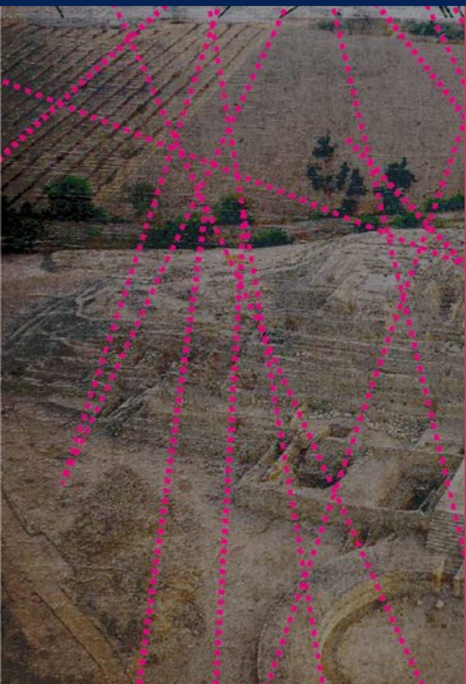
Capítulo 2



Editores

VIII Escuela Doctoral Intercontinental de Matemáticas PUCP-UVA 2015

CIMPA RESEARCH SCHOOL

BIBLIOTECA NACIONAL DEL PERÚ
Centro Bibliográfico Nacional

512.0072 VIII Escuela doctoral intercontinental de matemáticas PUCP-UVA 2015:
E CIMPA research school / Francisco Ugarte Guerra, Nuria Corral Pérez, editores.-- 1a ed.-- Lima: Pontificia Universidad Católica del Perú, Fondo Editorial, 2016 (Lima: Tarea Asociación Gráfica Educativa).
244 p.; il., retrs.; 21 cm.

Incluye bibliografías.

D.L. 2016-12927
ISBN 978-612-317-203-9

1. Algebra - Estudio y enseñanza 2. Teoría de los números 3. Teoría de Galois 4. Teoría de los grupos 5. Ecuaciones diferenciales I. Ugarte Guerra, Francisco, 1972-, editor II. Corral Pérez, Nuria, editora III. Pontificia Universidad Católica del Perú

BNP: 2016-1193

VIII Escuela Doctoral Intercontinental de Matemáticas PUCP-UVA 2015
Francisco Ugarte Guerra y Nuria Corral Pérez, editores

Av. Universitaria 1801, Lima 32, Perú
feditor@pucp.edu.pe
www.fondoeditorial.pucp.edu.pe

Corrección de estilo y cuidado de la edición: Fondo Editorial PUCP
Diseño de cubierta: Francisco Ugarte

Primera edición: octubre de 2016
Tiraje: 500 ejemplares

Hecho el Depósito Legal en la Biblioteca Nacional del Perú Nº 2016-12927
ISBN: 978-612-317-203-9
Registro del Proyecto Editorial: 31501361601055

Impreso en Tarea Asociación Gráfica Educativa
Pasaje María Auxiliadora 156, Lima 5, Perú

El grupoide de Galois de una transformación racional

Guy Casale

DEPARTMENT OF MATHEMATICS, IRMAR, UNIVERSITÉ DE RENNES 1,
35042 RENNES CEDEX, FRANCE

E-mail address: guy.casale@univ-rennes1.fr

Índice

1 Introducción

Este curso tiene dos objetivos:

1. En primer lugar, definir el grupoide de Galois de una transformación racional:

$$\begin{aligned} f : \mathbb{C}^n &\dashrightarrow \mathbb{C}^n \\ (z_1, \ldots, z_n) &\mapsto (f_1(z), \ldots, f_n(z)) \end{aligned}$$

   con $f_i \in \mathbb{C}(z_1, \ldots z_n)$ tal que $\det Jac(f) \not\equiv 0$.

   Cuando f está dada por funciones lineales con respecto a $z_1, \ldots, z_n$, existe una teoría de Galois casi-completa (con una correspondencía de Galois ...). Se puede leer esta teoría en [15]. Para generalizar la definición a una transformación no lineal, necesitamos introducir un grupoide (más precisamente un pseudogrupo) siguiendo a B. Malgrange [10].

2. En segundo lugar, describir completamente el caso $n = 1$ para probar un teorema de Ritt sobre la trascendencia diferencial de la dinámica de f.

La prueba de Ritt utiliza la teoría de eliminación en los anillos de ecuaciones diferenciales. Nuestra demostración reemplaza la eliminación por argumentos de teoría de grupos.

1.1 El teorema de Ritt

El libro de J. Milnor [13] es nuestra referencia para los resultados de dinámica holomorfa en dimensión uno. Un teorema de Koenigs [13, capítulo 8] dice que si $f : \mathbb{C} \dashrightarrow \mathbb{C}$ tiene un punto fijo z_0 tal que $|f'(z_0)| > 1$ entonces existe $h \in \mathbb{C}\{w\}$ con $h(0) = z_0$ y $h'(0) = 1$ tal que $h^{-1} \circ f \circ h(w) = \lambda w$.

La construcción de la linealización h se hace por medio del límite de una sucesión de funciones holomorfas. Por eso podemos pensar que, generalmente, la linealización es trascendental. La linealización de un monomio $f(z) = z^k$ en el punto fijo $z_0 = 1$ es $h(w) = e^w$; los monomios son ejemplos de sistemas dinámicos con una linealización trascendental pero diferencialmente algebraica. El teorema de Ritt dice que no hay muchos más ejemplos de este tipo.

Definición 1. Una función holomorfa $f : U \to \mathbb{C}$ sobre un abierto U es *diferencialmente algebraica* si existe una ecuación diferencial $E \in \mathbb{C}[z, y, y', \ldots y^{(n)} \ldots]$ tal que

$$E(z, f(z), f'(z), \ldots, f^{(n)}(z)) = 0 \text{ sobre } U.$$

Una función que no es diferencialmente algebraica es *diferencialmente trascendental.*

Teorema 2 (Ritt [18]). *Si* $f : \mathbb{C} \dashrightarrow \mathbb{C}$ *tiene un punto fijo* z_0 *tal que* $|f'(z_0)| > 1$ *y su linealización* h *satisface una ecuación diferencial polinomial, entonces* f *es:*

- *una homografía*
- *o un monomio*
- *o un Chebyshev* [1]
- *o un Lattès* [2]

en una buena coordenada homográfica sobre $\mathbb{C}$.

La prueba la realizaremos será de la siguiente manera:

1. Daremos la definición del grupoide de Galois de una transformación f.
2. Probaremos que las transformaciones f con un grupoide "pequeño" están en la lista de Ritt .
3. Si f satisface las hipótesis de Ritt entonces su grupoide es "pequeño" .

Este lista aparece en otros teorema de Ritt ([17, 19])

1.2 Las ecuaciones en diferencias

Otra interpretación de este teorema es la siguiente.

Sean $f \in \mathbb{C}(z)$ y $\lambda \in \mathbb{C}$ con $|\lambda| > 1$. Si existe una solución meromorfa sobre $\mathbb{C}$ de la ecuación en diferencias multiplicativa $y(\lambda w) = f(y(w))$ que satisface una ecuación diferencial, entonces f está en la lista de Ritt. Para éstos f, la solución y está dada por funciones clásicas: $\exp(aw^k + b), \cos(aw^k + b), \mathcal{P}(aw^k + b)$ u otras funciones elípticas.

Desde este punto de vista, estamos mirando a las funciones que son soluciones de una ecuación diferencial y de una ecuación en diferencias. Las funciones que satisfacen ecuaciones diferenciales y en diferencias lineales son estudiadas de manera analítica en [16] y de manera muy diferente en [8] donde se hace uso de la teoría de Galois.

