Beca de Colaboración

Facultad de Matemáticas

Ecuaciones sin solución elemental
Funciones de Liouville

Autor: Raúl Sastriques Guardiola

Director: Dr. Celso Martínez Carracedo
Realizado en: Departamento de Matemática Aplicada

Valencia, 1 de julio de 2016

Resumen

Es bien conocido del cálculo integral, que no toda integral de una función, pese a ser integrable, pueda ser escrita haciendo uso de funciones más simples y conocidas, las cuales llamamos funciones elementales. En el presente texto trataremos con el problema análogo para la teoría de las ecuaciones diferenciales. Así pues, trataremos con la definición de función elemental, extendiéndola ligeramente (admitiendo integrales de estas) con tal de crear un nuevo concepto de funciones, funciones de Liouville, las cuales finalmente veremos que fallan en su cometido de ser soluciones de ecuaciones tan simples como la ecuación de Riccati.
Esto es, probaremos que en particular la ecuación de Riccati

$$y' + y^2 = 1 + t/x^2 \quad \text{con } t \neq 0$$

no admite soluciones elementales, ni de Liouville, salvo para una cantidad numerable de valores del parámetro t, lo cual pone de manifiesto la necesidad de métodos numéricos para la resolución, aun cuando solo sea aproximada, de las ecuaciones diferenciales.

Parte de la teoría aquí expuesta, se asume como elemental o bien ya conocida, aun cuando la conjunción de la misma nos permita exponer un resultado probablemente desconocido para el lector. Por otro lado, a lo largo del documento se desarrollarán resultados propios con base en nuestra finalidad, de los cuales gran parte son resultados de divisibilidad en anillos y conceptos básicos de álgebra.

Las líneas del presente documento son una adaptación, se entiende más explicativa, de los resultados del capítulo 20 del libro *Introducción a las Ecuaciones Diferenciales Ordinarias* de los autores Celso Martínez Carracedo y Miguel A. Sanz Alix.

Prerrequisitos

Pese a que fundamentalmente el desarrollo de la teoría es algebraico, en tanto que nos encontramos en al ámbito de las ecuaciones diferenciales, requerimos ciertos resultados propios del análisis complejo. Estos son:

1. Teorema de la función Implícita.
2. Los ceros de una función holomorfa sobre un abierto conexo no vacío son aislados.
3. Toda función holomorfa admite primitiva sobre un abierto simplemente conexo.

Mientras que los dos primeros teoremas se requiere para la demostración de ciertos resultados, el segundo tiene un carácter mas formal para la teoría.

Con respecto a la notación, si A es un anillo conmutativo sin divisores de ceros (A dominio de integridad), $P(A)$ denota al conjunto de polinomios sobre A. Decimos que un polinomio es **propio** si no es de grado cero, en caso contrario decimos que es **constante** o **no propio**.

DEFINICIÓN 1. Dados $f, g \in P(A)$, se dice que g divide a f si existen $a \in A$, $a \neq 0$ y $q \in P(A)$ tales que:

$$af = qg.$$

En este caso también se dice que f es múltiplo de g o que g es divisor de f.

Se dice que un polinomio propio g es primo si no existe ningún polinomio propio distinto de g que le divida. De forma similar, dos polinomios propios son primos entre sí, si no existe otro polinomio propio que sea divisor común a ambos.

Teorema 0.0.1 (Algoritmo de la división)**.**
Sea R un anillo, f y g polinomios no nulos sobre R. Supongamos que el coeficiente director de g es una unidad de R. Entonces existen dos únicos polinomios q, r tales que $f = q{\cdot}g + r$ con $grad(r) < grad(g)$.

En caso de ser g no mónico, existen $q, r \in P(A)$ y $c \in (A), c \neq 0$ tal que $c \cdot f = g \cdot q + r$

Teorema 0.0.2 (Existencia del m. c. d)**.**
Sea A un dominio de integridad y sean $f, g \in P(A)$. Se tiene existe un polinomio de grado máximo divisor común de f y g. Además, es único salvo multiplicación por una unidad del anillo A.

Teorema 0.0.3 (Identindad de Bezout)**.**
Siendo d un máximo común divisor de los polinomios $f, g \in P(A)$, se tiene existen $v, w \in P(A)$ tales que

$$vf + wg = d.$$

DEFINICIÓN 2. Sea A es un subanillo propio de otro anillo B y sea $\phi \in B$. Decimos que un polinomio propio Q es **anulador** de ϕ si al sustituir la variable formal por el elemento ϕ resulta $Q(\phi) = 0$. Cuando el grado de Q es mínimo decimos que Q es anulador mínimo.

Hacemos dos aclaraciones con respecto a la anterior definición:

1. Escribimos Q con letras capitales aquí abusando de notación. En el siguiente capítulo ϕ será una función dependiendo de x, por lo que el polinomio Q, tras sustituirse la variable formal por ϕ nos deja una función, la cual puede ser evaluada en x, la igualdad $Q(\phi) = 0$ se entiende como $Q(\phi)$ es la función cero, esto es: vale cero para todo x del dominio de ϕ. La escritura en mayúsculas del polinomio Q se entiende heredada de la teoría de polinomios sobre anillos de matrices.
2. Al igual que Teorema de Hamilton Cayley la sustitución no se entiende formalmente, esto es, haciendo uso del homomorfismo de sustitución. La sustitución no es más que la consideración de relación con ϕ proporcionada por el polinomio.

Teorema 0.0.4 (Polinomio anulador mínimo)**.**
Si Q es polinomio anulador mínimo de $\phi \in B$, se verifica que Q es primo en B y cualquier otro polinomio anulador es múltiplo de Q. Consecuentemente, el anulador mínimo es único, salvo producto por un factor de A.

Capítulo 1

Dependencia algebraica

Siendo $\Omega \subseteq \mathbb{C}$ región, i. e., abierto conexo no vacío, denotamos por H_Ω al anillo de todas las funciones analíticas sobre Ω y dado $F \subseteq H_\Omega$, denotamos por $A(F)$ al subanillo de H_Ω formado por las funciones de la forma: $\sum_{k=1}^{n} \alpha_k f_k^{n_k}$ donde $\alpha_k \in \mathbb{C},\ f_k \in F$ y $n \in \mathbb{N}$.

Si $Q \in P(A(F))$, Q es de la forma $Q = z_p X^{p-1} + z_{p-1} X^{p-1} + ... + z_1 X + z_0$ donde X es la variable formal y las funciones z_i pertenecen al anillo $A(F)$. Con esto, si $h \in A(F)$ y $x \in \Omega$ podemos sustituir la variable formal por la función holomorfa h evaluada en x al igual que el resto de funciones z_i, con tal de obtener la expresión:

$$Q(x, h(x)) = z_p(x)h(x)^{p-1} + z_{p-1}(x)h(x)^{p-1} + ... + z_1(x)h(x) + z_0(x).$$

A menudo escribiremos $Q(\cdot, h) = z_p h + z_{p-1} h + ... + z_1 h + z_0$ por tal simplificar la expresión en tanto que el punto x es arbitrario. La escritura de Q en esta forma, nos lleva a una función de varias variables $Q(x, h)$, de modo que su parcial respecto de la primera variable es, por la regla de la cadena:

$$\frac{\partial Q}{\partial x} = \frac{\partial Q}{\partial x} \cdot \frac{\partial x}{\partial x} + \frac{\partial Q}{\partial h} \cdot \frac{\partial h}{\partial x}, \quad \text{donde } \frac{\partial x}{\partial x} = 1.$$

Remarcamos que el siguiente concepto estará presente a lo largo de toda la teoría.

DEFINICIÓN 3. Decimos que $\phi \in H_\Omega, \phi \neq 0$ **depende algebraicamente** de $F \subset H_\Omega$ si existe un polinomio no necesariamente propio $Q \in P(A(F))$ anulador de ϕ.

Con el fin de establecer el primer teorema del capítulo resaltamos, lo que en parte, es una de sus principales motivaciones.

OBSERVACIÓN 4. En general, dadas $g, \phi \in H_\Omega$, dos relaciones del tipo:

$$F(x, g(x), \phi(x)) = 0, \;\; G(x, g(x)) = 0 \;\forall x \in \Omega,$$

no es fácil "eliminar" la función g de las relaciones anteriores obteniendo otra nueva relación H verificando

$$H(x, \phi(x)) = 0.$$

Sin embargo, escogiendo una **clase de polinomios adecuada**, la teoría de la divisibilidad permite obtener esta nueva relación H cuando F y G son polinómicas y además asegura que H es de nuevo polinómica. El siguiente teorema es la prueba de esta afirmación.

