p(f) = 0$.

   Además,

   $$\pi_p(p^{1-v_p(f)}D(f)) = v_p(f)\pi_p(p^{-v_p(f)}f)\pi_p(D(p)).$$

2. *Si p es un polinomio especial, entonces $v_p(D(f)) \geq v_p(f)$.*

3. *Si p es un polinomio especial de primer tipo y $v_p(f) \neq 0$, entonces $v_p(D(f)) = v_p(f)$.*

Demostración:

Sean $p \in K[t]$ un polinomio irreducible y $f \in K(t) \setminus \{0\}$ y denotamos $n = v_p(f)$. Dado $g = fp^{-n}$, por ser p irreducible, se tiene que $g \in \Theta_p$ por el quinto apartado de la proposición 2.4.4. Además, al aplicar la derivada D,

$$D(f) = D(gp^n) = p^n D(g) + gnp^{n-1}D(p). \tag{2.8}$$

Consideramos ahora $g = b/c$ donde $b, c \in K[t]$ y $mcd(b, c) = 1$. Como

$$v_p(g) = v_p(fp^{-n}) = v_p(f) + v_p(p^{-n}) = v_p(f) - nv_p(p) = n - n = 0,$$

entonces $v_p(g) = v_p(b) - v_p(c) = 0$, es decir, $v_p(b) = v_p(c)$. Pero no puede ocurrir que $v_p(b)$ y $v_p(c)$ sean no nulos al mismo tiempo, ya que sino b y c tendrían una potencia de p como divisor común, contradiciendo que $mcd(b, c) = 1$. Luego $v_p(b) = v_p(c) = 0$. Además, como

$$D(g) = \frac{cD(b) - bD(c)}{c^2},$$

entonces tenemos que

$$v_p(D(g)) = v_p(cD(b) - bD(c)) - v_p(c^2) = v_p(cD(b) - bD(c)).$$

Luego, por ser $cD(b) - bD(c) \in K[t]$, se tiene que $v_p(D(g)) \geq 0$.

Si $n = 0$, entonces $f = g$ y por tanto $D(f) = D(g) \in \Theta_p$. Luego $v_p(D(f)) = v_p(D(g)) \geq 0$ y

$$v_p(pD(f)) \geq v_p(p) + v_p(D(f)) > v_p(D(f)) \geq 0.$$

Es decir, $v_p(pD(f)) > 0$ y por tanto $pD(f) \in p\Theta_p = ker(\pi_p)$, por la proposición 2.4.4 y el teorema 2.4.4. Y se concluye que $\pi(pD(f)) = 0$. Todo lo anterior es cierto para cualquier polinomio, ya sea normal o especial, por lo que (1) y (2) quedan probados para el caso $n = 0$.

Supongamos ahora que $n \neq 0$:

1. Consideramos que p es un polinomio normal, es decir, $mcd(p, D(p)) = 1$ y por tanto, $v_p(D(p)) = 0$. Por ser p un polinomio irreducible por hipótesis, la última igualdad equivale a que $D(p) \in \Theta_p$, por la proposición 2.4.4. Además,

$$\begin{aligned} v_p(ngp^{n-1}D(p)) &= v_p(n) + v_p(g) + v_p(p^{n-1}) + v_p(D(p)) = \\ &= 0 + 0 + n - 1 + 0 = n - 1 < n \end{aligned}$$

y

$$v_p(p^n D(g)) = v_p(p^n) + v_p(D(g)) \geq n.$$

Luego

$$\begin{aligned} v_p(D(f)) &= v_p(p^n D(g) + gnp^{n-1}D(p)) = \\ &= min(v_p(p^n D(g)), v_p(gnp^{n-1}D(p))) = \\ &= n - 1 = v_p(f) - 1. \end{aligned}$$

Quedando probada la primera parte. Así que

$$v_p(p^{1-n}D(f)) \geq v_p(p^{1-n}) + v_p(D(f)) = 1 - n + n - 1 = 0,$$

es decir, $p^{1-n}D(f) \in \Theta_p$. Además, sabemos que $g, D(g), p, D(p) \in \Theta_p$ y que π_p es un homomorfismo de anillos,

$$\begin{aligned}\pi_p(p^{1-n}D(f)) &= \pi_p(pD(g)) + \pi_p(gnD(p)) = \\ &= \pi_p(p)\pi_p(D(g)) + n\pi_p(g)\pi_p(D(p)) = \\ &= n\pi_p(g)\pi_p(D(p)) = \\ &= n\pi_p(fp^{-n})\pi_p(D(p)) = \\ &= v_p(f)\pi_p(fp^{-v_p(f)})\pi_p(D(p)).\end{aligned}$$

2. Sea $p \in S$, y veamos que $v_p(D(f)) \geq v_p(f)$. Sabemos que

$$D(f) = p^n D(g) + gnp^{n-1}D(p),$$

luego

$$\begin{aligned}v_p(D(f)) &= v_p(p^n D(g) + gnp^{n-1}D(p)) \geq \\ &\geq min\left(v_p(p^n D(g)), v_p(gnp^{n-1}D(p))\right)\end{aligned}$$

Por definición $mcd(p, D(p)) = 1$, es decir, $p|D(p)$. Luego $v_p(D(p)) \geq 1$. Así que,

$$v_p(ngp^{n-1}D(p)) = v_p(g) + v_p(p^{n-1}) + v_p(D(p)) \geq n - 1 + 1 = n.$$

Además,

$$v_p(p^n D(g)) = v_p(p^n) + v_p(D(g)) = nv_p(p) + v_p(D(g)) \geq n.$$

Y por tanto, se concluye que $v_p(D(f)) \geq n = v_p(f)$.

3. Sea $p \in S_1$ y supongamos que $n \neq 0$. Comenzanos probando este apartado del teorema suponiendo que $p = t - \alpha$, $\alpha \in K$. Por definición de polinomio especial de primer tipo se tiene que $p_\alpha(\alpha)$ no es una derivada logarítmica de un $K-$radical, siendo

$$p_\alpha(\alpha) = \frac{D(t) - D(\alpha)}{t - \alpha} = \frac{D(p)}{p}.$$

Consideramos ahora $h = D(g) + np_\alpha g$. Como p es un polinomio especial de primer tipo, en particular es un polinomio especial, luego $mcd(p, D(p)) = p$, es decir, $p|D(p)$. Por lo tanto, $p_\alpha \in K[t]$. Además, como

$$v_p(p_\alpha) = v_p(D(p)/p) = v_p(D(p)) - v_p(p) \geq 1 - 1 = 0,$$

entonces $p_\alpha \in \Theta_p$. También sabemos que $g, D(g) \in \Theta_p$, así que $h \in \Theta_p$ y podemos aplicarle el homomorfismo π_p dando como resultado

$$\pi_p(h) = \pi_p(D(g) + np_\alpha g) = \pi_p(D(g)) + \pi_p(np_\alpha g).$$

Como $v_p(g)$ es nulo, entonces $g \notin p\Theta_p = ker(\pi_p)$, por la proposición 2.4.4. Luego, $\pi_p(g) \neq 0$. Supongamos que $\pi_p(h) = 0$, entonces usando que $I = (p)$ es un ideal diferencial de $K[t]$ y que, por la proposición 2.1.3, $D^* \circ \pi_p = \pi_p \circ D$, donde D^* es la derivación inducida en $K[t]/I$, se tiene que:

$$-np_\alpha = -n\pi_p(p_\alpha) = \frac{\pi_p(D(g))}{\pi_p(g)} = \frac{D^*(\pi_p(g))}{\pi_p(g)},$$

donde $\pi_p(g) \in K[t]/(t-\alpha)$. Pero $K[t]/(t-\alpha) \simeq K$ y D^* es una extensión de la derivación D, luego $\pi_p(g) \in K$ y $D(\pi_p(g)) = D^*(\pi_p(g))$. Todo esto implica que p_α es una derivada logarítmica de un $K-$radical, llegando a contradicción, ya que habíamos supuesto que p era especial de primer tipo. Así que $\pi_p(h) \neq 0$, es decir, $h \notin ker(\pi_p) = p\Theta_p$, luego $v_p(h) = 0$. Por lo tanto, como

$$\begin{aligned} D(f) &= ngp^{n-1}D(p) + p^n D(g) = \\ &= p^n(ngp^{-1}D(p) + D(g)) = \\ &= p^n(ngp_\alpha + D(g)) = p^n h, \end{aligned}$$

se tiene que

$$\begin{aligned} v_p(Df) &= v_p(p^n h) = v_p(p^n) + v_p(h) = \\ &= v_p(p^n) = nv_p(p) = n = v_p(f). \end{aligned}$$

Ahora supongamos que p es un polinomio arbitrario de grado m y consideremos $\bar{K}$ la clausura algebraica de K y $p = (t-\alpha_1)\dots(t-\alpha_m)$

la factorización del polinomio p en $\bar{K}$. t es un monomio en $\bar{K}$ y $t-\alpha_i \in S_{1,K\bar{(}t):\bar{K}}$, luego $p \in S_{1,K\bar{(}t):\bar{K}}$, ya que el producto finito de polinomios especiales es especial y si consideramos α una raíz de p en S, entonces es raíz de algún factor de p en S_1, luego $p_\alpha(\alpha)$ no es derivada logarítmica de un $\bar{K}(\alpha)-$radical. Luego $v_{t-\alpha_i}(f) = n$ para cada i, por lo tanto por la primera parte de este apartado $v_{t-\alpha_i}(D(f)) = n$. Luego $v_p(D(f)) = n$.

■

Proposición 2.4.6 *Sean $f \in K(t)$ y $p \in K[t]$ un polinomio irreducible y normal.*

1. *Si f es simple entonces $v_p(f) \geq -1$.*

2. *Se tiene que f es reducible con respecto a la derivación D si y sólo si, $v_p(f) \geq 0$.*

3. *El conjunto de todos los elementos reducibles de $K(t)$ con respecto a la derivación D es un subanillo diferencial de $K(t)$*

Demostración:

1. Sea $f \in K(t)$ y escribamos $f = a/b$ siendo $a, b \in K[t]$, $mcd(a, b) = 1$ y $b \neq 0$, y sea $p \in K[t]$ un polinomio irreducible y normal. Si f es simple entonces b es normal, es decir, $mcd(b, Db) = 1$. Luego b es un polinomio libre de cuadrados.

   - Si $p|b$ entonces $p \nmid a$, luego $v_p(f) = v_p(a) - v_p(b) = -v_p(b) \geq -1$ por ser b libre de cuadrados.
   - Si $p \nmid b$, entonces puede ocurrir que p divida a a o que no. Si ocurre lo primero, entonces $v_p(f) = v_p(a) \geq 0$. En caso contrario, $v_p(f) = 0$.

   Por tanto, se concluye que en cualquier caso $v_p(f) \geq -1$.

2. Consideramos de nuevo $f \in K(t)$ y escribimos $f = a/b$ siendo $a, b \in K[t]$, $mcd(a, b) = 1$ y $b \neq 0$. Sea $p \in K[t]$ un polinomio irreducible y normal. Veamos la primera implicación. Para ello supongamos que f es un polinomio reducible con respecto a D. Entonces b es especial. Luego $p \nmid b$, ya que de hacerlo, entonces p sería un polinomio especial contradiciendo que p es normal. Luego $v_p(b) = 0$ y $v_p(f) = v_p(a) \geq 0$. Recíprocamente, supongamos que $v_p(f) \geq 0$, y sea $p \in K[t]$ un factor irreducible y normal de b. Por ser p un factor de b, entonces $p \nmid a$, luego $v_p(f) = -v_p(b) < 0$, contradiciendo la hipótesis de que la función orden evaluada en f era positiva para cualquier polinomio irreducible y normal de $K[t]$. Por lo tanto, todos los factores irreducibles de b son especiales, luego b también lo es por ser su producto. Y queda probado que f es reducible con respecto a la derivación D.

3. El conjunto de todos los elementos reducibles de $K(t)$ con respecto a la derivación D es un conjunto no vacío, ya que $K[t]$ pertenece a dicho conjunto. Consideramos f, g reducibles con respecto a la derivación D y $p \in K[t]$ irreducible y normal. Por el apartado anterior, sabemos que $v_p(f) \geq 0$ y $v_p(g) \geq 0$. Luego $v_p(f - g) \geq min(v_p(f), v_p(-g)) \geq 0$ por ser $v_p(-g) = v_p(g) \geq 0$. Así que, de nuevo por el apartado anterior, $f - g$ es reducible. Además, $v_p(fg) = v_p(f) + v_p(g) \geq 0$, es decir, fg es reducible. Por lo tanto, el conjunto de todos los elementos reducibles de $K(t)$ con respecto a la derivación D es un subanillo de $K(t)$.
Veamos que es diferencial. Para ello vamos a probar que $D(f)$ pertenece a dicho conjunto, viendo que $v_p(D(f)) \geq 0$ y aplicando el apartado anterior. Si $v_p(f) > 0$ entonces por ser p normal podemos aplicar el teorema 2.4.6, obteniendo $v_p(D(f)) = v_p(f) - 1 \geq 0$. En otro caso, $v_p(D(f)) \geq 0$ de nuevo por el teorema 2.4.7. Luego se concluye que el conjunto de todos los elementos reducibles de $K(t)$ es un subanillo diferencial de $K(t)$.

■

Proposición 2.4.7 *Sea $f \in K(t) \setminus \{0\}$ y $p \in K[t]$ irreducible. Entonces,*

1. $v_p(Df/f) \geq -1$
2. *Se da la igualdad en (1) si y sólo sí, $v_p(f) \neq 0$ y p es normal.*

Demostración:

Sea $f \in K(t) \setminus \{0\}$ y $p \in K[t]$ irreducible. Denotamos $n = v_p(f)$ y $m = v_p(Df)$ para facilitar la demostración.

1. $v_p(D(f)/f) = m - n \geq -1$, ya que por la proposición 2.4.6 se tiene que $m = n - 1$ o $m \geq 0 = n$.