[1] 16 de Mayo de 1821 - 8 de diciembre de 1894, fue un matemático ruso. `https://es.wikipedia.org/wiki/Pafnuti_Chebyshov`

[2] 21 de Febrero de 1873 - 5 de julio de 1918, fue un matemático francès `https://de.wikipedia.org/wiki/Samuel_Lattès` y [1]

1.3 Otro teorema de tipo "Ritt"

Un teorema similar de Bergweiler-Aschenbrenner [4] puede demostrarse de manera análoga. Si $f : \mathbb{C} \dashrightarrow \mathbb{C}$ tiene un punto fijo z_0 tal que $f'(z_0) = 1$, entonces existe $k \in \mathbb{N}$, $c \in \mathbb{C}$ y $h \in \mathbb{C}[[z]]$ tal que $h^{-1} \circ f \circ h = \exp\left(\frac{z^{k+1}}{1-cz^k}\frac{d}{dz}\right)$ (ver [11, chap. I §§1,2]).

Teorema 3. *No existe $f : \mathbb{C} \dashrightarrow \mathbb{C}$ con un punto fijo z_0 tal que $f'(z_0) = 1$ y su normalización formal h satisfaga una ecuación diferencial.*

La organización del curso es la siguiente:

1. El ejemplo de una aplicación lineal.
2. El ejemplo de una aplicación lineal en las $n-1$ coordenadas últimas.
3. La definición del grupoide (o pseudogrupo) de Galois de f.
4. Los pseudogrupos en dimensión $n = 1$.
5. El pseudogrupo de Galois de f en dimensión $n = 1$.
6. El teorema de Ritt.

1.4 Agradecimientos

Quiero dar las gracias a Jesus David Piñeda Escobar para la ayudad a escribir las notas del curso en español. Muchas gracias a Nuria Corral y Francisco Ugarte para la organización de la escuela CIMPA "Transformation Groups and Dynamical Systems".

2 Transformaciones lineales y grupos algebraicos

Una transformación lineal es un elemento de un grupo, este último será utilizado para simplificar la definición general de grupoide de Galois, no obstante, esta simplificación es muy fuerte y muchas cosas parecerán artificiales.

Definición 4. Sean E un espacio vectorial y $A \in GL(E)$ una aplicación lineal invertible. La envolvente algebraica ("enveloppe" en francés) de A es el subgrupo algebraico minimal $G_A \subset GL(E)$ tal que $A \in G_A$.

Es posible leer una introducción sobre los aspectos básicos de los grupos algebraicos lineales en [6] o resultados más complejos en [9]. Aunque existe una amplia literatura acerca de grupos algebraicos, daremos una breve introducción.

2.1 Grupos algebraicos lineales

En adelante consideraremos conjuntos algebraicos sobre el cuerpo de los números complejos. El espacio $\mathbb{C}^n$ posee un álgebra de funciones polinomiales $\mathbb{C}[X_1, \ldots, X_n]$ con muy buenas propiedades, es por esto que le llamamos un conjunto algebraico o una variedad algebraica.
Podemos construir otros conjuntos algebraicos utilizando un ideal de polinomios $I \subset \mathbb{C}[X_1, \ldots, X_n]$. El conjunto $V_I = \{x \in \mathbb{C}^n \mid f(x) = 0 \text{ para todo } f \in I\}$ es un conjunto algebraico con álgebra de funciones polinomiales $\mathbb{C}[V] = \mathbb{C}[X_1, \ldots, X_n]/\sqrt{I}$. Una variedad algebraica es un objeto un poco más general pero no vamos a utilizarlas.

El conjunto algebraico minimal que contiene un subconjunto C de una variedad algebraica V se llama la clausura de Zariski de C o la clausura algebraica de C, se escribe $\overline{C}$. Un abierto de Zariski es el complementario de un conjunto algebraico.

El conjunto $GL_n(\mathbb{C})$ es un conjunto algebraico. Podemos verlo como el subconjunto de $\mathbb{C}^{n^2+1}$ de los ceros del polinomio $P(X_1^1, \ldots, X_n^n, t) = t \det X - 1$. Su álgebra de funciones es $\mathbb{C}[X_1^1, \ldots, X_n^n, \frac{1}{\det X}]$. El conjunto $GL_n(\mathbb{C})$ es también un grupo y las dos estructuras son compatibles: Si $g \mapsto P(g)$ es una función polinomial entonces

- $(g_1, g_2) \mapsto P(g_1 g_2)$ es una función polinomial sobre $GL_n \times GL_n$,
- $g \mapsto P(g^{-1})$ es una función polinomial sobre GL_n.

Definición 5. Un subgrupo $G \subset GL_n$ que es un conjunto algebraico es un subgrupo algebraico.

Ejercicio 6. Comparar con la definición del curso del Pr. Aroca y probar que las dos definiciones son compatibles.

Ejercicio 7. Probar que si $G \subset GL(E)$ es un subgrupo, entonces $\overline{G}$ es un grupo algebraico.

Ejemplo 8. El subgrupo $SL_n \subset GL_n$ es algebraico.
El grupo de las matrices triangulares superiores U_n es algebraico.

En general, si E es un espacio vectorial, podemos elegir una base $e_1, \dots, e_n$ y el isomorfismo $e : \mathbb{C}^n \to E$ determina un isomorfismo de $GL_n \to GL(E)$ que hace de $GL(E)$ un grupo algebraico. Entonces podemos definir sus subgrupos algebraicos. Casi todos los teoremas básicos e importantes sobre grupos algebraicos se prueban utilizando la acción del grupo sobre $\mathbb{C}[GL(E)]$ por traslaciones. Para $g \in GL(E)$, escribiremos $T_g : g' \mapsto g'g$ para denotar la traslación y $T_g^* : \mathbb{C}[GL(E)] \to \mathbb{C}[GL(E)]\ ;\ P \mapsto P \circ T_g$.

Definición 9. Un invariante (resp. invariante racional) de $g \in GL(E)$ es una función $H \in \mathbb{C}[GL(E)]$, (resp. $H \in \mathbb{C}(GL(E))$) tal que $H = H \circ T_g$. Un invariante de un subgrupo G de $GL(E)$ es un invariante común a todos los elementos de G.

El siguiente es el teorema más importante para este curso, es un teorema de Kolchin y Chevalley pero realizaremos una prueba de J. Drach [7, §§16 – 19 pp 466 – 474].

Teorema 10 ([5])**.** *Si $G \subset GL(E)$ es un grupo algebraico, entonces existen $H_1, \dots, H_p \in \mathbb{C}(GL(E))$ en el cuerpo de funciones racionales tales que*

$$G = \{g \in GL(E) \mid H_i = H_i \circ T_g \text{ para todo } i\}.$$

Demostración. – Tenemos una acción lineal de G por $T_g^* : \mathbb{C}[GL(E)] \to \mathbb{C}[GL(E)]$. Utilizaremos algunos lemas sobre esta acción.

Lema 11. *El subespacio vectorial $I \subset \mathbb{C}[GL(E)]$ de las funciones que se anulan sobre G es estable por G.*

Ejercicio 12. Probar el lema precedente.

Ahora tenemos que el grupo

$$G = \{g \in GL(E) \mid T_g^*(I) \subset I\},$$

es el estabilizador de un subespacio vectorial I de $\mathbb{C}[GL(E)]$. El problema es que tenemos dos espacios vectoriales de dimensión infinita y para construir invariantes necesitamos espacios de dimensión finita. Vamos a construirlos.

Sean $F_1, \dots, F_p$ generadores linealmente independientes del ideal I. Dado que $F_i(gg')$ es un polinomio,

$$\text{para todo } (g, g') \in GL(E) \times GL(E) \quad \text{se tiene} \quad F_i(gg') = \sum_{j=1}^{n} D_i^j(g')B_j(g),$$

para funciones D y B en $\mathbb{C}[GL(E)]$. Esta suma no es única, escribimos una suma con un número minimal de términos y $F_i = B_i$ para $i \leq p$.

Lema 13. *En virtud de la minimalidad del número de términos, los B_j para $j = 1, \dots, n$ son linealmente independientes y las columnas $(D_i^j)_i$ para $j = 1, \dots, n$ también.*

Ejercicio 14. Probar el lema precedente.