Teorema 1.0.1 (Carácter transitivo de la dependencia algebraica)**.**
Si una función $\phi \in H_\Omega$ depende algebraicamente de $F \cup G \subset H_\Omega$ y a su vez, las funciones de G dependen algebraicamente de las funciones de F, entonces ϕ depende algebraicamente de F.

DEMOSTRACIÓN. Dado un polinomio de $P(A(F))$ se tiene de la propia definición de $A(F)$ que sus coeficientes constan de una cantidad finita de elementos de $F \cup G$, basta así probar en el caso en el que F es finito y G consta de un único elemento $g \in H_\Omega$. Esto es así dado que ϕ es combinación lineal **finita** de funciones de F, lo cual motiva dicha definición).

Existirán dos polinomios: $Q \in P(A(F))$ y $T \in P(A(F \cup \{g\}))$ ambos polinomios anuladores mínimos: Q anulador de g y T de ϕ.

Sean $f_0, f_1, \ldots, f_n \in A(F)$ con $f_0 \neq 0$ tales qué $Q = f_0 Y^q + f_1 Y^{q-1} + \ldots + f_{q-1} Y + f_q$.

Análogamente, sean $h_0, h_1, \ldots, h_n \in A(F \cup \{g\})$ con $h_0 \neq 0$ tal que$T = h_0 Z^n + h_1 Z^{n-1} + \ldots + h_{n-1} Z + h_n$.

Dado que cada función h_i es de la forma $\sum_{k=1}^{n} \alpha_k \psi_k^{n_k} g^{n_k}$ con $\psi \in F$ tenemos existen polinomios $T_i \in P(A(F))$ de modo que $T_i(g) = h_i$ (es suficiente identificar g^{n_k} con Y^{n_k}); además podemos suponer que el grado de cada T_i es menor que grado de Q:

Siendo T_i de grado mayor al de Q efectuamos el algoritmo de división obteniendo:

$$p_i T_i = C_i Q + R_i, \text{ con } p_i \in A(F) \text{ no nula,}$$

y C_i, R_i elementos de $P(A(F))$ con $grad(R_i) < q$;
Ahora, por ser Q anulador de g se tiene: $p_i T_i(g) = R_i(g)$ por lo que basta considerar los polinomios $p_i T_j \quad j \neq i$ y R_i si $j = i$ para obtener una relación análoga a la

que verifican los T_i, ahora, respecto del polinomio anulador mínimo $p_i T$.
Puesto que hay una cantidad finita de polinomios T_i, basta en caso de no ser de grado menor que q reemplazarlos mediante este procedimiento.

En tanto que pretendemos probar que ϕ depende algebraicamente de F, con tal de eliminar el conjunto $G = \{g\}$ de esta dependencia, consideramos el polinomio de *varias variables* Z, Y:

$$T^* = T_0 Z^n + T_1 Z^{n-1} + \ldots + T_{n-1} Z + T_n,$$

el cual verifica informalmente $T^*(g) = T$; notamos que T^* depende de dos funciones así como de la variable x y verifica $T^*(x, g(x), \phi(x)) = 0 \ \forall x$.

T^* generaliza a T sin hacer uso de la función g; podemos considerar $T^* \in P(P(A(F)))$ esto es: T^* es un polinomio con coeficientes en el anillo de los polinomios sobre $A(F)$; claramente, un polinomio sobre el anillo $A(F)$ como Q pertenece también al anillo $P(P(A(F)))$, basta notar que se trata de un polinomio no propio para la variable Z.

Por otro lado, si reordenamos T^* respecto de la variable Y queda como:

$$T^* = S_0 Y^r + S_1 Y^{r-1} + \ldots + S_{r-1} Y + S_r, \quad S_j \in P(A(F)) \text{ con } S_0 \neq 0,$$

donde sabemos que $r < q = grad(Q)$ pues r es el grado de algún T_i, y los polinomios S_j tienen a Z como variable formal.

Dado que la variable formal Z ha sido introducida al definir T^*, parece razonable abusando de notación dejarla como variable formal para polinomios de $P(P(A(F)))$. Sin embargo, dentro de esta demostración resulta necesario remarcar en cada momento que variable es la del polinomio y cuál la del coeficiente.
Así, tras haber reordenado T^* procedemos a ver las variables en $P(P(A(F)))$ de modo contrario, esto es: Z es la variable de los coeficientes del polinomio mientras que Y es la variable, digamos propia, del anillo más general. Así, Q no es constante mientras que si lo son sus coeficientes.

El objetivo de la demostración puede entenderse mejor a partir de la observación previa.
Nuestra función polinómica H queda aquí identificada con Q mientras que F, puesto que depende de dos funciones, con T^*. La nueva relación H debe ser un polinomio de $P(A(F))$, denotado por D, el cual debe anular a ϕ.

Tomamos como D el máximo común divisor de Q y T^* en $P(P(A(F)))$ de variables Y como variables del polinomio y Z como variable de los coeficientes; Probaremos mediante la relación de Bezout que D es anulador de ϕ y mantiene el carácter polinómico, $D \in P(A(F))$, teniéndose el resultado.

Para ello veamos que Q y T^* son coprimos en $P(P(A(F)))$, relación para la que es suficiente probar que Q es primo, dado que al ser T^* de grado inferior no podrá ser múltiplo pero tampoco divisor de Q. Para el razonamiento de Q es primo en $P(P(A(F)))$ razonamos por contradicción usando que es anulador mínimo de g.

Sea, pues, una división en polinomios propios de Q:

$$H_0(Z)\overbrace{[f_0Y^q + f_1Y^{q-1} + \ldots + f_{q-1}Y + f_q]}^{Q} = \overbrace{[U_0(Z)Y^s + \ldots + U_s(Z)]}^{U}\overbrace{[V_0(z)Y^{q-s} + \ldots + V_{q-s}(Z)]}^{V},$$

con H_0, U_0, V_0 no nulos. Sustituyendo Z por una función $z_0 \in \mathbb{C}$ (función constante) satisfaciendo que $H_0(z_0) \in A(F)$ sea una función no nula, se obtiene un polinomio propio (por medio de $U(z_0, Y)$ o de $V(z_0, Y)$) anulador de g y de grado menor que q, hecho contradictorio.

Ya que Q, T^* son coprimos, cualquier máximo común divisor debe ser no propio, equivalentemente, pertenecer a $P(A(F))$, así D no consta de la variable Y mientras que constará de la variable Z si y solo si es un polinomio propio de $P(A(F))$.

El teorema de Bezout nos da la existencia de polinomios $P, W \in P(P(A(F)))$ tales que

$$PQ + WT^* = D.$$

De ser D un polinomio no propio de $P(A(F))$ (D no consta de las variables Y ni Z) tomamos $x \in \Omega$ y sustituyendo las variables Y por $g(x)$ y Z por $\phi(x)$ en la relación anterior llegamos a la relación:

$$0 = P(x, g(x), \phi(x)) \cdot \underbrace{Q(x, g(x))}_{=0} + W(x, g(x), \phi(x)) \cdot \underbrace{T^*(x, g(x), \phi(x))}_{=0} = D(x),$$

quedando así contradicho el hecho de ser el máximo común divisor no nulo.

Tenemos que D es un polinomio propio de $P(A(F))$ y así consta de la variable formal Z, pero no de Y, repitiendo lo anterior escribiendo ahora en la relación de Bezout

$D(x, \phi(x))$, en lugar de $D(x)$ tenemos que D es anulador de ϕ, dándose la dependencia algebraica de ϕ respecto de F. $\square$

Este teorema permite probar que la dependencia algebraica es una relación de equivalencia: mientras que la propiedad reflexiva y simétrica son directas de su definición, la propiedad transitiva es menos intuitiva y se trata del resultado anterior. Por ello denotaremos en ciertas ocasiones $\psi \sim G$ con tal de indicar que ψ es una función que depende algebraicamente del conjunto G.

COROLARIO 5. *Dadas $f, g \in H_\Omega$, y un subconjunto F de H_Ω, se verifican las siguientes propiedades:*

1. Si f, g dependen algebraicamente de F, se sigue verificando para $f + g$ y $f \cdot g$.

2. Si $f \neq 0$ depende algebraicamente de F, la función inversa $\frac{1}{f}$ *(definida sobre un abierto conexo)* también lo hace.

3. Si el anillo $A(F)$ es estable bajo derivación, entonces la dependencia algebraica de una función $f \in F$ implica la dependencia de f' en F.

DEMOSTRACIÓN. 1. Siendo $\phi = f + g$ y $\psi = f \cdot g$ funciones del anillo $A(F)$ que dependen algebraicamente de $F \cup \{f, g\}$, se tiene por el teorema anterior que $\phi\, \psi$ dependen algebraicamente de F.