2. Supongamos que $v_p(D(f)/f) = -1$, entonces $m - n = -1$, es decir, $m = n - 1 < n$. En el teorema 2.4.6 vimos que $m \geq n$ si p es un polinomio especial, o si $n = 0$. Luego debe ser p un polinomio normal, y $v_p(f) \neq 0$.
   Recíprocamente, supongamos que $n \neq 0$ y p es un polinomio normal. Entonces por el teorema 2.4.6, $m = n - 1$, es decir, $v_p(D(f)/f) = -1$.

■

Capítulo 3

El teorema de Liouville

En este capítulo enunciaremos y demostraremos el teorema de Liouville. Pero antes daremos unos conceptos necesarios para ello. Consideramos k un cuerpo diferencial de característica cero y K una extensión de k. Denotamos d a la derivación en K.

Definición 3.0.1 *Se dice que $t \in K$ es una primitiva sobre k si $d(t) \in k$, es decir, si existe un elemento $a \in k$ tal que $d(t) = a$.*

Proposición 3.0.1 *Sea t una primitiva sobre k de modo que $d(t)$ no sea la derivada de ningún elemento de k, entonces $d(t)$ no es la derivada de ningún elemento de una extensión algebraica de k.*
Como consecuencia, t no puede ser algebraico sobre k, por lo que debe ser trascendente sobre k.

Demostración:
Sea $t \in K$ una primitiva sobre el cuerpo diferencial k, es decir, $a = d(t)$ para un cierto $a \in k$, y supongamos que a no es la derivada de ningún elemento de k. Vamos a razonar por reducción al absurdo, considerando una extensión algebraica E de k, y suponiendo que existe un $e \in E$ de modo que $d(e) = a$. Consideramos la aplicación traza $T : k(e) \to k$, y $T(e)/N \in k$, donde N es el grado de la extensión $[k(e) : k]$. Cabe observar que N es no nulo debido a que nos encontramos en un cuerpo de característica cero. Sabemos,

por la proposición 2.2.4, que las aplicaciones T y d conmutan. Luego

$$d\left(\frac{T(e)}{N}\right) = \frac{1}{N}d(T(e)) = \frac{1}{N}T(d(e)) = \frac{1}{N}T(a) = \frac{1}{N}\sum_{i=1}^{N} a = a,$$

contradiciendo que a no es derivada de ningún elemento de k. ■

Teorema 3.0.1

- *Si t es trascendente y es una primitiva sobre k, y se cumple que $ctes(k(t)) = ctes(k)$, entonces $d(t)$ no es la derivada de ningún elemento de k.*

- *Si t es una primitiva sobre k y $d(t)$ no es la derivada de ningún elemento de k, entonces t es un monomio sobre k, $ctes(k(t)) = ctes(k)$, y se cumple que $S = k$, siendo S el conjunto de todos los polinomios especiales.*

Demostración:

- Sea t transcendente y una primitiva sobre k y supongamos que $ctes(k(t)) = ctes(k)$. Vamos a razonar por reducción al absurdo, suponiendo que existe un elemento $b \in k$ tal que $d(t) = d(b)$. Entonces $d(t-b) = d(t) - d(b) = 0$, luego $t - b \in ctes(k(t)) = ctes(k)$. Por lo tanto, $t - b \in k$ siendo t un elemento trascendente sobre k, lo que es absurdo. Así pues, $d(t)$ no es la derivada de ningún elemento de k.

- Sea t una primitiva sobre k, es decir, existe $a \in k$ tal que $d(t) = a$. Consideramos $\bar{k}$ la clausura algebraica de k y supongamos que a no es la derivada de ningún elemento de k. Entonces, por la proposición 3.0.1, se tiene que $d(e) \neq a$, para cualquier $e \in \bar{k}$. Luego t debe ser trascendente y como $d(t) \in k$, se tiene que t es un monomio sobre k, por la definición 2.3.1.

  Veamos ahora que $S = k$. Por definición, $k \subseteq S$. Para ver la otra contención, vamos a razonar por reducción al absurdo. Supongamos que $p \in S \setminus k$ y consideremos $r \in \bar{k}$ una raiz del polinomio p. Entonces, $d(r) = d(t) = a$ por la proposición 2.3.3, lo que contradice que $d(e) \neq a$

para todo $e \in \bar{k}$. Luego $p \in k$ y, por tanto, queda probada la igualdad.

Veamos por último que $ctes(k) = ctes(k(t))$. Por ser $k(t)$ una extensión diferencial de k, se tiene que $ctes(k) \subseteq ctes(k(t))$. Para la otra contención, consideramos $c \in ctes(k(t))$. Entonces la proposición 2.3.4, se tiene que tanto el numerador como el denominador de c son especiales. Luego por ser $S = k$, ambos deben estar en k, es decir, $c \in k$. Quedando probada la igualdad y, por lo tanto, el teorema.

■

Definición 3.0.2 *Un elemento $t \in K^*$ es una hiperexponencial sobre k si $d(t)/t \in k$, es decir, si existe un elemento $a \in k$ de modo que $d(t)/t = a$.*

Teorema 3.0.2

- *Si t es trascendente y es una hiperexponencial sobre k, y $ctes(k(t)) = ctes(k)$, entonces $d(t)/t$ no es la derivada logarítmica de ningún radical sobre k.*
- *Si t es una hiperexponencial sobre k de modo que $d(t)/t$ no sea una derivada logarítmica de ningún radical de k, entonces t es un monomio sobre k y $ctes(k(t)) = ctes(k)$. Además, el conjunto formado por todos los polinomios especiales e irreducibles coincide con el conjunto formado por los polinomios especiales de primer tipo e irreducibles. Además, estos conjuntos están formados únicamente por t.*

Demostración:

- Sea t transcendente y una hiperexponencial sobre k y supongamos que $ctes(k(t)) = ctes(k)$. Vamos a razonar por reducción al absurdo, suponiendo que existe un elemento $b \in k^*$ y un entero e no nulo tal que $nd(t)/t = d(b)/b$. Entonces

$$d\left(\frac{t^e}{b}\right) = \frac{et^{e-1}d(t)}{b} - \frac{t^e d(b)}{b^2} = \frac{t^{e-1}}{b}\left(ed(t) - t\frac{d(b)}{b}\right) = 0.$$

Luego $\frac{t^e}{b} \in ctes(k(t)) = ctes(k)$. Por lo tanto, $\frac{t^e}{b} \in k$ siendo t un elemento trascendente sobre k, lo que es absurdo. Así pues, $d(t)/t$ no es la derivada logarítmica de ningún radical de k.