Sea V el espacio vectorial sobre $\mathbb{C}$ generado por los B_i, probaremos que V es estable por $GL(E)$. Tenemos

$$B_j(gg') = \sum_k \widetilde{D}_j^k(g')B_k(g) + \sum_\ell A_j^\ell(g')C_\ell(g)$$

con los B y C linealmente independientes. Las dos fórmulas y la asociatividad dan:

$$\sum_j D_i^j(g'g'')B_j(g) = F_i(gg'g'') = \sum_j D_i^j(g'')B_j(gg')$$

$$\sum_j D_i^j(g'g'')B_j(g) = \sum_j \widetilde{D}_i^j(g'') \left(\sum_k \widetilde{D}_j^k(g')B_k(g) + \sum_\ell A_j^\ell(g')C_\ell(g) \right)$$

Por la independencia de los B y C tenemos $\sum_{j,\ell} \widetilde{D}_i^j(g'')A_j^\ell(g')C_\ell(g) = 0$. En virtud del lema anterior tenemos que las columnas $(\widetilde{D}_i^j)_j$ son independientes, entonces $\sum_\ell A_j^\ell(g')C_\ell(g)$ son cero, para cada j. Tenemos un espacio de dimensión finita de V estable por T_g^* para cada $g \in GL(E)$. El subespacio $V \cap I$ es un subespacio estable de dimensión q, entonces

$$G = \{g \in GL(E) \mid T_g^*|_V(V \cap I) \subset V \cap I\}.$$

Ahora elegimos una base de V tal que los q primeros vectores sean una base de $V \cap I$. Definimos n^2 funciones $\widetilde{D}_j^k$ sobre $GL(E)$ por las fórmulas de arriba. Un elemento g está en G si y solo si la traslación T_q preserva las funciones $F_{K,L}$ siguientes:

$$\text{para } K \subset \{1, \dots, n\}, L \subset \{1, \dots, n\}, \#K = \#L = n - q :$$

$$F_{K,L} = \frac{\det(\widetilde{D}_j^k)_{\substack{j=q+1,\dots n \\ k \in K}}}{\det(\widetilde{D}_j^k)_{\substack{j=q+1,\dots n \\ k \in L}}}$$

□

Nota 15. En la prueba utilizamos las buenas propiedades del producto tensorial sobre un cuerpo.

2.2 La envolvente algebraica

Para entender una aplicación lineal A podemos estudiar el grupo algebraico generado por A.

Definición 16. La envolvente algebraica de $A \in GL(E)$ es el grupo algebraico minimal G_A que contiene A.

Lema 17. *El conjunto algebraico minimal que contiene todos los A^n para $n \in \mathbb{Z}$ es G_A.*

Ejercicio 18. Probar el lema precedente.

Lema 19. *La envolvente algebraica de A es el grupo de los elementos que preservan los invariantes racionales de A.*

Ejercicio 20. Probar el lema precedente.

2.3 Los grupos de Galois de A

Para entender una aplicación lineal A podemos estudiar su prolongación sobre espacios más grandes. El conjunto de todas las bases de E es un conjunto algebraico

$$BE = \{e = (e_1, \ldots, e_n) \in E^n | e_1 \wedge \ldots \wedge e_n \neq 0\}$$

con

- una acción de $g \in GL_n$, $T_g : (e_1, \ldots, e_n) \mapsto (e_1, \ldots, e_n)g$,
- una acción de $A : (e_1, \ldots, e_n) \mapsto (Ae_1, \ldots, Ae_n)$

que conmutan. Elegimos una base e y miramos su órbita $O(e) = \{A^n e, n \in \mathbb{Z}\}$ y su clausura algebraica $\overline{O(e)}$.

Definición 21. El estabilizador de $\overline{O(e)}$ en GL_n es $Gal(A, e)$, el grupo de Galois de A en e.

Lema 22. *$\overline{O(eg)} = T_g(\overline{O(e)})$ y $Gal(A, eg) = gGal(A, e)g^{-1}$.*

Ejercicio 23. Probar el lema precedente.

2.4 Comparación

Si $E = \mathbb{C}^n$ y $e = identidad$ entonces $Gal(A, e) = G_A = \overline{O(e)}$.

La envolvente G_A actúa a la izquierda sobre todos los $\overline{O(e)}$ para cualquier $e \in BE$. El grupo de Galois $Gal(A, e)$ actúa a la derecha sobre la subvariedad $\overline{O(e)}$. La envolvente es intrínseca pero se necesita poner A dentro de un grupo con una topología para definirla. El grupo de Galois depende de una base pero solo necesitamos una acción de A sobre un espacio suficientemente grande para "desarollar" la dinámica de A.

2.5 Ejercicios

Ejercicio 24. Sea $G \subset GL(E)$ un subgrupo conmutativo. Probar que $\overline{G}$ es conmutativo. Deducir que para $A \in GL(E)$, G_A es conmutativo.

Ejercicio 25. Dar los grupos algebraicos generados por

$$A = \begin{bmatrix} \lambda & 1 \\ 0 & \lambda \end{bmatrix} \qquad \text{o} \qquad A = \begin{bmatrix} \lambda & 0 \\ 0 & \mu \end{bmatrix}.$$

3 Ecuaciones en diferencias lineales

La recta compleja $\mathbb{C}$ será denotada por L. Para una aplicación racional $A : L \dashrightarrow GL(E)$ nos interesa la transformación

$$\begin{aligned} f_A : L \times E &\dashrightarrow L \times E \\ (z, x) &\mapsto (z + 1, A(z)x) \end{aligned}$$

Podemos pensar en cambiar de cuerpo y proceder de manera análoga al caso lineal con $A \in GL(E \otimes \mathbb{C}(z))$. Pero $f_A \circ f_A \neq f_{A^2}$, por eso no es fácil dotar a $GL(E \otimes \mathbb{C}(z))$ de una estructura de grupo compatible con f, salvo en el caso constante $A \in GL(E)$. Es más fácil definir los grupos de Galois.

Tradicionalmente se escriben las ecuaciones de las aplicaciones $Y : L \to E$ con grafo invariante por f_A :

$$Y(z + 1) = A(z)Y(z)$$

y los grupos de Galois son los grupos de Galois del sistema de ecuaciones en diferencias de [15]. Estos se definen de manera análoga al caso constante pero la definición de la envolvente necesita colocar f_A dentro de un grupoide.

3.1 Los grupos de Galois

Como en el caso constante, estudiamos la acción de f_A sobre las bases de E :

$$\begin{aligned} f_A : L \times BE &\dashrightarrow L \times BE \\ (z, e) &\mapsto (z+1, A(z)e) \end{aligned}.$$

Aún tenemos la acción de GL_n a la derecha que conmuta con f_A.

Elegimos un punto z_0, una base e_0 y $V(z_0, e_0)$ será el conjunto algebraico minimal de $L \times BE$ tal que:

- $(z_0, e_0) \in V(z_0, e_0)$,
- $f_A(V(z_0, e_0)) \subset V(z_0, e_0)$,
- $pr_1(V(z_0, e_0))$ es un abierto de L.

Básicamente la minimalidad y las dos primeros condiciones significan que miramos a la clausura de Zariski de la órbita de (z_0, e_0). La tercera significa que esta órbita no se encuentra con el espacio de indeterminación de f_A.

Definición 26. El estabilizador de $V(z_0, e_0)$ en GL_n es el grupo de Galois de f_A en e_0: $Gal(f_A, e_0)$.

3.2 La envolvente algebraica

Podemos definir la envolvente algebraica, pero no en un grupo sino dentro en un grupoide. El grupoide es $\mathcal{G}r = L \times GL(E) \times L$. La composición es $(z_1, g, z_2)(z_2, h, z_3) = (z_1, gh, z_3)$ y es compatible con las álgebras de funciones polinomiales. Por lo tanto es un grupoide algebraico.

Ejercicio 27. Probar que $\{(z_1, g, z_2) \in L \times GL_1(\mathbb{C}) \times L \mid z_1 g = z_2\}$ es un subgrupoide algebraico.

La transformación f_A da muchos elementos de este grupoide: para cada $z \in L$ tal que $A(z)$ existe, tenemos $A_z = (z+1, A(z), z) \in \mathcal{G}r$. Podemos intentar una definición análoga a la definición 16.

Definición 28 (mala)**.** La envolvente de A, $\mathcal{G}_A$, es el subgrupoide algebraico minimal tal que $A_z \in \mathcal{G}_A$ para todo $z \in L$.

Sobre ejemplos podemos ver que este objeto es bastante grande.