2. En primer lugar, remarcar que siendo f holomorfa sobre Ω, abierto conexo, el conjunto de sus ceros es un conjunto discreto y aislado. Así, dado un punto x tal que $f(x) \neq 0$, es suficiente tomar una bola abierta de radio suficientemente pequeño como abierto conexo sobre el que definir la inversa (al ser los ceros aislados no se acumulan).

3. Si $Q = h_0 Y^n + h_1 Y^{n-1} + \ldots + h_{n-1} Y + h_n$ es polinomio anulador de f. Derivando la expresión $Q(x, f(x)) = 0$ respecto de x, por la regla de la cadena queda:

$$0 = \frac{\partial Q}{\partial x}(x, f(x)) = \frac{\partial Q}{\partial f}(x, f(x)) \cdot f'(x) + \frac{\partial Q}{\partial x}(x, f(x)).$$

Lo cual equivale a que el polinomio $\frac{\partial Q}{\partial f} Z + \frac{\partial Q}{\partial x}$ sea anulador de f'. Dicho polinomio es propio por ser Q anulador mínimo de f, en otro caso $\frac{\partial Q}{\partial Y} = 0$, luego $Q \in A(F)$, Q "constante" e igual a cero. Su expresión explicita es:

$$(h_0nf^{n-1}+h_1(n-1)f^{n-2}+\ldots+h_{n-2}2f+h_{n-1})Z+(h_0^{'}f^n+\ldots+h_{n-1}^{'}f+h_n^{'})$$

por lo que resulta pertenecer a $P(A(F)$ dada la supuesta estabilidad de $A(F)$ bajo derivación y el teorema 1.0.1. Así f' depende algebraicamente de F.

□

Teorema 1.0.2.
Dadas $h_0,\ldots,h_n\in H_\Omega$ *con* $h_0\neq 0$ $n\geq 1$ *existe un subconjunto abierto conexo* $\Omega_0\subset\Omega$ *y una función* $\phi\in H_\Omega$ *tal que*

$$Q=h_0Y^n+h_1Y^{n-1}+\ldots+h_{n-1}Y+h_n$$

es un polinomio anulador de ϕ*.*

DEMOSTRACIÓN. Sea Q_Y el derivado formal de Q respecto de Y. De existir $(x_0,z_0)\in\Omega\times\mathbb{C}$ con $Q(x_0,z_0)=0$ y $Q_Y(x_0,z_0)\neq 0$ por el teorema de la función implícita se tendrá la existencia de una función analítica ϕ definida en sobre un abierto conexo Ω_0 entorno de x_0, de modo que $Q(x,\phi(x))=0$ $\forall x\in\Omega_0$ teniéndose el resultado.

En otro caso, se tendrá $Q_Y(x,z)\neq 0$ para todo $(x,z)\in\Omega$ tal que $Q(x,z)=0$. Sea, pues, $F=\{h_0,\ldots,h_n\}$ y D el máximo común divisor en $P(A(F))$ de los polinomios Q y Q_Y, por el teorema de Bezout existen V,W polinomios de $P(A(F))$ tal que:

$$VQ+WQ_Y=D$$

Afirmamos que D es un polinomio propio de grado menor que n.
En caso de no ser propio, dado que $D\in A(F)$ verifica para cada $x\in\Omega$ con $h_0(x)\neq 0$ (los ceros la una función holomorfa son aislados), y $z(x)$ una raíz de $Q(x,z)=0$:

$$D(x)=V(x,z(x))Q(x,z(x))+W(x,z(x))Q_Y(x,z(x))=0$$

Consideramos el cociente $C_0\in P(A(F))$ resultado de dividir Q entre D. Tenemos dos posibilidades para C_0 : existe $(x_{0,}z_0)\in\Omega\times\mathbb{C}$ tal que $C_0(x_0,z_0)=0$ y $C(x_0,z_0)\neq 0$ o bien $C_0(x,z)=0$ $C_{0Y}(x,z)=0$ $\forall(x,z)\in\Omega\times\mathbb{C}$.

En el primer caso, dado que los coeficientes de C_0 son analíticos, por el teorema de la función implícita, existe una función analítica ϕ definida sobre un entorno de x_0 (supondremos abierto conexo), tal que C_0 es anulador de ϕ, y así lo será Q el cual es múltiplo de C_0.

En el segundo caso, aplicamos el mismo argumento, esto es: consideramos $C_1 \in P(A(F))$ resultado de dividir C_0 entre D_0, máximo común divisor de C_0 y C_{0Y}. Dado que podemos reiterar el argumento las veces que sea necesario, tenemos, en caso de ser falso el enunciado, existirán dos familias numerables de polinomios propios $\{C_n\}_{n\in\mathbb{N}}$ y $\{D_n\}_{n\in\mathbb{N}}$, de forma que $D_0 \cdot D_1 \cdot \ldots \cdot D_k$ dividen a Q, siendo Q polinomio de grado n, lo cual es absurdo. $\square$

Capítulo 2

Funciones Elementales

DEFINICIÓN 6. Dado un conjunto G de funciones analíticas, denotamos por $\mathbf{A}^*(\mathbf{G})$, al conjunto de todas las funciones analíticas que dependen algebraicamente de G sobre *algún* abierto conexo.

Un caso particular es cuando el conjunto G consta solo de la identidad compleja, aquí denotada por $\{x\}$. En tal caso, a las funciones de $A^*(\{x\})$ reciben el nombre de **funciones algebraicas**.

De ahora en adelante haremos el convenio, dada una función f, de denotar por e^f a la exponencial de f y por $\int f$ a una primitiva de f (salvo constante) sobre un dominio en el cual admite primitiva. Dado que ser holomorfa en Ω, abierto no vacío conexo, es equivalente a ser analítica en dicha región, y esta clase de funciones tienen siempre primitiva, podríamos restringir la anterior definición a abiertos simplemente conexos, sin perdida de generalidad, pues en ambos casos está garantizada la existencia de primitiva para $f \in H_\Omega$.
Por último, destacar que si se verifica $f \sim G$ sobre un entorno abierto sigue siendo cierto que $f \in A^*(G)$ pues es posible restringir el entorno para obtener Ω abierto conexo.

DEFINICIÓN 7. Dadas las sucesiones de conjuntos $\{R_n\}_{n\geq 1}$ y $\{M_n\}_{n\geq 0}$:

$$R_0 := A^*(\{x\})$$
$$M_n = \{e^f, \int f \ : f \in R_{n-1}\}$$
$$R_n = A^*(R_{n-1} \cup M_n) \ \ n = 1, 2, \ldots$$

Se define el conjunto $\mathscr{E}$, **conjunto de las funciones elementales** como:

$$\mathscr{E} = \cup_{n\geq 0} R_n$$

Sin entrar ahora en detalle, podemos entender por función elemental a toda función formada por una cantidad ***finita*** de sumas, productos y cocientes (donde tenga sentido tal operación) de funciones "elementales": exponenciales, trigonométricas y polinómicas; así como sus inversas, derivadas, integrales y composiciones de estas. Así, funciones como el logaritmo, raíces y del tipo 2^x siguen siendo elementales.

Lo cierto es que este tipo de funciones resultan muy cercanas a nuestra intuición, tanto que resulta complicado pensar en una función que no lo sea; los ejemplos más *"simples"* de funciones no elementales son las funciones $Zeta$, $Gamma\ Bessel$, $hypergeometricas$.

Teorema 2.0.1.
Se verifican las siguientes propiedades:

1. Si G es un subconjunto finito de funciones de R_n con dominio común Ω, y $g \in H_\Omega$ es tal que depende algebraicamente de G, entonces $g \in R_n$. Consecuentemente, si $f, g \in R_n$ se tiene $f + g, f{\cdot}g \in R_n$.

2. $f \in R_n \to f' \in R_n,\ e^f, \int f \in M_{n+1}$.

DEMOSTRACIÓN. 1. Tenemos $G \subset R_n = A^*(R_{n-1} \cup M_n)$, esto es: $G = \{f \text{ tal que } f \sim (R_{n-1} \cup M_n)\, sobre\, \Omega\}$. Si $g \in H_\Omega$ depende algebraicamente de G, así lo hace con respecto a $G \cup (R_{n-1} \cup M_n)$ y por el teorema 1.0.1 se tiene la dependencia de g con respecto a $(R_{n-1} \cup M_n)$ sobre Ω,i. e., $g \in A^*(R_{n-1} \cup M_n) = R_n$. La consecuencia explicitada en el enunciado, es directa de lo probado, mientras que notamos que por ser G finito, no hace uso de todas las funciones de R_{n-1} y M_n, por lo que es suficiente trabajar con dos subconjuntos finitos de R_{n-1} y M_n, que denotamos por R, M, con tal de concluir que dicha función g se encuentra en $A^*(R \cup M) \subset R_n$ (esto será útil en el teorema de Liouville).