- Sea t una hiperexponencial sobre k y supongamos que $a = d(t)/t$ no es la derivada de ningún radical de k. Entonces, a no es la derivada de ningún radical sobre la clausura algebraica de k, por la proposición 2.3.5. Por lo tanto t debe ser trascendente y como $d(t) = at \in k[t]$, se tiene que t es un monomio sobre k.
  Sea $p = bt^m$ donde $b \in k$ y $m \geq 0$. Entonces

$$\begin{aligned} d(p) &= t^m db + bmt^{m-1}d(t) = \\ &= t^m(d(b) + bmd(t)/t) = \\ &= t^m(d(m) + bma). \end{aligned}$$

  Luego $p|d(p)$, es decir, $mcd(p, d(p)) = p$. Por lo tanto, p es un polinomio especial. Sea ahora $p \in S^{Irr}$ y supongamos que p tiene una raíz no nula $r \in \bar{k}^*$. Entonces, $d(r)/r = d(t)/t = a$ por la proposición 2.3.3. Esto contradice que a no es la derivada de ningún radical sobre la clausura algebraica de k. Por lo que la única raíz de p en $\bar{k}$ es el 0. Luego debe ser $p = t$, para ser especial, mónico e irreducible.
  Por definición se tiene que $S_1^{Irr} \subseteq S^{Irr}$. Veamos que se cumple la otra contención. Sea $p \in S^{Irr}$. Entonces $p = t$ siendo $r = 0$ la única raíz de p en k. Tenemos que $p_r = p_0 = d(t)/t = a$, que no es la derivada logarítmica de ningún radical sobre k, por hipótesis. Luego $p \in S_1^{Irr}$. Por lo que se tiene la igualdad deseada.
  Por último, veamos que $ctes(k(t)) = ctes(k)$. Por ser $k(t)$ una extensión diferencial de k, se tiene que $ctes(k) \subseteq ctes(k(t))$. Veamos ahora la otra contención. Sea $c \in ctes(k(t))$. Entonces la proposición 2.3.4, se tiene que tanto el numerador como el denominador de c son especiales. Luego, $c = bt^q$, donde $b \in k$ y q es un número entero. Supongamos que tanto b como q son no nulos. Entonces,

$$0 = d(c) = d(b)t^q + bqt^{q-1}d(t) = (d(b) + abq)t^m.$$

  Luego $d(b)/b = qa$. Por lo tanto, a es la derivada logarítmica de un radical sobre k, contradiciendo nuestra hipótesis. Luego, debe ocurrir que $b = 0$ o $q = 0$, y por lo tanto, $c \in k$. Por consiguiente, $ctes(k(t)) \subseteq ctes(k)$.

■

Definición 3.0.3 *Se dice que un elemento $t \in K$ es de Liouville sobre k si es algebraico, o una primitiva o una hiperexponencial sobre k.*
Si t es de Liouville sobre k, trascendente y $ctes(k(t)) = ctes(k)$, se dice que t es un monomio de Liouville.

Proposición 3.0.2 *Sea t un monomio de Liouville sobre k y $f \in k(t)$ tal que $d(f) \neq 0$. Escribimos $f = p/q$ con $p, q \in k[t]$ y siendo q mónico.*

- *Si $v_\infty(f) = 0$ entonces, $v_\infty(d(f)) \geq 0$.*
- *Si $v_\infty(f) \neq 0$ entonces,*

$$v_\infty(d(f)) = \begin{cases} v_\infty(f) & si \quad d(t)/t \in k \quad y \quad d(l(p)) \neq 0. \\ v_\infty(f) + 1 & si \quad dt \in k \quad y \quad d(l(p)) = 0. \end{cases}$$

Demostración:
El primer punto es consecuencia del teorema 2.4.3. Supongamos por tanto que $v_\infty \neq 0$, entonces $v_\infty = m - n \neq 0$, siendo $m = gr(q)$ y $n = gr(p)$. Veamos cual es el valor de $v_\infty(d(f))$. Por ser $f = p/q$ se tiene que

$$d(f) = d\left(\frac{x}{y}\right) = \frac{qd(p) - pd(q)}{q^2}.$$

Luego

$$\begin{aligned} v_\infty(d(f)) &= gr(q^2) - gr(qd(p) - pd(q)) = \\ &= 2gr(q) - gr(qd(p) - pd(q)) = \\ &= 2m - gr(qd(p) - pd(q)). \end{aligned}$$

Supongamos ahora que p y q son dos polinomios de la forma $p = bt^n + r$ y $q = t^m + s$, donde $b \in k^*$ es el coeficiente lider del polinomio p y $r, s \in k[t]$ de modo que $gr(r) < n$ y $gr(s) < m$. Y diferenciamos dos casos:

- Si t es una hiperexponencial, entonces $dt/t = a \in k$. Así que,

$$d(p) = d(b)t^n + bnt^{n-1}d(t) + d(r) = d(b)t^n + bnt^n a + d(r)$$

y

$$d(q) = mt^{m-1}d(t) + ds = mt^m a + d(s).$$

Luego,

$$\begin{aligned} & qd(p) - pd(q) = \\ & = (t^m + s)(d(b)t^n + bnt^n a + d(r)) - (bt^n + r)(mt^m a + d(s)) = \\ & = d(b)t^{m+n} + bnat^{m+n} + t^m d(r) + s(d(b)t^n + bnt^n a + d(r)) - \\ & \quad - bmat^{m+n} - bt^n d(s) - r(mt^m a + d(s)) = \\ & = (d(b) + bna - bma)t^{m+n} + t^m d(r) + sd(p) - bt^n d(s) - rd(q). \end{aligned}$$

Además,

$$\begin{aligned} gr(d(s)) &\leq gr(s) + max(0, \delta(t) - 1) < m, \\ gr(d(r)) &\leq gr(r) + max(0, \delta(t) - 1) < n, \\ gr(d(p)) &\leq gr(p) + max(0, \delta(t) - 1) = n \end{aligned}$$

y

$$gr(d(q)) \leq gr(q) + max(0, \delta(t) - 1) = m.$$

Luego los términos $t^m d(r)$, $sd(p)$, $bt^n d(s)$ y $rd(q)$ tienen grado estrictamente menor que $m+n$. Así que, si probamos que $d(b)+bna-bma \neq 0$ entonces se tendrá que $gr(qd(p) - pd(q)) = m + n$. Pero por ser t una hiperexponencial,

$$d(b) + bna - bma = d(b) + ba(n - m) = d(bt^{n-m}).$$

Además, $n \neq m$ y $b \neq 0$, luego $bt^{n-m} \notin k$ y como $ctes(k(t)) = ctes(k)$ por ser t un polinomio de Liouville, se tiene que $d(bt^{n-m}) \neq 0$. Por lo tanto, se concluye que

$$v_\infty(df) = 2m - m - n = m - n = v_\infty(f).$$

- Si t es una primitiva, entonces $d(t) = a \in k$. Así que,

$$d(p) = d(b)t^n + bnt^{n-1}d(t) + d(r) = d(b)t^n + bnt^{n-1}a + d(r)$$

y

$$d(q) = mt^{m-1}d(t) + d(s) = mt^{m-1}a + d(s).$$

Por lo tanto, se cumple que $gr(d(q)) < m$ por ser

$$gr(d(s)) \leq gr(s) + max(0, \delta(t) - 1) < m.$$

Ahora separamos la demostración en dos casos, distinguiendo si $d(b)$ es nulo o no.