Definición 29 (buena)**.** La envolvente de A, $\mathcal{G}_A$, es el conjunto algebraico minimal tal que

- para todo $z \in dom(A) \subset L$ el dominio de A, $A_z \in \mathcal{G}_A$,
- existe $U \subset L$ un abierto de Zariski tal que $\mathcal{G}_A|_{U \times U}$ es un grupoide algebraico.

Tenemos teoremas análogos a los dos lemas de la parte 2.2.

Teorema 30. *$\mathcal{G}_A$ es la clausura de Zariski del conjunto*

$$\{(z, \prod_{i=0}^{n-1} A(z+i), z+n), n \in \mathbb{N}, z \in L^\circ\} \cup \{(z, Id, z), z \in L\} \cup$$

$$\{(z+n, \prod_{i=0}^{n-1} A^{-1}(z+n-1-i), z), n \in \mathbb{N}, z \in L^\circ\}.$$

siendo L° un subconjunto de L donde las fórmulas tienen sentido.

Definición 31. Un invariante racional de f_A es un $H \in \mathbb{C}(L \times BE)$ tal que $H \circ f_A = H$. El cuerpo de los invariantes de f_A será $Inv(A) \subset \mathbb{C}(L \times BE)$.

Teorema 32. *La envolvente de f_A está dada por sus invariantes:*

$$\mathcal{G}_A = \{(z_1, g, z_2) \in \mathcal{G}r \mid H(z_2, e) = H(z_1, g(e)) \text{ para todo } H \in Inv(A)\}.$$

Las pruebas de estos dos teoremas son difíciles y no son más fáciles que sus versiones no lineales, entonces no vamos a hacerles aquí.

3.3 Ejercicios

Ejercicio 33. Si $A : \mathbb{C} \dashrightarrow \mathbb{C}^*; z \to z$ y $f_A(z,x) = (z+1, zx)$.

Probar $Gal(T_A, e) = \mathbb{C}^*$.

Indicación: la ecuación en diferencias $y(z+1) = zy(z)$, es la ecuación de la función Γ. Calcular el grupo de Galois es equivalente a probar que Γ no es una función algebraica.

4 Los referentes y los invariantes diferenciales

Ahora queremos definir la envolvente algebraica de una aplicación racional $f : M \dashrightarrow M$. Necesitamos introducir los objetos que reemplazarán las bases de E: los referentes. Son versiones no lineales de los referentes móviles de E. Cartan.

Definición 34.

- Un referente $p \in M$ es un germen de coordenadas locales holomorfas: $r : (\mathbb{C}^n, 0) \to (M, p)$ invertible en 0.
- Un referente de orden k es el jet de orden k, $j_k(r)$, de un referente r.
- El conjunto de todos los referentes de orden k es una variedad algebraica R_kM.

Se puede escribir un referente como n series de potencias. Si $(t_1, \dots, t_n)$ son coordenadas sobre $\mathbb{C}^n$ y $(z_1, \dots, z_n)$ son coordenadas sobre M entonces un referente r se escribe $r(t) = (r_1(t), \dots, r_n(t))$ donde

$$r_i(t) = \sum_{\alpha \in \mathbb{N}^n} \partial^\alpha r_i(0) \frac{t^\alpha}{\alpha!}.$$

Su jet de orden k es

$$j_k r_i = \sum_{\substack{\alpha \in \mathbb{N}^n \\ |\alpha| \leq k}} \partial^\alpha r_i(0) \frac{t^\alpha}{\alpha!}.$$

Entonces el anillo de funciones polinomiales sobre R_kM es

$$\mathbb{C}[R_kM] = \mathbb{C}\left[z_i^\alpha | 1 \leq i \leq n, \alpha \in \mathbb{N}^n, |\alpha| \leq k\right] \left[\frac{1}{\det z_i^{\epsilon_j}}\right]$$

con

$$z_i^\alpha(j_k r) = \partial^\alpha r_i(0).$$

Definición 35. El conjunto de los referentes formales es $RM = \lim\limits_{\leftarrow} R_kM$. Un referente formal $\widehat{r}$ está dado, en coordenadas locales, por n series de potencias $(\widehat{r}_1(t), \dots \widehat{r}_n(t))$ pero sin ninguna condición de convergencia.

El espacio RM tiene muchas propiedades buenas que vamos a definir.

4.1 R_kM es un espacio natural

Significa que si $\varphi : U \to V$ es un biholomorfismo local entre abiertos de M entonces tenemos $R_k\varphi : R_kU \to R_kV$ un biholomorfismo local canónico entre el abierto de los referentes en U y el de los referentes en V definido por

$$R_k\varphi(j_k r) = j_k(\varphi \circ r_k).$$

La asociatividad de la composición da $R_k(\varphi_1 \circ \varphi_2) = R_r\varphi_1 \circ R_k\varphi_2$. En particular, f actúa sobre R_kM. La elevación $R\varphi$ de un biholomorphismo local φ se llama la prolongación de φ al espacio de los referentes.

Podemos también prolongar los campos de vectores: si X es un campo de vectores sobre M con flujo $\exp(\epsilon X)$ entonces R_kX es el generador infinitesimal de la familia $R_k(\exp(\epsilon X))$ para pequeños ϵ. Esta prolongación es compatible con el paréntesis de Lie $R_k[X_1, X_2] = [R_kX_1, R_kX_2]$.

4.2 R_kM es un fibrado principal

El grupo de cambio de coordenadas sobre $(\mathbb{C}^n, 0)$ actúa sobre los referentes.

Definición 36. El grupo $\Gamma_k = \{j_k\gamma \mid \gamma : (\mathbb{C}^n, 0) \to (\mathbb{C}^n, 0) \text{ invertible}\}$ es un grupo algebraico.

Ejercicio 37. Probar que Γ_k es un subgrupo algebraico de $GL(E)$ donde E es el espacio vectorial de los jets de orden k de funciones holomorfas sobre $(\mathbb{C}^n, 0)$.

Este grupo actúa sobre R_kM : si $j_k\gamma \in \Gamma_k$, $T_{j_k\gamma}(j_kr) = j_k(r \circ \gamma)$ y la acción satisface que

$$\begin{gathered} R_kM \times \Gamma_k \to R_kM \underset{M}{\times} R_kM \\ (j_kr, j_k\gamma) \mapsto (j_kr, T_{j_k\gamma}j_kr) \end{gathered}$$

es un isomorfismo de variedades algebraicas.

Lema 38. *Las aplicaciones $T_{j_k\gamma}$ y $R_k\varphi$ conmutan.*

Ejercicio 39. Probar el lema precedente.

4.3 $\mathbb{C}[RM]$ es un álgebra diferencial

El anillo de funciones sobre RM es

$$\varinjlim \mathbb{C}[R_kM] = \mathbb{C}\left[z_i^\alpha | 1 \le i \le n, \alpha \in \mathbb{N}^n\right] \left[\frac{1}{\det jac}\right].$$

Los operadores $\partial_i = \sum_{j,\alpha} z_j^{\alpha+\epsilon(i)} \frac{\partial}{\partial z_j^\alpha}$, donde $\epsilon(i) = (0\ldots, 1, \ldots 0)$ es el multiíndice cuya única componente no nula es la i-esima, actúan sobre $\mathbb{C}[RM]$ como derivaciones :

$$\partial_i(P + Q) = \partial_i(P) + \partial_i(Q) \quad , \quad \partial_i(PQ) = \partial_i(P)Q + P\partial_i(Q).$$

Además satisfacen

$$\partial_i \circ (R_k\varphi)^* = (R_{k+1}\varphi)^* \circ \partial_i.$$

4.4 RM tiene una conexión de Cartan plana

Es una condición de compatibilidad de las estructuras de fibrado principal y de álgebra diferencial. La definición general puede encontrarse en el libro de Sharpe [20].

Para definir la condición de compatibilidad, necesitamos

- El álgebra de Lie $\widehat{\chi}$ de los campos de vectores formales :

$$\widehat{\chi} = \{\sum a_i(t)\frac{\partial}{\partial t_i} \mid a_i(t) \in \mathbb{C}[[t_1, \ldots, t_n]]\},$$

- un teorema que se puede probar leyendo el curso de los Profesores López-Hernanz y Ribón.