2. La segunda implicación es directa de la definición de M_n. Para ver que $f \in R_n \to f' \in R_n$ utilizaremos inducción.

   Para $n = 0$, estamos en el caso de las funciones algebraicas y el enunciado resulta ser el aparado tercero del corolario 5. Supuesto cierto para $n - 1$, tenemos que si $f \in R_n$ entonces $f \sim F \subset R_{n-1} \cup M_n$ (sobre un abierto conexo Ω). Es claro que podemos considerar F finito, basta considerar los coeficientes del polinomio anulador y Ω un dominio común de estos. Basta ahora probar que el anillo $A(F)$ es estable bajo derivación, de donde tendremos que la función $f' \in H_\Omega$ depende algebraicamente de F, y por el apartado anterior se concluirá el resultado.

   Ver que el anillo es estable bajo derivación, consiste en ver que un monomio con coeficiente una función del tipo h^m, $\int h$, e^h con $h \in R_{n-1}$, se convierte tras derivar en una expresión del tipo anterior, lo cual es directo teniendo en cuenta que los factores dependen exclusivamente h y h' pertenecen a R_{n-1}, el primero por definición, y el segundo por hipótesis de inducción.

$\square$

El siguiente resultado es clave para la demostración de nuestro cometido, probar que existen ecuaciones elementales sin solución elemental- En particular, la ecuación de Riccati: $\psi' + \psi^2 = 1 + \frac{t}{x}$, solo admite soluciones elementales para valores algebraicos del parámetro t.

Pese a no ser un teorema especialmente enrevesado, resulta tedioso formalizarlo, dado que requiere de numerosas operaciones de carácter simple, pero necesarias. Por ello, se presentará la demostración de forma distinta: la demostración se presenta divida en etapas, encontrándose al final de esta un resumen de la misma. La finalidad es evitar dejar indicaciones para la demostración, que de tenerse que probar puedan no resultar tan sencillas como se indican, al tiempo que se evita una demostración larga y tediosa.

En primera instancia, el lector debería leer atentamente la demostración verificando los pasos de dentro de cada etapa, con el propósito de entender la demostración, en una segunda lectura, por medio de las conclusiones de las etapas, más que por el contenido de las mismas.

Teorema 2.0.2 (Teorema de Liouville)**.**
Dado $n \geq 0$, sea $f \in R_n$ y suponer que existe una solución de la ecuación de Riccati

$$y' + y^2 = f$$

de manera que dicha solución pertenece a $R_m,\ m > n$. Entonces existe otra solución de la ecuación de Riccati perteneciente a R_{m-1}.

En particular, si f es algebraica y la ecuación diferencial admite solución elemental, admite también solución algebraica.

DEMOSTRACIÓN. Si ψ es solución, y $\psi \in R_m$, entonces ψ depende algebraicamente, sobre un conjunto finito de la forma $F \cup G$ con $F \subset R_{m-1}$ y $G \subset M_m$, y donde supondremos G no vacío, en otro caso, se daría $\psi \in R_{m-1}$ teniéndose el resultado.

Pese a que no podemos reducir G al conjunto vacío, tiene sentido eliminar la mayor cantidad de funciones de G; tras esta idea se esconde una necesidad posterior en la demostración, que por conveniencia exponemos ahora:

G irreducible: Si $g \in G$ es tal que $q \sim (G \backslash \{g\}) \cup R_{m-1}$, por el teorema 1.0.1 $\psi \sim (G \backslash \{g\}) \cup F'$ donde F' es el conjunto F, junto al resto de funciones de R_{m-1} de las cuales depende g. Notar que F' sigue siendo finito. Por otra parte, la cantidad de funciones g de esta forma debe ser también finita, pues así lo es G pudiéndose eliminar tales funciones de dicho conjunto. Bajo esta forma decimos que G es irreducible.

Debemos probar que existe otra solución del problema, ϕ, que no dependa de ninguna función de M_n. Podemos relacionar esto con nuestras observaciones de la siguiente forma:

ϕ no dependerá de g, para ningún $g \in G \subseteq M_m$. Así fijada $g \in G$, es suficiente probar que existe una solución que dependa algebraicamente de $(G\backslash\{g\}) \cup R_{m-1}$, pues reiterando el proceso, llegaríamos a la existencia de una solución ϕ, que no dependa de ninguna función de G, de donde $\phi \in R_{m-1}$.

Requerimos *otra* solución del problema y que además dependa del conjunto $(G\backslash\{g\}) \cup R_{m-1}$

La pregunta natural a plantearse ahora es: **¿Como hacemos esto?**

Para ello utilizaremos el teorema 1.0.2el cuál definirá una función, que con los pasos adecuados probaremos que en efecto es solución; además, la dependencia algebraica sobre el conjunto deseado será consecuencia del propio teorema.

Conclusión de: ¿Cómo? Requerimos las funciones de $(G\backslash\{g\}) \cup R_{m-1}$ $(= H_\Omega)$ adecuadas. Si denotamos por $h_0^*, \ldots, h_p^*$ a dichas funciones, nuestra nueva solución está determinada por ser el polinomio:

$$Q^* = h_0^* V^p + h_1^* V^{p-1} + \ldots + h_{p-1}^* V + h_p^*$$

el polinomio anulador mínimo de ϕ.

Empezamos la demostración estudiando el polinomio anulador mínimo de ψ el cual denotamos por Q y abusando de notación para el subíndice p:

$$Q = h_0 Y^p + h_1 Y^{p-1} + \ldots + h_{p-1} Y + h_p$$

Debemos estudiar los coeficientes h_j y pensar en como definir h_j^*.

Recordamos que al mismo tiempo que hacemos esto pretendemos eliminar g de la dependencia de la solución. Procedemos, por tanto, a obtener una expresión de nuestro polinomio Q en el que podamos visualizar la indeseada función $g \in G$.

Dispuestos a usar la condición $\psi' + \psi^2 = f$, realizamos la derivada respecto de $\cdot$ en $Q(\cdot, \psi(\cdot)) = 0$. Tras derivar, eliminamos la derivada de ψ, por la relación anterior (ec. de Riccati), y reordenando la expresión como si de un polinomio en ψ se tratase, obtenemos:

$$0 = -ph_0\psi^{p+1} + [-(p-1)h_1 + h_0']\psi^p + \ldots + h_{p-1}f + h_p'$$

Si identificamos ψ con la variable formal Y, obtendremos un polinomio de grado $p+1$ anulador de ψ, el cual llamamos T y cuya expresión es:

$$\begin{aligned} T &= -ph_0Y^{p+1} + [-(p-1)h_1 + h_0']Y^p + [-(p-2)h_2 + ph_0f + h_1']Y^{p-1} + \\ &\quad \ldots + [-h_{p-1} + 3h_{p-3}f + h_{p-2}']Y^2 + [2h\_p - 2f + h\_p - 1]Y + h_{p-1}f + h_p' \end{aligned}$$

de donde se deduce que T, tiene sus coeficientes en el anillo $A(G \cup R_{m-1})$, por el teorema anterior.

Con una finalidad posterior, escribimos ahora T identificando $\cdot$ con x, esto es, como: $T = \frac{\partial Q}{\partial \psi}\frac{\partial \psi}{\partial x} + \frac{\partial Q}{\partial x}\frac{\partial x}{\partial x} = (-\psi^2 + f)\frac{\partial Q}{\partial \psi} + \frac{\partial Q}{\partial x}$. Tras tomar $V = \psi$, queda como:

$$T = (-V^2 + f)\frac{\partial Q}{\partial V} + \frac{\partial Q}{\partial x}$$

Siendo Q, T anuladores de ψ sobre un mismo anillo, con Q mínimo, se concluye por el Teorema 0.0.1, existen σ, τ, $\mu \in A(G \cup R_{m-1})$? tales que:

$$\sigma T = (\tau Y + \mu)Q$$

Sistema.

Identificando los coeficientes de Y^k, $k = 0, \ldots, p$ obtenemos un sistema de $p+1$ ecuaciones. Antes de dar su expresión la simplificaremos un poco.

Del coeficiente de Y^{p+1} obtenemos la relación $\sigma(-ph_0) = \tau h_0$ y dado que $h_0 \neq 0$ $\tau = -p\sigma$.

Del coeficiente de Y^p obtenemos $-(p-1)h_1 + h_0' = \tau h_1 + \mu h_0$, usando la anterior queda $\sigma(h_1 + h_0') - \mu h_0$.

Del coeficiente de Y^{p-1} obtenemos $-(p-2)h_2 + ph_0f + h_1' = \tau h_2 + \mu h_1$ y de nuevo de la primera relación: $\sigma(2h_2 + ph_0f + h_1') - \mu h_0$.