- Si $d(b) \neq 0$, entonces como $gr(d(r)) \leq gr(r)+max(0,\delta(t)-1) < n$ se tiene que $gr(d(p)) = n$. Luego

$$gr(qd(p)) = gr(q) + gr(d(p)) = m + n$$

y

$$gr(pd(q)) = gr(p) + gr(d(q)) < n + m.$$

Por lo tanto, se concluye que

$$\begin{aligned} v_\infty &= 2m - gr(qd(p) - pd(q)) = 2m - (m+n) = \\ &= m - n = gr(q) - gr(p) = v_\infty(f). \end{aligned}$$

- Consideramos ahora el caso en el que $d(b) = 0$, y consideramos s y r de la forma $s = \alpha t^{m-1} + u$ y $r = \beta t^{n-1} + v$, siendo $u, v \in K[t]$ con $gr(u) < m-1$ y $gr(v) < n-1$, y $\alpha, \beta \in k$. Luego

$$d(s) = d(\alpha)t^{m-1} + \alpha(m-1)t^{m-2} + d(u)$$

y

$$d(r) = d(\beta)t^{n-1} + \beta(n-1)t^{n-2} + d(v).$$

Así que, desarrollando únicamente los coeficientes de los términos de mayor grado para reducir la dificultad, se tiene que

$$\begin{aligned} &qd(p) - pd(q) \\ &= (t^m + s)(bnt^{n-1}a + d(r)) - (bt^n + r)(mt^{m-1}a + d(s)) = \\ &= (t^m + \alpha t^{m-1} + u)\left(bnt^{n-1}a + d(\beta)t^{n-1} + \beta(n-1)t^{n-2} + d(v)\right) - \\ &- (bt^n + \beta t^{n-1} + v)(mt^{m-1}a + d(\alpha)t^{m-1} + \alpha(m-1)t^{m-2} + d(u)) = \\ &= (bna + d(\beta))t^{m+n-1} + \beta(n-1)t^{m+n-2} + d(v)t^m + \\ &\quad + (\alpha t^{m-1} + u)d(p) - (bma + bd(\alpha))t^{m+n-1} - \\ &\quad - b\alpha(m-1)t^{m+n-2} - bd(u)t^n - (\beta t^{n-1} + v)d(q) = \\ &= (ba(n-m) + d(\beta) - bd(\alpha))t^{m+n-1} + \\ &\quad + (\beta(n-1) - b\alpha(m-1))t^{m+n-2} + \\ &\quad + d(v)t^m + (\alpha t^{m-1} + u)d(p) - bd(u)t^n - (\beta t^{n-1} + v)d(q). \end{aligned}$$

Sabemos que

$$gr(d(v)) \leq gr(v) + max(0, \delta(t) - 1) < n - 1$$

y

$$gr(d(u)) \leq gr(u) + max(0, \delta(t) - 1) < m - 1.$$

Además, por ser $db = 0$, se tiene que $gr(d(p)) < n$. Por lo tanto, $d(v)t^m$, $(\alpha t^{m-1} + u)d(p)$, $bd(u)t^n$ y $(\beta t^{n-1} + v)d(q)$ tienen grado menor estrictamente que $m + n - 1$. Así que, si probamos que el coeficiente que acompaña a t^{m+n-1} es no nulo, entonces $gr(qd(p) - pd(q)) = m+n-1$. Es decir, veamos que $ba(n-m)+d(\beta)-bd(\alpha)$ es distinto de cero. Pero como

$$ba(n-m) + d(\beta) - bd(\alpha) = d\left(bt(n-m) + \beta - b\alpha\right),$$

por ser $d(t) = a$ y $d(b) = 0$, basta ver que

$$d\left(bt(n-m) + \beta - b\alpha\right) \neq 0.$$

Sabemos que $n \neq m$ y $b \neq 0$, entonces $bt(n-m) + \beta - b\alpha \notin k$ y como $ctes(k(t)) = ctes(k)$ por ser t un monomio de Liouville, se tiene que $d\left(bt(n-m) + \beta - b\alpha\right) \neq 0$. Concluimos entonces que

$$v_\infty(d(f)) = 2m - m + n - 1 = m + n - 1 = v_\infty(f) - 1.$$

■

3.1. Teorema de Liouville

Definición 3.1.1 *Se dice que $t \in K$ es un logaritmo sobre k si existe un elemento $a \in k^*$ tal que $d(t) = d(a)/a$. Un elemento $t \in K^*$ es una exponencial sobre el cuerpo k si $d(t)/t = d(a)$ para un cierto $a \in k$.*

Definición 3.1.2 *Se dice que $t \in K$ es elemental sobre k si t es un elemento algebraico, o un logarítmo o una exponencial.*
La extensión K del cuerpo k es elemental si existen $t_1, \ldots, t_n$ tal que $K = k(t_1, \ldots, t_n)$ y t_i es elemental en $k(t_1, \ldots, t_{i-1})$ para $i \in \{1, \ldots, n\}$.

Teorema 3.1.1 *(Teorema de Liouville) Sea K un cuerpo diferencial y $f \in K$. Si existe una extensión elemental E de K de manera que todos los elementos constantes de E sean los mismos que los de K, y un elemento $g \in E$ tal que $d(g) = f$, entonces existen $v \in K$, $u_1, ..., u_n \in K^*$ y $c_1, ..., c_n$ elementos constantes de K tal que*

$$f = d(v) + \sum_{i=1}^{n} c_i \frac{du_i}{u_i}.$$

Obsérvese la similitud con el enunciado de la reducción de Hermite.

Demostración:

Supongamos que se cumplen las hipótesis del enunciado. Sean C el conjunto de todos los elementos constantes de K y E una extensión elemental de K con los mismos elementos constantes que este último y $g \in E$ tal que $d(g) = f$. Entonces existen $t_1, ..., t_m \in E$ tal que $E = K(t_1, ..., t_m)$ y cada t_i es elemental sobre $K(t_1, ...t_{i-1})$. Vamos a probar el teorema por inducción en m. Para $m = 0$, se tiene que $E = K$, luego tomando $v = g \in K$ se tiene que $f = d(v)$, que es de la forma deseada. Ahora dado m>0 supongamos que el teorema es cierto para cualquier extensión elemental generada por $m - 1$ elementos, y veamos que dadas las hipótesis del enunciado, existe una una extensión E de K, generada por m elementos que cumple el teorema. Sea $t = t_1$ y $F = K(t)$. Entonces como $K \subseteq F \subseteq E$, se tiene que los elementos constantes de F coinciden exactamente con los de K, es decir, $ctes(F) = ctes(K) = C$, ya que $C \subseteq ctes(F) \subseteq ctes(E) = C$. Además, $f \in F$ y $E = F(t_2, .., t_m)$ es una extensión elemental de F generada por $m - 1$ elementos, luego por hipótesis de inducción, existen $v \in F$, $u_1, ..., u_n \in F^*$ y $c_1, ..., c_n \in C$ tal que

$$f = d(v) + \sum_{i=1}^{n} c_i \frac{d(u_i)}{u_i}. \tag{3.1}$$

Continuamos la demostración del teorema diferenciando si t es un elemento algebraico o trascendente sobre K.