Teorema 40.

1. *Para cada $\widehat{\gamma}$ en el grupo Γ existe un campo vectorial formal $\widehat{a} = \sum a_i(t)\frac{\partial}{\partial t_i}$ tal que $\widehat{a}(0) = 0$ y para todo $F : (\mathbb{C}^n, 0) \to \mathbb{C}$; $\exp(\widehat{a}) \cdot F = F \circ \widehat{\gamma}$*

2. *Para cada $\widehat{a}$ tal que $\widehat{a}(0) = 0$, existe un $\widehat{\gamma}$ tal que $\exp(\widehat{a}) \cdot F = F \circ \widehat{\gamma}$.*

Utilizando el teorema, cada $\widehat{a} = \sum a_i(t)\frac{\partial}{\partial t_i}$ tal que $\widehat{a}(0) = 0$ actúa sobre $R(M)$ por un campo vectorial $T_{\widehat{a}}$ que es el generador infinitesimal de la familia $T_{\exp \epsilon\widehat{a}}$ para pequeños ϵ: $T_{\widehat{a}} = \lim \frac{1}{\epsilon}(T_{\exp \epsilon\widehat{a}} - T_{id})$

Los campos $\frac{\partial}{\partial t_i}$ actúan también por ∂_i.

Proposición 41. Las dos acciones arriba definen un morfismo T de álgebras de Lie de $\widehat{\chi}$ en el álgebra de Lie de los campos vectoriales sobre RM.

Esta estructura no es importante para la definición del grupoide de Galois pero lo es para los cálculos.

4.5 Los invariantes diferenciales de f

La definición siguiente es muy similar a las definiciones anteriores.

Definición 42. Un invariante diferencial de f es una función racional $H \in \mathbb{C}(RM)$ tal que $H \circ Rf = H$.

Lema 43. *Si H es un invariante de f y $\gamma \in \Gamma$ entonces $H \circ T_\gamma$ es un invariante de f.*

Lema 44. *Si H es un invariante de f entonces $\partial_i H$ es un invariante de f.*

Ejercicio 45. Probar los lemas precedentes.

4.6 El estabilizador de una variedad de referentes

Los grupos de Galois son estabilizadores de subvariedades de un fibrado principal. Entonces antes de dar las definiciones de grupos y grupoide de Galois necesitamos especificar lo que son "los" estabilizadores de una subvariedad de RM.

Definición 46. El estabilizador de una subvariedad $V \subset RM$ es un par $(G, \mathfrak{g})$ donde

1. $G = \{\gamma \in \Gamma \mid T_\gamma(V) = V$ es el estabilizador de V por la acción de Γ,
2. $\mathfrak{g} = \{a \in \widehat{\chi} \mid T_a|_V \in TV\}$ es el estabilizador de V por la acción de $\widehat{\chi}$.

El álgera de Lie de G es una subalgebra de Lie de $\mathfrak{g}$.

4.7 Ejercicios

Ejercicio 47. Si f es la aplicación $(z, x) \mapsto (z + 1, zx)$.

- Calcular $R_1 f$.
- Probar que z^α son invariantes si $|\alpha| > 0$.
- Probar que $\frac{\det jac}{x}$ es un invariante.
- Calcular el estabilizador de un nivel común de los invariantes.

Ejercicio 48. Si $\widehat{a}$ es un campo de vectores formal que se anula dos veces en cero. Su flujo puede definirse como

$$(t_1, \ldots, t_n, \epsilon) \mapsto (\sum \frac{1}{\ell!}(\epsilon\widehat{a})^\ell t_1, \ldots, \sum \frac{1}{\ell!}(\epsilon\widehat{a})^\ell t_n)$$

- Probar que $(\widehat{a})^\ell t_1$ se anula para un orden mayor que $\ell + 1$ en cero.
- Probar que la fórmula está bien definida en el anillo $\mathbb{C}[[t_1, \ldots t_n]]$.

5 Los grupoides

5.1 El grupoide $\mathcal{A}utM$

Este grupoide es

$$\mathcal{A}ut(M) = \{(q, \widehat{\varphi}, p) \mid q \in M, p \in M, \widehat{\varphi} : (M, p) \to (M, q)\}$$

y $\widehat{\varphi}$ está dado por n series de potencias sin condiciones de convergencia tal que det $Jac(\varphi)(p) \neq 0$.

$$\varphi = (\varphi_1, \ldots, \varphi_n) \text{ con } \varphi_i = q_i + \sum_{\substack{\alpha \in \mathbb{N}^n \\ |\alpha| > 0}} \varphi_i^\alpha \frac{(z-p)^\alpha}{\alpha!}$$

La composición es $(q_1, \widehat{\varphi}, p)(p, \widehat{\psi}, q_2) = (q_1, \widehat{\varphi} \circ \widehat{\psi}, q_2)$. Gracias a las fórmulas de Faa di Bruno, este grupoide es un grupoide algebraico con anillo de funciones polinomiales

$$\mathbb{C}[\mathcal{A}utM] = \mathbb{C}[p_1, \ldots, p_n, q_1, \ldots, q_n, \ldots \varphi_i^\alpha \ldots][1/\det(\varphi_i^{\epsilon(j)})]$$

Este grupoide actúa sobre RM :

$$\begin{aligned} &\mathcal{A}utM \underset{M}{\times} RM \to RM \\ &(q, \varphi, p)(p, r) \mapsto R(q, \varphi, p)(p, r) = (q, \varphi \circ r) \end{aligned}$$

y conmuta con la acción de Γ.

5.2 Pseudogrupos algebraicos

Es posible dar una definición intrínseca de grupoide algebraico y probar el teorema de Drach:

Teorema 49. *Un grupoide algebraico es el grupoide de invarianza de sus invariantes sobre un abierto de Zariski $U \subset M$.*

La prueba del teorema de Drach es casi la misma que la prueba del teorema de Kolchin y Chevalley. La diferencia es que tenemos que trabajar con productos tensoriales sobre $\mathbb{C}[M]$. Para hacer la misma prueba necesitamos trabajar sobre $\mathbb{C}(M)$, *i.e.*, sobre un abierto de Zariski.

Utilizando este teorema podemos dar una definición alternativa.

Definición 50. Un subgrupoide $\mathcal{G}$ de $\mathcal{A}ut(M)$ tal que existe une subcuerpo $Inv \subset \mathbb{C}(RM)$ con

$$\mathcal{G} = \{\varphi \mid H \circ R\varphi = H \text{ para todo } H \in Inv\}$$

es un subgrupoide algebraico.

Definición 51. Un subgrupoide algebraico $\mathcal{G}$ de $\mathcal{A}ut(M)$ tal que su cuerpo de invariantes $Inv \subset \mathbb{C}(RM)$ es un subcuerpo diferencial es un pseudogrupo algebraico.

5.3 El grupoide de Galois

Este grupoide es el análogo no lineal de la envolvente algebraica. Existe también un análogo de los grupos de Galois. Son definidos por H. Umemura [21] y la definición puede resultar mucho más difícil que la definición del grupoide.

Para cada punto p tal que f es localmente invertible en p, podemos definir un punto $(f(p), \widehat{f}_p, p)$ de $\mathcal{A}ut(M)$ con el desarrollo de f en serie de potencias alrededor de p. De esta manera tenemos la definición topológica de la envolvente.

Definición 52. $\mathcal{G}al(f)$ es la subvariedad algebraica minimal de $\mathcal{A}ut(M)$ tal que para todo $n \in \mathbb{N}, f^{\circ n} \in \mathcal{G}al(f)$.

Esta fórmula significa que para cada $p \in M$ tal que $f^{\circ n}$ es localmente invertible en p, $(f^{\circ n}(p), \widehat{f^{\circ n}}_p, p) \in Gal(f)$. Los dos teoremas siguientes son análogos de las construcciones alternativas de la envolvente.

Teorema 53. *Existe un abierto de Zariski $U \subset M$ tal que $\mathcal{G}al(f)|_{U\times U}$ es un pseudogrupo algebraico.*

Teorema 54. *Si $Inv(f) \subset \mathbb{C}(RM)$ es el subcuerpo diferencial de los invariantes de f entonces*

$$\mathcal{G}al(f) = \{\varphi \mid \forall H \in Inv(f) \ ; \ H \circ R\varphi = H\}$$

La prueba del teorema 53 es difícil. Se necesita un teorema de Americ y Campana [2].