Equivalentemente, se tiene el sistema de $p+1$ ecuaciones:

$$
\begin{aligned}
p\sigma + \tau &= 0 \\
\sigma[h_1 + h_0'] - \mu h_0 &= 0 \\
\sigma[2h_2 + ph_0 f + h_1'] - \mu h_1 &= 0 \\
&\vdots \\
\sigma[ph_p + 2h_{p-2} f + h_{p-1}'] - \mu h_{p-1} &= 0 \\
\sigma[h_{p-1} f + h_p'] - \mu h_p &= 0
\end{aligned} \tag{2.0.1}
$$

Siendo $g \in G$, puesto que cada una de las ecuaciones anteriores no es más que un polinomio sobre $A(G \cup R_{m-1})$, tenemos que o bien existe alguna función que depende algebraicamente de g, o bien ninguna de ellas lo hace en cuyo caso tenemos que ψ es solución del problema tal que no depende de g.

Situándonos en el caso desfavorable, alguna de las funciones del sistema depende algebraicamente de g. Estamos ya en disposición de dar una expresión que haga uso explicito de la función g.

Sean S, M, $Q_0, \ldots, Q_p, H_0, \ldots, H_p$ polinomios (de variable Z) sobre un anillo generado por $(G\backslash\{g\}) \cup R_{m-1}$ de modo que:

$$
\begin{gathered}
S(g) = \sigma\,,\ M(g) = \mu, \\
Q_0(g) = h_0\,, \ldots,\ Q_p(g) = h_p, \\
H_0(g) = h_0', \ldots,\ H_p(g) = h_p'.
\end{gathered}
$$

Notar que tales polinomios existen, dado que es suficiente en la expresión de cada una de las funciones anteriores, funciones del anillo $A(G \cup R_{m-1})$, identificar g con la variable formal Y, para obtener un polinomio con coeficientes en el anillo $(G\backslash\{g\}) \cup R_{m-1}$.
Además, podemos exigir que $grad(H_j) < grad(Q_j)$ $j = 0, 1, ..., p$, pues $Q_j'(g) = h_j'$ y el anillo es estable bajo derivación.

Haciendo uso de las nuevas funciones, el sistema queda como:

$$\begin{aligned} S(g)[Q_1(g)+H_0(g)]-M(g)Q_0(g) &= 0, \\ S(g)[2Q_2(g)+pQ_0(g)f+H_1(g)]-M(g)Q_1(g) &= 0, \\ &\vdots \\ S(g)[pQ_p(g)+2Q_{p-2}(g)f+H_{p-1}(g)]-M(g)Q_{p-1}(g) &= 0, \\ S(g)(Q_{p-1}(g)f+H_p(g))-M(g)Q_p(g) &= 0. \end{aligned}$$

Dado que G no tiene funciones que dependan algebraicamente de otras funciones de dicho conjunto, ni de funciones de R_m (G irreducible), tenemos que cada una de las ecuaciones funcionales deben ser idénticamente nulas.

Así, el sistema queda, sin depender de g, como:

$$\begin{aligned} S[Q_1+H_0]-MQ_0 &= 0, \\ S[2Q_2+pQ_0f+H_1]-MQ_1 &= 0, \\ &\vdots \\ S[pQ_p+2Q_{p-2}f+H_{p-1}]-MQ_{p-1} &= 0, \\ S(Q_{p-1}f+H_p)-MQ_p &= 0. \end{aligned} \tag{2.0.2}$$

Conclusión de: Sistema. Notamos que han aparecido nuevas funciones, polinomios, $S,\ M,\ Q_0,\ldots,\ Q_{p,}\ H_{0,}\ldots,\ H_p$, sobre $A((G\backslash\{g\})\cup R_{m-1})$, las cuales tienen relación directa con $h_j,\ j=1,...,p$, lo cual nos acerca a la definición de h_j^*. Además, hemos eliminado la función g de estas nuestras identidades funcionales, sistema 2.0.2 el cual vemos ahora que *"generalizan"* al sistema 2.0.1

Estudio del sistema.

Es claro que podemos dividir cada ecuación por él $m.c.d(S,M)$ obteniendo el mismo sistema. Así, podemos suponer que S,M son coprimos, y de igual forma, suponemos que las funciones $Q_j\ j=0,\ldots,p$ han sido dividas por el máximo común divisor del conjunto de todas ellas, lo cual es posible, ya que si dividimos Q por el divisor común de estos, el polinomio resultante sigue siendo anulador de ψ.

Afirmamos que $S,\ M$ tienen ambas grado cero. El grado de S es cero, ya que de la ecuación $i-ésima$, se deduce que S divide a MQ_i, y dado que $S,\ M$ son coprimos, S a de dividir a Q_i para todo i. Ahora, si suponemos si M es polinomio propio no cero, de la primera ecuación se tiene:

$$grad(Q_1) > grad(Q_2).$$

Recordamos que los polinomios H_j se habían tomado de modo que $grad(H_j) < grad(Q_j)$.
Análogamente, de la segunda ecuación se tiene que $grad(Q_2) > grad(Q_1)$ y reiterando el proceso obtenemos de la $p - ésima$ ecuación que $grad(Q_p) > grad(Q_{p-1})$, y por último de la $(p+1) - ésima$ tenemos $grad(Q_{p-1}) > grad(Q_p)$ llegando a una contradicción. Así M es de grado cero, al igual que S.

Queda claro que de ser $grad(Q_j) > grad(Q_0)$ para algún j, repitiendo el proceso, ahora recorriendo el sistema hacia arriba, llegaríamos a una contradicción con el hecho de ser $grad(Q_0) > grad(Q_0)$. Así, el grado de Q_j no excede el de Q_0 para ningún j.

Conclusión de: Estudio del sistema. Tenemos que $grad(Q_0) > grad(Q_j)\ \forall j$ y la familia $\{Q_j\}_{j=1}^{p}$ no tiene divisor común. Los polinomios S, M si son considerados coprimos tienen grado cero, lo cual equivale a que $S = \sigma$ y $M = \mu$, de donde se tiene además que $\sigma, \mu \in A((G\backslash\{g\}) \cup R_{m-1})$, esto es, σ, μ no hacen uso de la función g.

Definición de $\mathbf{h_j^*}$.

Requerimos definir h_j^* de forma que la función ϕ, la cual tiene por anulador el polinomio Q^*, sea solución de la ecuación de Riccati. Por otra parte, las funciones h_j junto con dicha ecuación, dan lugar al sistema 2.0.1. Definiremos h_j^*, de forma que se mantenga dicho sistema, o similar, y "volviendo hacia atrás", obtendremos que ϕ es solución de la ec. de Riccati.

Del sistema 2.0.2, dado que cada ecuación es en efecto suma de polinomios con Z como variable, considerar los coeficientes de Z^k con k arbitrario, obteniendo un sistema similar al sistema 2.0.1. Por otro lado, es natural definir h_j^* de forma que mantengan relación con h_j, así como sus derivadas entre sí.

Guiados por esta intuición nos disponemos a definir h_j^* por medio del coeficiente de Z^k de Q_j.

Recordamos:

$$Q_0(g) = h_0\,, \ldots,\ Q_p(g) = h_p,$$
$$H_0(g) = h_0', \ldots,\ H_p(g) = h_p'.$$

Nos tomamos la libertad de escribir $Q_j = c_0 Z^r + c_1 Z^{r-1} + ... + c_{r-1} Z + c_r$, en donde no aparece el subíndice j. Con esto:

$$H_j(g) = h'_j = (Q_j(g))' = \quad (c_r g^r + c_{r-1} g^{r-1} + ... + c_1 g + c_0)'.$$

Vemos que la g, hace presencia por medio de $\frac{\partial g}{\partial x}$, así distinguimos según sea $g = \int g_0$ o bien $g = e^{g_0}$ donde $g_0 \in M_m$.

Caso $\mathbf{g = \int g_0}$.

Para todo $s \in \mathbb{N}$, se verifica:

$$\frac{\partial g^s}{\partial x} = s(g^{s-1}) g_0.$$

Así:

$$H_j(g) = \frac{\partial c_r}{\partial x} g^r + (\frac{\partial c_{r-1}}{\partial x} + r c_r g_0) g^{r-1} + ... + (\frac{\partial c_1}{\partial x} + 2 c_2 g_0) g + (c_1 g_0 + \frac{\partial c_0}{\partial x}).$$

Vemos, que el único coeficiente c_k de Q_j que verifica que su derivada es el coeficiente k-ésimo de H_j, es c_r, el coeficiente de la potencia más grande.

Siendo q el grado de Q_0, por ser $grad(Q_0) \geq grad(Q_j) > grad(H_j) \, \forall j$ tenemos que de ser q igual a cero, así lo serán todos los Q_j, H_j, concluyéndose que ninguna de las funciones S, M, Q_j, H_j, dependen algebraicamente de g, caso que habíamos supuesto que no era (razonamiento posterior al sistema 2.0.1).