- Si t es algebraico sobre K:
  Consideramos las aplicaciones traza, $T : F \to K$, y norma, $N : F \to K$, y sea $m = [F : K]$ el grado de la extensión F sobre K o dimensión del

K-espacio vectorial F. Aplicando la primera aplicación a la ecuación 3.1, se tiene que:

$$T(f) = T\left(d(v) + \sum_{i=1}^{n} c_i \frac{d(u_i)}{u_i}\right) = T(d(v)) + \sum_{i=1}^{n} c_i T\left(\frac{d(u_i)}{u_i}\right)$$

ya que la traza es una aplicación lineal y las $c_i's$ son constantes en K. Como $f \in K$, $T(f) = mf$. Además, por la proposición 2.2.4,

$$T(d(v)) = d(T(v)),$$

es decir, T conmuta con d. En esa misma proposición también vimos que

$$T\left(\frac{d(u_i)}{u_i}\right) = \frac{d(N(u_i))}{N(u_i)}.$$

Luego

$$mf = T(f) = d(T(v)) + \sum_{i=1}^{n} c_i \frac{d(N(u_i))}{N(u_i)}.$$

Por lo tanto, si tomamos $w = T(v)/m \in K$ y $w_i = N(u_i) \in K^*$ tenemos la igualdad deseada,

$$f = d(w) + \sum_{i=1}^{n} \frac{c_i}{m} \frac{d(w_i)}{w_i}.$$

- Si t es trascendente sobre K, entonces como $ctes(F) = C$, t es un monomio de Liouville sobre K, como consecuencia de los teoremas 3.0.1 y 3.0.2. Consideramos un polinomio $p \in K[t]$ irreducible y normal. Por la proposición 2.4.7, se tiene que $v_p(d(u_i)/u_i) \geq -1$, por lo que

$$v_p\left(\sum_{i=1}^{n} c_i \frac{d(u_i)}{u_i}\right) = min\left(v_p\left(\frac{d(u_i)}{u_i}\right)/i = 1, \ldots, n\right) \geq -1.$$

Veamos ahora que $v_p(v) \geq 0$. Razonamos por reducción al absurdo, suponiendo que $v_p(v) < 0$. Entonces, por el teorema 2.4.6, $v_p(d(v)) = v_p(v) - 1 < -1$. Por lo tanto,

$$v_p(f) = v_p\left(d(v) + \sum_{i=1}^{n} c_i \frac{d(u_i)}{u_i}\right) = min(v_p(d(v)), -1) < -1.$$

Esto último contradice que $f \in K$, ya que si se cumple esto último, entonces $v_p(f) \geq 0$. Así que, $v_p(v) \geq 0$, y como esto es cierto para todo polinomio $p \in K[t]$ irreducible y normal, entonces v es reducible en F por la proposición 2.4.6. Consideramos ahora $u_i = w_i \prod_{j=1}^{n_i} p_{ij}^{e_{ij}}$, donde $w_i \in K^*$, todos e_{ij} son enteros y cada $p_{ij} \in K[t]$ es mónico e irreducible. Entonces,

$$\begin{aligned}
f &= d(v) + \sum_{i=1}^{n} c_i \frac{d(u_i)}{u_i} = d(v) + \sum_{i=1}^{n} c_i \frac{d\left(w_i \prod_{j=1}^{n_i} p_{ij}^{e_{ij}}\right)}{w_i \prod_{j=1}^{n_i} p_{ij}^{e_{ij}}} = \\
&= d(v) + \sum_{i=1}^{n} c_i \frac{d(w_i) \prod_{j=1}^{n_i} p_{ij}^{e_{ij}} + w_i d\left(\prod_{j=1}^{n_i} p_{ij}^{e_{ij}}\right)}{w_i \prod_{j=1}^{n_i} p_{ij}^{e_{ij}}} = \\
&= d(v) + \sum_{i=1}^{n} c_i \frac{d(w_i)}{w_i} + \sum_{i=1}^{n} c_i \frac{d\left(\prod_{j=1}^{n_i} p_{ij}^{e_{ij}}\right)}{\prod_{j=1}^{n_i} p_{ij}^{e_{ij}}} = \\
&= d(v) + \sum_{i=1}^{n} c_i \frac{d(w_i)}{w_i} + \\
&+ \sum_{i=1}^{n} c_i \left(\frac{e_{i1} p_{i1}^{e_{i1}-1} d(p_{i1}) \prod_{j=2}^{n_i} p_{ij}^{e_{ij}}}{\prod_{j=1}^{n_i} p_{ij}^{e_{ij}}} + \ldots + \frac{e_{in_i} p_{in_i}^{e_{in_i}-1} d(p_{in_i}) \prod_{j=1}^{n_i-1} p_{ij}^{e_{ij}}}{\prod_{j=1}^{n_i} p_{ij}^{e_{ij}}} \right) = \\
&= d(v) + \sum_{i=1}^{n} c_i \frac{d(w_i)}{w_i} + \sum_{i=1}^{n} c_i \left(\frac{e_{i1} d(p_{i1})}{p_{i1}} + \ldots + \frac{e_{in_i} d(p_{in_i})}{p_{in_i}} \right).
\end{aligned}$$

Si alguno de los polinomios $p_{i1}, \ldots, p_{in_i}$ está repetido, teniendo en cuenta que $e_{i1}, \ldots, e_{in_i}$ son enteros, podemos sacar factor común, y podemos suponer que todos los polinomios q_j del segundo sumatorio son diferentes. Así, obtenemos la expresión

$$f = d(v) + \sum_{i=1}^{n} c_i \frac{d(w_i)}{w_i} + \sum_{j=1}^{N} b_j \frac{d(q_j)}{q_j},$$

donde $b_j \in C$ y $q_j \in K[t]$ son mónicos, irreducibles y coprimos, para todo $j = 1, \ldots, N$.
Supongamos ahora que existe un q_j de los anteriores que es normal, digamos q_J. Se tiene que $v_{q_J}(q_J) = 1$, y por ser todos $q_j's$ coprimos, $v_{q_J}(q_j) = 0$ para todo $j \neq J$. Luego

$$v_{q_J}(b_J d(q_J)/q_J) = v_{q_J}(d(q_J)) - v_{q_J}(q_J) = -1$$

por ser q_J normal, y

$$v_{q_J}(b_j d(q_j)/q_j) = v_{q_J}(d(q_j)) - v_{q_J}(q_j) \geq 0.$$

Por lo tanto, $v_{q_J}(\sum_{j\neq J} b_j d(q_j)/q_j) \geq 0$, y $v_{q_J}(\sum_{j=1}^{N} b_j \frac{d(q_j)}{q_j}) = -1$. Pero q_J es un polinomio normal y $d(v)$ es reducible en $K(t)$, por ser v reducible en $K(t)$ y el conjunto de todos los elementos reducibles de $K(t)$ un subanillo diferencial por la proposición 2.4.6, por lo que $v_{q_J}(d(v)) \geq 0$. Así que,

$$v_{q_J}(f) = min\left(dv, \sum_{i=1}^{n} c_i \frac{d(w_i)}{w_i}, \sum_{j=1}^{N} b_j \frac{d(q_j)}{q_j}\right) = -1,$$

contradiciendo que $f \in K$. Luego todos los polinomios q_j son especiales. A partir de ahora vamos a separar la demostración en dos casos, diferenciando si t es exponencial o logarítmica:

- Si t es una exponencial sobre K, entonces $d(t)/t = d(a)$ para algún $a \in K$. Además, por el teorema 3.0.2, t es el único polinomio irreducible que es especial, luego debe ocurrir que $N = 1$ y $q_1 = t$. Por lo tanto, $b_1 d(q_1)/q_1 = b_1 d(t)/t = b_1 d(a)$. Luego

  $$f = d(v) + \sum_{i=1}^{n} c_i \frac{d(w_i)}{w_i} + b_1 d(a) = d(v + b_1 a) + \sum_{i=1}^{n} c_i \frac{d(w_i)}{w_i},$$

  donde $v + b_1 a$ es reducible en $K(t)$. Supongamos que $v_t(v + b_1 a) < 0$, entonces

  $$v_t(d(v + b_1 a)) = v_t(v + b_1 a) < 0,$$

  por el teorema 2.4.6, ya que t es un polinomio especial, mónico e irreducible. Luego $v_t(f) < 0$, contradiciendo que $f \in K$. Luego $v_t(v + b_1 a) \geq 0$ y por tanto, $v + b_1 a \in K[t]$. Además, como $d(t)/t \in K$, se tiene que $v_\infty(d(v + b_1 a)) = v_\infty(v + b_1 a)$, por la proposición 3.0.2. Por lo tanto, $gr(d(v + b_1 a)) = gr(v + b_1 a)$. Luego como

  $$f = d(v + b_1 a) + \sum_{i=1}^{n} c_i \frac{d(w_i)}{w_i} \in K,$$

  entonces $gr(v + b_1 a) = 0$. Así que, concluimos que $v + b_1 a \in K$ y

  $$f = d(v + b_1 a) + \sum_{i=1}^{n} c_i \frac{d(w_i)}{w_i} \in K,$$

  que es de la forma deseada.

- Si t es un logaritmo sobre K, entonces $d(t) = d(a)/a$ para algún $a \in K^*$. Además, por el teorema 3.0.1, todo polinomio irreducible es normal. Luego por ser todos los polinomios q_j irreducibles y especiales, debe ocurrir que $N = 0$. Así que,

$$f = d(v) + \sum_{i=1}^{n} c_i \frac{d(w_i)}{w_i},$$

es decir,

$$d(v) = f - \sum_{i=1}^{n} c_i \frac{d(w_i)}{w_i} \in K.$$

Por lo tanto, $v_\infty(dv) = 0$ y por la proposición 3.0.2, como $d(t) \in K$ entonces debe ser $v = mt + l$ donde $m, l \in K$ y $d(m) = 0$. Así pues, concluimos que

$$f = d(v) + \sum_{i=1}^{n} c_i \frac{d(w_i)}{w_i} = d(m)t + d(t)m + d(l) + \sum_{i=1}^{n} c_i \frac{d(w_i)}{w_i} =$$
$$= \frac{da}{a} m + d(l) + \sum_{i=1}^{n} c_i \frac{d(w_i)}{w_i},$$

que es de la forma deseada.

■

3.1.1. Ejemplo de aplicación del teorema de Liouville

Sean $f(z)$ y $g(z)$ dos funciones en $\mathbb{C}(z)$ de modo que $g(z)$ no es una función constante. Denotamos $K = \mathbb{C}(z)$. Veamos que la condición necesaria y suficiente que deben cumplir dichas funciones para que la solución de la integral

$$\int f(z) e^{g(z)}$$

venga dada en términos de funciones elementales es que $f = d(a) + ad(g)$, siendo $a \in \mathbb{C}(z)$.
Supongamos que $\int f(z)e^{g(z)}$ es elemental, y consideramos $t = e^{g(z)}$ de modo que $d(t)/t = d(g)$. Entonces, por definición, t es una exponencial. En

particular, t es una hiperexponencial. Para aplicar el teorema de Liouville a nuestra función, necesitamos que $ctes(K(t)) = ctes(K)$ y que t sea trascendente. Para ello, vamos a probar que $d(t)/t$ no es la derivada logarítmica de ningún $K-$radical. Una vez probado esto, estaremos en condiciones de aplicar el teorema 3.0.2, del que obtendremos que t es un monomio sobre K y que $ctes(K(t)) = ctes(K)$. Además, por definición de monomio sobre K, tendremos que t es trascendente. Por lo tanto, veamos que dt/t no es la derivada logarítmica de ningún radical sobre K, es decir, que no existe ningún $h(z) \in \mathbb{C}$ y ningún entero n tal que

$$nd(g) = n\frac{d(t)}{t} = \frac{d(h)}{h}. \tag{3.2}$$

Vamos a razonar por reducción al absurdo, suponiendo que existen un elemento $h \in \mathbb{C}(z)$ y un entero no nulo n de modo que se cumpla la igualdad 3.2.

- Si $h(z) \in \mathbb{C}$, entonces $\frac{d(h)}{h} = 0$. Hemos llegado a un absurdo, ya que $g(z)$ no es una función constante, luego su derivada no puede ser nula.

- Sea $h(z) \notin \mathbb{C}$. Entonces, $\frac{d(h)}{h} \in \mathbb{C}(z)$. Consideramos z_0 un polo de $d(h(z))/h(z)$. Este es de orden uno, por la forma en la que viene definida la función. Entonces, por ser

  $$nd(g) = n\frac{d(t)}{t} = \frac{d(h)}{h},$$

  z_0 debe ser un polo de $d(g(z))$ del mismo orden. Pero, como vamos a ver a continuación, todos los polos de $d(g(z))$ tienen orden 0 o mayor o igual que 2. Vamos a probarlo, separando en dos casos, dependiendo de si z_0 es un polo o no, de $g(z)$:

  - Si z_0 no es un polo de $g(z)$, entonces

    $$g(z) = g_0 + g_1(z - z_0) + g_2(z - z_0)^2 + \dots.$$

    Luego,

    $$d(g(z)) = g_1 + 2g_2(z - z_0) + \dots,$$

    es decir, $d(g(z))$ no tiene polo en z_0.

- Si z_0 es un polo de $g(z)$ de orden $k \geq 1$, entonces z_0 es un polo de $d(g(z))$ de orden $k+1$. Y por el punto anterior, llegamos a un absurdo.

Por lo tanto, todos los polos de $g(z)$ tienen orden nulo, o mayor o igual que 2. Pero todos los polos de $d(h(z))/h(z)$ tienen orden 1. Luego no puede darse la igualdad 3.2.