La prueba del teorema 54 es el teorema de Drach. En este curso es una consecuencia fácil de la definición.

5.4 Ejercicios

Ejercicio 55. Si f es la aplicación $(z,x) \mapsto (z+1, zx)$.

- Probar que $\mathcal{G}al(f) \subset \{\varphi : (z,x) \mapsto (z+a, g(z)x) \mid a \in \mathbb{C}$ y $g \in \mathbb{C}[[z]], g(0) \neq 0\}$.
- Probar la igualdad (¡es difícil! y será necesario estudiar [8]).

Ejercicio 56. Probar que $\mathcal{A}ut(M)$ es el cociente de $RM \times RM$ por la acción diagonal de Γ.

6 Aplicación en dimensión 1: los pseudogrupos

Cuando M es la recta compleja L, solo miramos a funciones analíticas (o series de potencias) de una variable. Tenemos $\mathbb{C}[RL] = \mathbb{C}[z, z_1, z_2, \ldots,][1/z_1]$, la derivación $\partial = \sum z_{i+1} \frac{\partial}{\partial z_i}$ y el álgebra de Lie $\widehat{\chi} = \mathbb{C}[[t]]\frac{d}{dt}$. No hay espacio para muchos invariantes :

Lema 57. *Si un pseudogrupo $\mathcal{G}$ tiene un invariante entonces el cuerpo de los invariantes es el cuerpo diferencial generado por un H de orden minimal k. Diremos que este H es* el invariante *de f.*

Demostración. – Sea k el orden minimal de los invariantes $Inv(f)$. La intersección $Inv(f) \cap \mathbb{C}(R_{k-1}) = \{0\}$, entonces el grado de trascendencia de $Inv(f) \cap \mathbb{C}(R_k)$ sobre $\mathbb{C}$ es 1. El teorema del elemento primitivo implica que $Inv(f) \cap \mathbb{C}(R_k)$ está generado por un elemento H. Las derivadas $\partial^p H$ son lineales en z_{k+p} entonces $Inv(f) = \mathbb{C}(H, \partial H, \ldots)$. □

Vamos a estudiar un nivel común particular de los invariantes: la subvariedad $V = \cap_n \{\partial^n H = 0\} \subset RL$ y sus estabilizadores.

1. $G \subset \Gamma$ es $\{\gamma \mid T_\gamma(V) \subset V\}$
2. $\mathfrak{g} \subset \widehat{\chi}$ es $\{\widehat{a} \mid T_{\widehat{a}}|_V \in TV\}$

Lema 58. *El grupo G es un subgrupo algebraico de Γ de dimensión $k-1$. El álgebra de Lie $\mathfrak{g}$ es una subálgebra de Lie de $\widehat{\chi}$ de dimensión k que contiene $\frac{d}{dt}$.*

Ejercicio 59. Probar el lema.

6.1 Un teorema de Lie

Teorema 60. *Si $\mathfrak{g}$ es una subalgebra de Lie de $\widehat{\chi} = \mathbb{C}[[t]]\frac{d}{dt}$ de dimensión finita que contiene $\frac{d}{dt}$, entonces existe $\gamma \in \Gamma$ tal que*

$$\gamma^*\mathfrak{g} \subset sl_2 = \{(c_0 + c_1 t + c_2\frac{t^2}{2})\frac{d}{dt} \mid c_0, c_1, c_2 \in \mathbb{C}\}.$$

Demostración. – Sea $\frac{d}{dt}, a_1(t)\frac{d}{dt}, \dots a_n(t)\frac{d}{dt}$ una base de $\mathfrak{g}$.

El paréntesis de Lie $[\frac{d}{dt}, a_i(t)\frac{d}{dt}] = a_i'(t)\frac{d}{dt}$ está en $\mathfrak{g}$, entonces $(1, a_1, \dots, a_n)$ satisface a un sistema diferencial lineal con coeficientes constantes.

Podemos resolver este sistema con exponenciales y polinomios.

En el caso semisimple $a_i(t) = \exp(\lambda_i t)$ y

$$\left[\exp(\lambda_i t)\frac{d}{dt}, \exp(\lambda_j t)\frac{d}{dt}\right] = (\lambda_j - \lambda_i)\exp((\lambda_i + \lambda_j)t)\frac{d}{dt},$$

dado que tenemos un número finito de λ's, tenemos menos de 3: $\lambda, 0, -\lambda$. El álgebra de Lie está dentro del algebra de Lie con base

$$\exp(\lambda t)\frac{d}{dt}, \frac{d}{dt}, \exp(-\lambda t)\frac{d}{dt}$$

i.e.,

$$\lambda(\exp(\lambda t))^2\frac{d}{d(\exp(\lambda t))}, \lambda\exp(\lambda t)\frac{d}{d(\exp(\lambda t))}, \lambda\frac{d}{d(\exp(\lambda t))}.$$

El cambio de variable $\gamma(t) = \exp \lambda t - 1$ conjuga estos campos a

$$\lambda(t+1)^2\frac{d}{dt}, \lambda(t+1)\frac{d}{dt}, \lambda\frac{d}{dt}$$

que generan sl_2.

Si el sistema no es semisimple tenemos que hacer cálculos parecidos. □

Ejercicio 61. Probar el teorema de Lie en el caso general.

Sea γ el cambio de variable del teorema de Lie. La variedad

$$V_0 = T_\gamma(V) = \{r \circ \gamma \mid r \in V\}$$

Sus estabilizadores son

1. $G_0 = \{\gamma \in \Gamma | T_\gamma(V_0) \subset V_0\} \subset \{\gamma : t \mapsto \frac{\alpha t}{1-\beta t} \mid \alpha \in \mathbb{C}^*, \beta \in \mathbb{C}\}$

2. $\mathfrak{g}_0 = \{\widehat{a} \in \widehat{\chi} \mid T_{\widehat{a}}|_{V_0} \in TV_0\} \subset sl_2$

6.2 Las ecuaciones de V_0

Supongamos que $\mathfrak{g}_0 = sl_2$ y escribimos $F(z, z_1, z_2, z_3) = \left(2\frac{z_3}{z_1} - 3\left(\frac{z_2}{z_1}\right)^2\right)\frac{1}{(z_1)^2} \in \mathbb{C}[R_3L]$.

Lema 62. *V_0 es un fibrado principal para el grupo G_0 sobre un abierto de Zariski de L.*

Lema 63. *Existe $\nu \in \mathbb{C}(z)$ tal que*

$$V_0 = \left\{ r \in RM \mid \left(2\frac{r'''}{r'} - 3\left(\frac{r''}{r'}\right)^2\right)\frac{1}{(r')^2} - \nu(r) = 0 \right\}.$$

Esta fórmula significa que el ideal de definición de V_0 está generado diferencialmente por $q(z)F(z, z_1, z_2, z_3) - p(z)$ donde $\nu = \frac{p}{q}$.

Los referentes de V_0 en un punto $p \in L$ son una órbita de la acción de G_0 sobre RL. Es fácil verificar que sus órbitas en R_3L son los niveles de F :
Si $r = r_0 + r_1 t + r_2\frac{t^2}{2} + r_3\frac{t^3}{6} + \ldots$ y $\gamma = \alpha t + 2\alpha\beta\frac{t^2}{2} + 6\alpha\beta^2\frac{t^3}{6} + \ldots$ entonces

$$r \circ \gamma = r_0 + r_1\alpha t + (r_2\alpha^2 + 2r_1\alpha\beta)\frac{t^2}{2} + (r_3\alpha^3 + 6r_2\alpha^2\beta + 6r_1\alpha\beta^2)\frac{t^3}{6} + \ldots$$

y tenemos $F(r) = F(r\circ\gamma)$. La restricción de esta función sobre V_0 es una función invariante por G_0, entonces es una función racional en r_0.

6.3 Las ecuaciones de $\mathcal{G}$

Obtenemos las ecuaciones de $\mathcal{G}$ mirando las ecuaciones de V_0.