Siendo $q \geq 1$, definimos h_j^* como el coeficiente de Z^q en Q_j, y expresando en cada relación de 2.0.2, que el coeficiente de Z^q debe ser nulo, obtenemos el sistema:

$$(2.0.3) \qquad \begin{array}{rcl} \sigma[h_1^* + (h_0^*)'] - \mu h_{0^*} & = & 0, \\ \sigma[2h_2^* + p h_0^* f + (h_1^*)'] - \mu h_1^* & = & 0, \\ & \vdots & \\ \sigma[p h_p^* + 2 h_{p-2}^* f + (h_{p-1}^*)'] - \mu h_{p-1}^* & = & 0. \\ \sigma[h_{p-1}^* f + (h_p^*)'] - \mu h_p^* & = & 0. \end{array}$$

Caso $\mathbf{g = e^{g_0}}$.

Para todo $s \in \mathbb{N}$ se verifica:

$$\frac{\partial g^s}{\partial x} = s(g^s)g_0'.$$

Así:

$$H_j(g) = (\frac{\partial c_r}{\partial x} + c_r r g_0')g^r + (\frac{\partial c_{r-1}}{\partial x} + c_{r-1}(r-1)g_0')g^{r-1} + ... + (\frac{\partial c_1}{\partial x} + c_1 g_0)g + \frac{\partial c_0}{\partial x}.$$

Ahora, al contrario que antes, el único coeficiente c_k de Q_j que verifica que su derivada es el coeficiente k-ésimo de H_j, es c_0, el término independiente.

Definimos h_j^*, como el término independiente de Q_j, obteniendo de nuevo el sistema 2.0.3, aunque ahora con otro significado para h_j^*.

Notamos en ambos casos que $h_0^* \neq 0$.

En el primero, es consecuencia de ser el coeficiente de la potencia más grande de Q_0, el cual no es constante.

Notamos en el segundo caso que $h_0^* = 0$, pues en ese caso, de la primera ecuación del nuevo sistema, tenemos que $h_1^* = 0$ y descendiendo en el sistema llegaríamos a que en todos los h_j^*, el término independiente es cero, por lo que 0 es raíz de cada polinomio Q_j siendo por tanto $(Z - 0)$ divisor de común de Q_j, lo cual es absurdo.

Conclusión de: Definición de $\mathbf{h_j^*}$. Quedan definidas las funciones h_j^*, $j = 0, ..., p$, según sea $g \in G$. En ambos casos se verifica $h_0^* \neq 0$ y el sistema 2.0.3.

Última etapa.

Definimos el polinomio:

$$Q^* = h_0^* V^p + h_1^* V^{p-1} + ... + h_{p-1}^* V + h_0.$$

el cual es ciertamente de grado p.

Teníamos que de la identidad:

$$\sigma T = (\tau Y + \mu)Q,$$

deducíamos el sistema 2.0.1. El cual, salvo por la notación, coincide con 2.0.3 (τ, σ, μ son los mismos en ambas ecuaciones, así se tiene que la ecuación $p\sigma + \tau = 0$, sigue siendo cierta en el último sistema).

Dado que el sistema 2.0.1, es equivalente a $\sigma T = (\tau Y + \mu)Q$, en donde además $T = (-V^2 + f)\frac{\partial Q}{\partial V} + \frac{\partial Q}{\partial x}$, tenemos que el sistema 2.0.3, equivale con:

$$\sigma[(-V^2 + f)\frac{\partial Q^*}{\partial V} + \frac{\partial Q^*}{\partial x}] = (-p\sigma V + \mu)Q^*. \tag{2.0.4}$$

Sabemos que Q^* define una función $\phi \in H_{\Omega_0}$, con $\Omega_0 \subseteq A((G\backslash\{g\}) \cup R_{m-1})$, tal que Q^* es anulador de ϕ. Estamos ahora en condiciones de ver que ϕ es solución, concluyendo la demostración.

Sea r el primer orden de derivación tal que $\frac{\partial^r Q^*}{\partial V^r}(\phi) \neq 0$, el cual existe pues $\frac{\partial^p Q^*}{\partial V^p}(\phi) = p!h_0^* \neq 0$. Derivando $r-1$ veces en 2.0.4 y sustituyendo V por ϕ, llegamos a:

$$(-\phi^2 + f)\frac{\partial^r Q^*}{\partial V^r}(\phi) + \frac{p!}{(p-r+1)!}(h_0^*)'\phi^{p-r+1} + ... + (r-1)!(h_{p-r+1}^*)' = 0.$$

Por otra parte, derivando respecto de x en $\frac{\partial^{r-1} Q}{\partial V^{r-1}}(\phi) = 0$, obtenemos:

$$\frac{\partial^{r-1} Q}{\partial V^{r-1}}(\phi)\frac{\partial \phi}{\partial x} + \frac{\partial^{r-1} Q}{\partial x}\frac{\partial x}{\partial x} = \frac{\partial^{r-1} Q}{\partial V^{r-1}}(\phi)\phi' + \frac{p!}{(p-r+1)!}(h_0^*)' + ... + (r-1)!(h_{p-r+1}^*)' = 0.$$

Restando esta dos ecuaciones, concluimos que:

$$-\phi^2 + f - \phi' = 0,$$

de donde ϕ es solución de la ecuación de Riccati.

$\square$

A continuación presentamos el que será el último teorema. Pero antes recordar que un número complejo α es algebraico si es raíz de algún polinomio con coeficientes en $\mathbb{Z}$. En particular $\sqrt{2}$ es algebraico, mientras que π no lo es, y pese a nuestra intuición: la cantidad total de números algebraicos es numerable.

Teorema 2.0.3.
Si la ecuación de Riccati $y' + y^2 = 1 + t/x^2$ con $t \neq 0$ tiene alguna solución algebraica para algún valor del parámetro t, entonces este ha de ser un número algebraico.

Consecuentemente, por el teorema anterior, si t no es algebraico, la ecuación de Riccati no admite solución elemental.

DEMOSTRACIÓN. Sea ϕ solución algebraica de le ecuación de Riccati. Existen funciones polinómicas $h_0, ..., h_p$,i. e. , $h_i \in A(\{x\})$, sin divisores comunes y con h_0, h_p no idénticamente nulas, de modo que:

$$Q(\cdot,\phi) = h_0\phi^p + ... + h_{p-1}\phi + h_p = 0,$$

y p mínimo respecto a esta condición, esto es, $Q \in P(A(\{x\}))$ es polinomio anulador mínimo de ϕ.

Procedemos a obtener un sistema de forma similar a la del teorema anterior. Si denotamos por T al derivado de Q respecto de variable formal V, tenemos la expresión:

$$T = (-V^2 + f)\frac{\partial Q}{\partial V} + \frac{\partial Q}{\partial x},$$

en donde consideramos $f = 1 + t/x^2$. Ahora, al ser Q, T ambos anuladores de ϕ sobre el mismo anillo, con Q mínimo y coeficiente director unidad del anillo, existe $\kappa \in P(A(\{x\}))$ tal que:

$$T = \kappa Q,$$

y de la relación $grad(T) = grad(Q + 1)$, deducimos que $grad(\kappa) = 1$. Siendo el procedimiento análogo al del teorema anterior, realizamos la siguiente observación con tal de simplificar cálculos:

Si multiplicamos T por x^2 obtenemos la expresión:

$$Tx^2 = ([-V^2 + 1]\frac{\partial Q}{\partial V} + \frac{\partial Q}{\partial x})x^2 + t\frac{\partial Q}{\partial V},$$

así

$$Tx^2 = \tilde{\kappa}Q\,, \text{ con } \tilde{\kappa} = \tau V + \mu.$$

Podemos así obtener el nuevo sistema, sin más que identificar $\sigma = x^2$, tomar la función $f = 1$ y finalmente sumar el término correspondiente de $t\frac{\partial Q}{\partial V}$, el cual es, para la ecuación $j + 1$ del sistema: $th_j(p - j)$ (siempre que $j + 1$ tenga sentido). El sistema es:

$$\begin{aligned}
x^2[h_1 + h_0'] - \mu h_0 &= 0,\\
x^2[2h_2 + ph_0 + h_1'] - \mu h_1 + pth_0 &= 0,\\
x^2[3h_3 + (p-1)h_1 + h_2'] - \mu h_2 + (p-1)th_1 &= 0,\\
&\vdots\\
x^2[ph_{p-1} + 2h_{p-3} + h_{p-2}'] - \mu h_{p-2} + 3th_{p-3} &= 0,\\
x^2[ph_p + 2h_{p-2} + h_{p-1}'] - \mu h_{p-1} + 2th_{p-2} &= 0,\\
x^2[h_{p-1} + h_p'] - \mu h_p &= 0,
\end{aligned}$$

con $\mu \in A(\{x\})$.