Por lo tanto $d(g(z))$ no es la derivada logarítmica de ningún $K-$radical. Luego, aplicando el teorema 3.0.2, se tiene que t es un monomio sobre K y que $ctes(K(t)) = ctes(K)$.
Ahora, podemos aplicar la demostración del teorema de Liouville, en el caso en el que t es trascendente y exponencial, este teorema nos dice que podemos expresar la función $f(z)e^g(z)$ de la siguiente forma:

$$f(z)t = d(v) + b\frac{d(t)}{t} + \sum_{i=1}^{n} c_i \frac{d(w_i)}{w_i},$$

donde $b \in ctes(K)$, $v \in K(t)$ y cada $w_i \in K$. Luego,

$$d(v) = f(z)t - b\frac{d(t)}{t} - \sum_{i=1}^{n} c_i \frac{d(w_i)}{w_i}. \tag{3.3}$$

Además, por ser $v \in K(t)$, utilizando la descomposición en fracciones simples, es de la forma

$$v = A(t) + \sum_{l=1}^{n_l} \frac{A_l(t)}{q_k^l(t)} = \sum_{j=1}^{m} b_j t^j + \sum_{l=1}^{n_l} \frac{A_l(t)}{q_k^l(t)}, \tag{3.4}$$

siendo $A(t) \in K$ y todos los $A_l(t) \in K[t]$,$q_k(t) \in K[t]$ mónicos, irreducibles y coprimos dos a dos, y $gr(A_l(t)) < gr(q_k^l(t))$. Luego

$$dv = \sum_{j=0}^{m} (d(b_j) + jb_j d(g))t^j + \sum_{l=1}^{n_l} d\left(\frac{A_l(t)}{q_k^l(t)}\right). \tag{3.5}$$

Probemos ahora que en la expresión 3.4 el único polinomio $q_k(t)$ que aparece es el polinomio t. Supongamos que $q_k(t) \neq t$. Por lo tanto, por el teorema 3.0.2, $q_k(t)$ es normal.

Aplicando el teorema 2.4.6, se tiene que

$$\text{si } k' \neq k, \quad v_{q_k(t)}\left(\frac{A_l(t)}{q^l_{k'}(t)}\right) \geq 0 \Rightarrow v_{q_k(t)}\left(d\left(\frac{A_l(t)}{q^l_{k'}(t)}\right)\right) \geq 0.$$

$$\text{si } k' = k, \quad v_{q_k(t)}\left(\frac{A_l(t)}{q^l_{k'}(t)}\right) = -l < 0 \Rightarrow v_{q_k(t)}\left(d\left(\frac{A_l(t)}{q^l_{k'}(t)}\right)\right) = -l - 1 < 0.$$

Luego en 3.5, se tiene que $v_{q_k(t)}(d(v)) = -n_k - 1 < 0$. Por otra parte, tomando $q(t)$ cualquier polinomio normal, irreducible y mónico, y aplicando $v_{q(t)}$ a la ecuación 3.3, se tiene que $v_{q(t)}(d(v)) \geq 0$. Luego, necesariamente, debe ser $q_k(t) = t$, para todo k. Luego, podemos escribir v, de la siguiente forma

$$v = \sum_{j=-m'}^{m} b_j t^j.$$

Además, 3.5 queda como

$$dv = \sum_{j=-m'}^{m} (d(b_j) + j b_j d(g)) t^j.$$

Así que, tomando $m = 1$, se tiene que $d(b_1) + b_1 d(g) = f$, es decir, eligiendo $a = b_1$ tenemos la igualdad deseada.

Recíprocamente, si $f = d(a) + ad(g)$, entonces

$$fe^g = d(a)e^g + ad(g)e^g = d(ae^g),$$

donde ae^g es una función elemental.

Ejemplo:

Con este último razonamiento podemos ver, por ejemplo, que la integral de la función e^{-z^2} no puede expresarse en términos de funciones elementales. Vamos a razonar por reducción al absurdo, suponiendo que dicha integral es elemental, entonces por el razonamiento anterior existe un elemento $a \in \mathbb{C}(z)$ de modo que $f(z) = d(a) + ad(g(z))$, donde $f(z) = 1$ y $g(z) = -z^2$. Entonces, $1 = d(a) - a2z$. Supongamos que a es de la forma $a = \frac{p(z)}{q(z)}$, donde $p(z)$ y $q(z)$ son polinomios de $\mathbb{C}[z]$. Además, podemos suponer sin pérdida de generalidad que $p(z)$ y $q(z)$ no tienen raíces en común. Luego,

$$1 = \frac{d(p(z))q(z) - d(q(z))p(z)}{q(z)^2} + \frac{p(z)}{q(z)}(-2z),$$

es decir,

$$q(z)^2 = d(p(z))q(z) - d(q(z))p(z) + p(z)q(z)(-2z).$$

Por lo tanto,

$$d(q(z))p(z) = q(z)\left(d(p(z))q(z) - p(z)2z - q(z)\right).$$

Supongamos que el polinomio $q(z)$ tiene una raíz R de multiplicidad m, es decir, $(z-R)^m|q(z)$. Entonces, $p(R) \neq 0$, ya que $p(z)$ y $q(z)$ son coprimos por hipótesis. Así que, por la igualdad anterior R debe ser una raíz de $d(q)$, de hecho, debe ocurrir que $(z-R)^m|d(q(z))$. Pero hemos llegado a un absurdo, ya que $d(q)$ y q no pueden tener una misma raíz con igual multiplicidad. Por lo tanto, $q(z)$ no tiene raíces, es decir, es un polinomio constante. Sea $q(z) = c$, entonces $a = \frac{p(z)}{c}$, es decir, a es un polinomio. Pero,

$$0 = gr(1) = gr\left(d(a(z)) - a(z)2z\right) = gr(a) + 1,$$

es decir, hemos llegado a contradicción. Por lo tanto queda probado que $\int e^{-z^2}$ no es una integral elemental.

Siguiendo el mismo razonamiento, puede probarse que funciones como $\frac{1}{z}e^z$ o $\frac{sen(z)}{z}$ no poseen integral elemental.

Bibliografía

[1] JONES GARETH A. Y DAVID SINGERMAN, *Complex functions: An algebraic and geometric viewpoint*, Cambridge University Press 1987.

[2] BRONSTEIN, M., *Symbolic Integration I. Transcendental Functions*, Springer-Verlag 1997.

[3] MAXWELL ROSENLICHT, *Liouville's theorem on functions with elementary integrals*, Pacific journal of mathematics Vol.24 No.1, 1968.

[4] IRVING KAPLANSKY, *An introduction to differential algebra*, Hermann, 1957.

[5] JOSEPH FELS RITT, *Differential Algebra*, American Mathematical Society,1950.

[6] TERESA CRESPO, ZBIGNIEW HAJTO , *Algebraic Groups and Differential Galois Theory*, American Mathematical Society,2011.

[7] MARIUS VAN DER PUT , MICHAEL F. SINGER, *Galois Theory of Linear Differential Equations*, Springer 2003.

[8] LANG, S., *Algebra*, Aguilar 1973.

[9] C. IVORRA, *Funciones sin primitiva elemental*, La Gaceta de la Real Sociedad Matemática Española Vol.12 No.3, 2009.

[10] MICHAEL F.SINGER, *Elementary solutions of differential equations*, Pacific journal of mathematics Vol.59 No.2, 1975.