Lema 64. *Si $\mathcal{G}$ es un pseudogrupo con su invariante de orden 3 entonces*

$$\mathcal{G} = \{\varphi \mid 2\frac{\varphi'''}{\varphi'} - 3\left(\frac{\varphi''}{\varphi'}\right)^2 + \nu(\varphi)(\varphi')^2 = \nu(z)\}$$

Demostración. – Si

$$r = r_0 + r_1 t + r_2 \frac{t^2}{2} + r_3 \frac{t^3}{6} + \dots$$

y

$$\varphi = \varphi_0 + \varphi_1 (z - r_0) + \varphi_2 \frac{(z - r_0)^2}{2} + \varphi_3 \frac{(z - r_0)^3}{6} + \dots$$

tenemos

$$\varphi \circ r = \varphi_0 + (\varphi_1 r_1) t + (\varphi_2 (r_1)^2 + \varphi_1 r_2) \frac{t^2}{2} + (\varphi_3 (r_1)^3 + 3\varphi_2 r_1 r_2 + \varphi_1 r_3) \frac{t^3}{6} + \dots$$

Si $r \in V_0$ y $\varphi \circ r \in V_0$ podemos eliminar r y obtener ecuaciones en φ :

$$2\frac{\varphi_3}{\varphi_1} - 3\left(\frac{\varphi_2}{\varphi_1}\right)^2 + \nu(\varphi_0)(\varphi_1)^2 = \nu(r_0).$$

□

Llamaremos $\mathcal{G}_3(\nu)$ este tipo de pseudogrupos.

6.4 Ejercicios

Ejercicio 65. Probar que si $\mathfrak{g}_0 = (\mathbb{C} + \mathbb{C}t)\frac{d}{dt}$, entonces existe $\mu \in \mathbb{C}(z)$ tal que

$$\mathcal{G} = \{\varphi | \frac{\varphi''}{\varphi'} + \mu(\varphi)\varphi' = \mu(x)\}.$$

Ejercicio 66. Probar que si $\mathfrak{g}_0 = \mathbb{C}\frac{d}{dt}$ entonces tenemos dos casos

1. existe $\eta \in \mathbb{C}(z)$ y $k \in \mathbb{N}$ tal que

$$\mathcal{G} = \{\varphi | \eta(\varphi)(\varphi')^k = \eta(x)\},$$

2. existe $h \in \mathbb{C}(z)$ tal que

$$\mathcal{G} = \{\varphi | h(\varphi) = h(x)\}.$$

7 Aplicación en dimensión 1: el pseudogroupo de Galois de $f : \mathbb{C} \dashrightarrow \mathbb{C}$

Queremos probar el siguiente teorema:

Teorema 67. *Si $f : L \dashrightarrow L$ es tal que $\mathcal{G}al(f) \neq \mathcal{A}ut(L)$ entonces f está en la lista de Ritt: existe una homografía A tal que $A \circ f \circ A^{-1}$ es*

- *una homografía*
- *un monomio, $M_k(z) = z^k$,*
- *un Chebishev, $T_k(z) = \cos(k \arccos(z))$*
- *un Lattès, $L_e(z) = \mathcal{P}(e(\mathcal{P}^{-1}(z)))$ donde e es un endomorfismo de grado > 1 de la curva elíptica de la función elíptica $\mathcal{P}$.*

Utilizando la clasificación de los pseudogrupos, el problema es: dar los $f \in \mathbb{C}(z)$ tal que existe un $\nu \in \mathbb{C}(z)$ tal que $f \in \mathcal{G}_3(\nu)$, *i.e.*,

$$2\frac{f'''}{f'} - 3\left(\frac{f''}{f'}\right)^2 + \nu(f)(f')^2 - \nu(z) = 0.$$

7.1 La linealización de un punto fijo repulsivo

Para resolver la ecuación utilizaremos elementos de la dinámica de f.

Teorema 68 (Koenigs)**.** *Si $f : (\mathbb{C}, 0) \to (\mathbb{C}, 0)$ es tal que $\lambda = |f'(0)| > 1$ entonces existe $h \in \mathbb{C}\{w\}$ con $h(0) = 0, h'(0) = 1$ tal que $h^{-1} \circ f \circ h(w) = \lambda w$. Llamaremos a h una linealización de f.*

Teorema 69 ([13] chap. 10 corollary 10.16.)**.** *Si $f \in \mathbb{C}(z)$ pero no es una homografía entonces para cada $k \in \mathbb{N}$ existe $n \in \mathbb{N}$ tal que $f^{\circ n}$ tiene más de k puntos fijos repulsivos.*

La prueba del segundo teorema es más difícil. La cantidad de puntos fijos crece con n pero tenemos una cota sobre el número de puntos fijos que no son repulsivos.

Podemos suponer que $f : L \dashrightarrow L$ tiene un punto fijo repulsivo con linealización h que no es un polo de ν.

Lema 70. *La linealización $h : (\mathbb{C}, 0) \to L$ es el germen de una función meromorfa sobre $\mathbb{C}$.*

Demostración. – Si $w \in \mathbb{C}$, existe n tal que $\frac{w}{\lambda^n}$ está en el dominio de h. Si $h\left(\frac{w}{\lambda^n}\right)$ está en el dominio de $f^{\circ n}$, definimos $h(w)$ por

$$f^{\circ n} \circ h\left(\frac{w}{\lambda^n}\right).$$

□

Nota 71. Para f en la lista de Ritt, tenemos $\lambda = k$ y

$$h = A \circ \exp,\ A \circ \cos,\ A \circ \mathcal{P},\ A \circ \mathcal{P}^2, A \circ \mathcal{P}' \text{ o } A \circ \mathcal{P}'^2.$$

Éstas son funciones que realizan los cocientes de $\mathbb{C}$ por grupos discretos de transformaciones afines : $w \to aw + b$.

7.2 El pull-back de $\mathcal{G}al$ por h y la estructura de h

Queremos probar que los φ tal que $h \circ \varphi = h$ son aplicaciones afines. El pseudogrupo "pull-back" de $\mathcal{G}al$ por h,

$$\{\varphi \mid \text{ existe } \psi \in \mathcal{G}_3(\nu) \text{ t.q. } h \circ \varphi = \psi \circ h\},$$

es un pseudogrupo de tipo $\mathcal{G}_3(\widetilde{\nu})$ con

$$\widetilde{\nu}(w) = \nu(h(w))h'(w)^2 + 2\frac{h'''}{h'} - 3\left(\frac{h''}{h'}\right)^2.$$

Conocemos una solución $w \to \lambda w$ de $\mathcal{G}_3(\widetilde{\nu})$, entonces

$$\widetilde{\nu}(\lambda w)\lambda^2 = \widetilde{\nu}(w).$$

Por otro lado, la fórmula para $\widetilde{\nu}$ nos da que $\widetilde{\nu}$ es holomorfa en 0 y por eso $\widetilde{\nu} = 0$.

Los elementos $\varphi \in \mathcal{G}_3(0)$ son gérmenes de homografías. Probamos que h es el cociente por un grupo de homografía. Los grupos que aparecen son

- $\mathbb{Z}$
- $\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
- $(\mathbb{Z} + \tau\mathbb{Z}) \times \mathbb{Z}/2\mathbb{Z}$
- $(\mathbb{Z} + i\mathbb{Z}) \times \mathbb{Z}/4\mathbb{Z}$

- $(\mathbb{Z} + j\mathbb{Z}) \times \mathbb{Z}/3\mathbb{Z}$
- $(\mathbb{Z} + j\mathbb{Z}) \times \mathbb{Z}/6\mathbb{Z}$

y las funciones que realizan este cociente son exp, cos o las funciones elípticas.

Probamos que si f está dentro de un $\mathcal{G}_3(\nu)$ entonces $f^{\circ n}$ está en la lista de Ritt. Para finalizar la prueba tenemos que ver que:

1. los f de la lista de Ritt pertenecen a un $\mathcal{G}_3(\nu)$,
2. si $f^{\circ n}$ está en la lista entonces f también.

El primero es un ejercicio de cálculo. Para probar el segundo, tenemos que verificar que si h es una linealización de $f^{\circ n}$ entonces $f \circ h$ también.