Afirmamos que μ es de la forma: $\mu(x) = \alpha x^2 + \beta x$.

μ es divisible por x

De la primera ecuación deducimos que x^2 divide a μh_0, y si μno fuese divisible por x, tendríamos que x divide a h_0. Ahora, de la segunda ecuación x^2, debe dividir a μh_1 concluyendo de nuevo que x divide a h_1. Reiterando el proceso, obtenemos que x divide a h_i $i = 0, 1, ..., n$,lo cual es una contradicción con el hecho de no tener divisor común.

μ es de grado no mayor que 2

Si fuera μ de grado mayor, de la primera ecuación obtenemos la relación de grados:

$$grad(h_1) + 2 = grad(h_0) + grad(\mu) > grad(h_0) + 2,$$

de donde $grad(h_1) > grad(h_0)$.

Utilizando esto, la segunda ecuación nos da la relación:

$$grad(h_2) + 2 = grad(h_1) + grad(\mu),$$

obteniendo $grad(h_2) > grad(h_1)$.

Reiterando el proceso hasta la p-ésima ecuación (penúltima), obtendremos que $grad(h_p) > grad(h_{p-1})$, y finalmente de la última, $grad(h_p) > grad(h_{p-1})$, contradicción.

h_j es múltiplo de x^{p-j}

Siendo μ múltiplo de la última ecuación del sistema, tenemos dice que h_{p-1} es divisible por x. Con esto, de la penúltima obtenemos que h_{p-2} es divisible por x^2. Ahora h_{p-3} es de igual forma divisible por x^2, y para obtener el grado cúbico recurrimos a la divisibilidad por x de los anteriores $h_{p-1}, h_{p-2}, h_{p-3}$, de donde el paréntesis de esta ecuación nos da el grado requerido para la x (es claro que μh_{p-2} es divisible por x^3). Reiterando el proceso, obtenemos a lo largo del sistema que x^{p-j} divide a h_j para $j = 1, ..., p$.

Definimos $g_i = x^{-(p-i)}h_i$ $i = 0, ..., p$, y observamos que $x^{-(p-j-1)}h'_j = (p-j)x^{-(p-j)}h_j = (p-j)g_p$.
Si multiplicamos la primera ecuación por $x^{-(p+1)}$, tenemos:

$$x^{-(p+1)}x^2[h_1 + h'_0] - \mu x^{-(p+1)}h_0 = x^{-(p-1)}h_1 + x^{-(p-1)}h'_0 - (\alpha x + \beta)x^{-p}h_0 = 0,$$

o equivalentemente,

$$g_1 + (p-0)g_0 - (\alpha x + \beta)g_0 = 0.$$

De forma similar, si numeramos las ecuaciones de 0 a p y tomamos $0 < j < p$, multiplicando la ecuación j-ésima por $x^{-(p-j+1)}$:

$$\underbrace{x^{-(p-j+1)}x^2}_{x^{-(p-j-1)}}[ph_{j+1}+(p-j)h_{j-1}+h'_j]-(\alpha x+\beta)xx^{-(p-j+1)}h_j+(p-j)tx^{-(p-j+1)}h_{j-1}.$$

Expandiendo la expresión:

$$\underbrace{px^{-(p-(j+1))}h_{j+1}}_{pg_{j+1}}+(p-j)x^{-(p-j+1)}x^2h_{j-1}+\underbrace{x^{-(p-j-1)}h'_j}_{(p-j)g_j}-(\alpha x+\beta)\underbrace{x^{-(p-j)}h_j}_{g_j}+(p-j)tx^{-(p-j+1)}h_{j-1}.$$

Para el término h_{j-1}, tenemos:

$$(p-j)\underbrace{h_{j-1}x^{-(p-j+1)}}_{g_{j-1}}[t+x^2],$$

llegando finalmente a la ecuación:

$$pg_{j+1} + (p-j-\alpha x-\beta)g_j + (p-j)g_{j-1}(t+x^2) = 0.$$

Vemos que en el sistema aparecen dos paramentos indeterminados α y β, con tal de simplificar el estudio, tomamos $x = 0$ obteniendo el sistema:

$$\begin{aligned}
g_1(0) + (p-\beta)g_0(0) &= 0,\\
2g_2(0) + (p-1-\beta)g_1(0) + ptg_0(0) &= 0,\\
3g_3(0) + (p-2-\beta)g_2(0) + (p-1)tg_1(0) &= 0,\\
&\vdots\\
(p-1)g_{p-1}(0) + (2-\beta)g_{p-2}(0) + 3tg_{p-3}(0) &= 0,\\
pg_p(0) + (1-\beta)g_{p-1}(0) + 2tg_{p-2}(0) &= 0,\\
-\beta g_p(0) + tg_{p-1}(0) &= 0,
\end{aligned}$$

donde $g_p(0) = h_p(0) \neq 0$, ya que los polinomios $h_0, h_1, ..., h_p$, no tienen ningún divisor común. Por lo tanto, al ser no nulo el vector de C^{p+1}, tenemos:

$$(g_0(0), g_1(0), ..., g_{p-1}(0), g_p(0)),$$

e interpretando matricialmente el sistema homogéneo anterior con solución el vector de arriba, debe ser nulo el determinante de la matriz de coeficientes del sistema:

$$D(\beta,t) = \begin{vmatrix}
p-\beta & 0 & 0 & 0 & \dots & 0 & 0 & 0,\\
pt & p-1-\beta & 2 & 0 & & 0 & 0 & 0,\\
0 & (p-1)t & p-2-\beta & 3 & & 0 & 0 & 0,\\
0 & 0 & (p-2)t & p-3-\beta & \dots & 0 & 0 & 0,\\
\vdots & & \vdots & \vdots & & \vdots & & \vdots,\\
0 & 0 & 0 & 0 & \dots & 2t & 1-\beta & p,\\
0 & 0 & 0 & 0 & \dots & 0 & t & -\beta.
\end{vmatrix} = 0.$$

Con respecto a nuestro propósito, probar que t es algebraico, de la anterior relación vemos que es suficiente probar que el parámetro β es entero, pues en tal caso $D(\beta, x)$ es una relación polinómica en $\mathbb{Z}[x]$ tal que $D(\beta, t) = 0$.

Por otra parte, el sistema admite una lectura en el sentido vectorial siguiente: siendo

$q \geq p$ el grado máximo de $h_0, h_1, ..., h_p$, estas funciones pueden escribirse en columna construyendo un vector $\mathbf{h}$ de la forma:

$$\mathbf{h} = x^q v_0 + x^{q-1} v_1 + ... + x v_{q-1} + v_q,$$

donde $v_i \in C^{p+1}$ tiene en la entrada $(j+1)$-ésima el coeficiente de x^{q-i} en h_j. Con esto, si volvemos al sistema e identificamos los coeficientes de x^q, obetenemos un nuevo sistema homogéneo el cual viene dado por la expresión:

$$(A - \alpha) v_0 = 0, , \tag{2.0.5}$$

en donde

$$A = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 & 0, \\ p & 0 & 2 & \dots & 0 & 0, \\ 0 & (p-1) & 0 & \dots & 0 & 0, \\ \vdots & \vdots & \vdots & & \vdots & \vdots, \\ 0 & 0 & 0 & \dots & 0 & p, \\ 0 & 0 & 0 & \dots & 1 & 0. \end{pmatrix}$$

Para obtener la matriz anterior, es suficiente asociar la columna i-ésima al polinomio h_{i-1}, y la fila j-ésima a la ecuación j del sistema. Si bien el coeficiente de x^{q+2} de cualquier ecuación, es resultado del producto de x^2 o μ por un h_i, pues q es el grado máximo de los h_i $i = 1, ..., p$, dejamos a un lado para la construcción de A el factor α de μ, pues al estar presente en todas las ecuaciones, podemos simplificar la ecuación a la forma en que se encuentra 2.0.5. Entendemos aquí $\alpha = \alpha I_{p+1}$. Con esto, vemos que la segunda columna de A está formada por 1 en la primera entrada y $(p-1)$ en la tercera, ya que 1 es el coeficiente de $h_1 x^2$ en la primera ecuación del sistema y $(p-1)$ en la tercera.

De forma similar, al identificar los coeficientes de x^{q-1}, salvo con la diferencia de que ahora interviene tanto la derivada de los h_i, así como β, obtenemos la ecuación:

$$(A - \alpha) v_1 + (q - \beta) v_0 = 0. \tag{2.0.6}$$

Si denotamos por k a la multiplicidad algebraica de α en A, y por m a la geométrica, sabemos que $m \leq k$ y $Ker(A-\alpha) \subseteq Ker(A-\alpha)^2 \subseteq ... \subseteq Ker(A-\alpha)^{m-1} \subseteq Ker(A-\alpha)^m$ siendo m el menor valor tal que $Ker(A-\alpha)^m = Ker(A-\alpha)^n \; \forall n \geq m$.

La ecuación 2.0.5 significa que α es valor propio de A,y en el caso de que se trate de un valor propio simple se tendrá:

$$Ker(A-\alpha) = Ker(A-\alpha)^k \text{ para } k \geq 1,$$

de donde, haciendo actuar $A-\alpha$ sobre la ecuación 2.0.6 resultará:

$$(A-\alpha)^2 v_1 = 0,$$

por lo que $(A-\alpha)v_1$ es también nulo, quedando reducida la ecuación 2.0.6 a:

$$(\beta - q)v_0 = 0,$$

lo que implica $\beta = q$ pues $v_0 \neq 0$.

Visto que es suficiente para concluir el resultado, ver que el parámetro β es un número entero, lo cual se da en caso de ser α valor propio simple de A, probaremos que todos los valores propios de A son simples.

Siendo la matriz tridiagonal, su determinante no varía si cambiamos los pares de elementos $\{1,p\}, \{2,(p-1), ..., \{p,1\}$ $(a_{ij}, a_{ji}$ con $j = i+1)$ por otros cuyo producto sea el mismo, puede probarse fácilmente por inducción al desarrollarse por la primera columna, o bien de la propia definición de determinante. En particular, tomamos la raíz cuadrada del producto, esto es: $\{\sqrt{p}, \sqrt{p}\}, \{\sqrt{2(p-1)}, \sqrt{2(p-1)}\}$, ..., $\{\sqrt{p}, \sqrt{p}\}$, obteniendo la matriz simétrica, y, por tanto, diagonalizable:

$$B = \begin{pmatrix} 0 & \sqrt{p} & 0 & \dots & 0 & 0, \\ \sqrt{p} & 0 & 2 & \dots & 0 & 0, \\ 0 & (p-1) & 0 & \dots & 0 & 0, \\ \vdots & \vdots & \vdots & & \vdots & \vdots, \\ 0 & 0 & 0 & \dots & 0 & \sqrt{p}, \\ 0 & 0 & 0 & \dots & \sqrt{p} & 0. \end{pmatrix}$$

La matriz B tiene a α como valor propio y si denotamos por k a la multiplicidad de α es B, entonces k es la multiplicidad de α en A como valor propio (el recíproco sigue siendo cierto).

Notamos que rango de la matriz $B-\alpha$ es al menos p, ya que si eliminamos la primera fila y la última columna, obtenemos una submatriz triangular superior con ninguna estrada nula en la diagonal, luego con determinante no nulo. Por otro lado, $dim(Ker(B-\alpha)) = k$ por ser B diagonalizable. Juntando ambas identidades:

$$k = dim(Ker(B-\alpha)) = p+1-rang(B-\alpha) \leq p+1-p = 1,$$

lo que nos permite concluir $k=1$ siendo así α valor simple de A. □

OBSERVACIÓN. La función e^x así como las funciones trigonométricas e hiperbólicas no son algebraicas, además si f es algebraica entonces f^{-1} es algebraica, de donde la inversa de una función del tipo anterior no es algebraica.

DEMOSTRACIÓN. Si la función e^x fuera algebraica, tendríamos:

$$P_0(x)e^{nx} + P_1(x)e^{(n-1)x} + ... + P_{n-1}(x)e^x + P_n(x) = 0. \tag{2.0.7}$$

donde $P_0, ..., P_n$ son polinomios no todos nulos; denotamos por $d_0, ..., d_n$ a los grados respectivos de estos polinomios.

Ahora, consideramos la EDO lineal homogénea con coeficientes constantes de orden $d_0 + ... + d_n$ cuyo polinomio característico sea:

$$T(z) = (z-n)^{g_0} \cdot (z-(n-1))^{g_1} \cdot ... \cdot (z-0)^{g_n},$$

Del primer curso de ecuaciones diferenciales sabemos que si toda raíz λ del polinomio característico es real, siendo k su multiplicidad las funciones:

$$\{e^{\lambda x}, xe^{\lambda x}, x^2 e^{\lambda x}, ..., x^{k-1}e^{\lambda x} \text{ tal que } \lambda \text{ es raíz de } T(Z)\},$$

forman un sistema fundamental de soluciones para la EDO.

Tenemos así que las funciones (soluciones):

$$\begin{gathered} x^m e^{nx}, \quad m = 0, ..., g_0 - 1, \\ \vdots \\ x^m e^{0x} \quad m = 0, ..., g_n - 1, \end{gathered}$$

son linealmente independientes, contradiciendo la relación 2.0.7.

El resultado sigue siendo cierto para $sin(x)$, pues puede reducirse al caso anterior sin más que multiplicar por $(2i)^n e^{inx}$ en la expresión

$$P_0(x)(\frac{e^{ix}-e^{-ix}}{2i})^n+P_1(x)(\frac{e^{ix}-e^{-ix}}{2i})^{(n-1)}+...+P_{n-1}(x)(\frac{e^{ix}-e^{-ix}}{2i})+P_n(x)=0,$$

obtenemos una nueva relación en la que, sin más que intercambiar ix por x, nos aparece el caso anterior de la exponencial.
Para las funciones $cos(x),\ sinh(x),\ cosh(x)$ sirve el mismo razonamiento con sus respectivas formulas.

Si una función inyectiva f es algebraica con inversa g, podemos deducir que g es algebraica a partir de la expresión:

$$P_0(x)(f(x))^n + P_1(x)(f(x))^{n-1} + ... + P_{n-1}(x)f(x) + P_n(x) = 0,$$

pues reordenando en potencias de x, llegamos a la expresión:

$$H_0(f(x))\,x^m + H_1(f(x))\,x^{m-1} + ... + H_1(f(x))\,x^1 + H_m(f(x)) = 0,$$

de donde finalmente:

$$H_0(y)\,g(y)^m + H_1(y)\,g(y)^{m-1} + ... + H_1(y)\,g(y)^1 + H_m(y) = 0,$$

Podemos concluir ahora, la observación para la función tangente: de ser la función $tan(x)$ algebraica, así lo sería: $(cos^2(x))^{-1} = 1 + tan(x)^2$ de donde $cos^2(x)$ sería algebraica y, por tanto, $sin^2(x) = 1 - cos^2(x)$ concluyendo que $cos(2x) = cos^2(x) - sin^2(x)$ es algebraica, lo cual es falso. □

OBSERVACIÓN. Si f y g son funciones elementales, entonces $f \circ g$ es elemental.

DEMOSTRACIÓN. Resaltar que si f es constante, así lo es $g \circ f \in A^*(\{x\})$. Podemos suponer que $f \in R_m$ es no constante.

Para demostrar que $g \circ f \in \cup_{n\geq 0} R_n$, $g \circ f$ es elemental, razonamos por inducción sobre el índice n tal que $g \in R_n$.

Para $g \in R_0 = A^*(\{x\})$, es cierto que $g \circ f$ depende algebraicamente de $\{f\}$, y por el carácter transitivo de la dependencia algebraica, concluimos que $g \circ f \in R_m$.

Supuesto cierto para todo $h \in R_{n-1}\ :\ h \circ f \in \cup_{k\geq 0} R_k$, veámoslo ahora para n.

Siendo $g \in R_n$, g depende algebraicamente de un subconjunto finito F de $R_{n-1} \cup M_n$, en el que además, las funciones de F que están en M_n son integrales o primitivas de funciones de R_{n-1}. Definimos el conjunto:

$$F_0 = \{h \in R_{n-1} \,/\, h \in F : \int h \in F \text{ o bién } e^h \in F\},$$

Por hipótesis de inducción, $h \circ f \in \cup_{k\geq 0} R_k\ \forall h \in F_0$ pudiéndose considerar el índice:

$$r := máx_{h\in F_0}\{p\ :\ h \circ f \in R_p\}.$$

Ahora, dada la estabilidad de R_m bajo derivación, $f' \in R_m$ de modo que si $h \in F_0$ es tal que $\int f \in F$, tenemos:

$$(\int h) \circ f = \int (h \circ f) f' \in M_{q+1} \text{ con } q = máx\{r, m\},$$

y si $h \in F_0$ es del tipo $e^h \in F$, entonces:

$$e^h \circ f = e^{h \circ f} \in M_{r+1}.$$

Concluimos que $G = \{\phi \circ F \,/\, \phi \in F\} \subset R_{q+1}$, y dado que la dependencia algebraica de g respecto de F implica la de $g \circ f$ respecto de G, por la transitividad de la dependencia algebraica, concluimos que $g \circ f \in R_{q+1}$ como deseábamos. $\square$