8 Aplicación en dimensión 1: el teorema de Ritt

Teorema 72. *Si la linealización h de un punto fijo repulsivo de $f : L \dashrightarrow L$ satisface una ecuación diferencial polinomial entonces f está en la lista de Ritt: existe una homografía A tal que $A \circ f \circ A^{-1}$ es*

- *una homografía*
- *un monomio $M_k(z) = z^k$,*
- *un Tchebitchev $T_k(z) = \cos(k \arccos(z))$*
- *un Lattes $L_e(z) = \mathcal{P}(e(\mathcal{P}^{-1}(z)))$ donde e es un endomorfismo de grado > 1 de la curva elíptica de $\mathcal{P}$.*

8.1 La ecuación de h

La linealización h es una función meromorfa de $\mathbb{C}$ en L entonces sus series de potencias en cada punto de su dominio son elementos de

$$F(\mathbb{C}, L) = \{(z_0, \widehat{k}, w_0) \mid \widehat{k} : (\mathbb{C}, w_0) \to (L, z_0)\}$$

$$\widehat{k}(w) = z_0 + \sum_{n>1} k_n \frac{(w - w_0)^n}{n!}.$$

El anillo de funciones polinomiales sobre $F(\mathbb{C}, L)$ es $\mathbb{C}[F] = \mathbb{C}[w_0, z_0, k_1, k_2, \ldots]$.

Sea $I \subset \mathbb{C}[F]$ el ideal de las ecuaciones satisfechas por todos los desarrollos de series de potencias de h.

Lema 73. *El ideal I es un ideal estable por $D = \frac{\partial}{\partial w_0} + k_1 \frac{\partial}{\partial z_0} + \sum_{i>0} k_{i+1} \frac{\partial}{\partial k_i}$*

Lema 74. *Sea Z el conjunto de los ceros de I en $F(\mathbb{C}, L)$. Este conjunto es de dimensión finita*

Demostración. – Por hipótesis I contiene un polinomio que no es 0: si $E(w, h, h', \ldots h^{(p)}) = 0$ es una ecuación de h de orden minimál entonces la dimensión de Z es $p + 1$. $\square$

8.2 Las acciones de f y $\mathbb{C}^*$

La transformación $f : L \dashrightarrow L$ actúa sobre $F(\mathbb{C}, L)$ por $Rf : \widehat{k} \mapsto f \circ \widehat{k}$. Pero no preserva Z. Queremos construir un conjunto algebraico de dimensión finita y invariante por Rf.

El grupo de transformaciones $\sigma_q : w \mapsto qw$ actúa sobre $F(\mathbb{C}, L)$ por cambios de variable. Si $\widehat{k} : (\mathbb{C}, w_0) \to (L, z_0)$ con

$$\widehat{k}(w) = z_0 + \sum_{n>1} k_n \frac{(w - w_0)^n}{n!}$$

entonces $T_q(\widehat{k}) : (\mathbb{C}, \frac{w_0}{q}) \to (L, z_0)$ está definida por

$$\widehat{k} \circ \sigma_q(w) = z_0 + \sum_{n>1} q^n k_n \frac{(w - \frac{w_0}{q})^n}{n!}.$$

La ecuación funcional de linealización es $Rf(\widehat{h}) = T_\lambda(\widehat{h})$. Vamos a construir un conjunto invariante utilizando esta igualdad y un teorema de Chevalley:

Teorema 75 ([12] por ejemplo)**.** *Si $f : X \to Y$ es una aplicación polinomial entre conjuntos algebraicos entonces existe un conjunto algebraico $S \subset \overline{f(X)}$ tal que*

- *$\overline{f(X)} - S$ es denso dentro de $\overline{f(X)}$,*
- *$\overline{f(X)} - S = f(X) - S$*

El conjunto $T_{\lambda^{-1}}(\overline{Rf(Z)})$ es un conjunto algébraico que contiene los desarrollos de h entonces contiene Z *i.e.* $\overline{Rf(Z)} \supset T_\lambda(Z)$. Como Rf y T_q conmutan $\overline{R_f(T_q Z)} \supset T_{q\lambda}(Z)$, el conjunto

$$V = \overline{\cup_{q\in\mathbb{C}^*} T_q(Z)}$$

es un conjunto algebraico invariante. Tenemos que probar que este conjunto es de dimensión finita.

Los invariantes de la acción de $\mathbb{C}^*$ sobre $F(\mathbb{C}, L)$ son

$$\begin{aligned} \pi : F(\mathbb{C}, L) &\to \mathbb{C}^{\mathbb{N}} \\ (w_0, z_0, h_1 \ldots) &\mapsto (z_0, w_0 h_1, (w_0)^2 h_2 \ldots) \end{aligned}$$

Los niveles de π son de dimensión uno. Por el teorema de Chevalley: $\overline{\pi(Z)}$ es un conjunto algebraico de dimensión más pequeña que la dimensión de Z y $V = \pi^{-1}(\overline{\pi(Z)})$ es un conjunto algebraico de dimensión menor que la dimensión de Z más uno, es el conjunto algebraico minimal $\mathbb{C}^*$-invariante que contiene Z, entonces

$$R_f(V) \subset V$$

La dimensión de V es finita y por lo tanto

$$\mathcal{G} = \left\{ \varphi \in \mathcal{A}ut(L) \;\middle|\; R\varphi(V) \subset V \right\}$$

es un pseudogrupo algebraico de dimensíon finita y contiene f. Por definición $\mathcal{G}al(f) \subset \mathcal{G}$. Entonces $\mathcal{G}al(f)$ es pequeño y el teorema de Ritt está probado.

Referencias

[1] Audin M. – Julia, Montel. The great prize of mathematical sciences of 1918, and beyond. Translated from the 2009 French original by the author. Lecture Notes in Mathematics, 2014. History of Mathematics Subseries. Springer, Heidelberg, 2011. viii+332 pp. 113

[2] Americ K. & Campana F. – Fibrations méromorphes sur certaines variétés à fibré canonique trivial. Pure Appl. Math. Q. 4 (2008), no. 2, Special Issue: In honor of Fedor Bogomolov. Part 1, 509–545. 125

[3] Bergweiler W. – Solution of a problem of Rubel concerning iteration and algebraic differential equations, Indiana Univ. Math. J. 44 (1995), 257–267;

[4] Bergweiler W. ;& Aschenbrenner M. – Julia's equation and differential transcendence 113

[5] Chevalley, C. & Kolchin, E. – Two proofs of a theorem on algebraic groups. Proc. Amer. Math. Soc. 2, (1951). 126–134. 115

[6] Crespo, T. & Hajto, Z. – Algebraic Groups and Differential Galois Theory, Graduate Studies in Mathematics 122, American Mathematical Society, 2011. 114

[7] Drach, J. – Sur l'intégration logique des équations différentielles ordinaires, Proceedings of the 5th international congress of mathematicians Cambrige university press (1913), Vol 1 pp 438–497 (available on `http://www.mathunion.org/ICM/`) 115

[8] Hardouin C. & Singer M.F. – Differential Galois theory of linear difference equations. Math. Ann. 342 (2008), no. 2, 333–377. 113, 125

[9] Hochschild, G. P. – Basic theory of algebraic groups and Lie algebras. Graduate Texts in Mathematics, 75. Springer-Verlag, New York-Berlin, 1981. viii+267 pp. 114

[10] Malgrange, B. – Le groupoïde de Galois d'un feuilletage. (French) [The Galois groupoid of a foliation] Essays on geometry and related topics, Vol. 1, 2, 465–501, Monogr. Enseign. Math., 38, Enseignement Math., Geneva, 2001. 112

[11] Martinet, J. & Ramis, J.-P. – Classification analytique des équations différentielles non linéaires résonnantes du premier ordre. Ann. Sci. École Norm. Sup. (4) 16 (1983), no. 4, 571–621 (1984). 113

[12] Matsumura H. – Commutative algebra, second ed., Mathematics Lecture Note Series, vol. 56, Benjamin/Cummings Publishing Co., Inc., Reading, Mass., 1980 131

[13] Milnor, J.W. – Dynamics in one complex variable. Introductory lectures. Ann. of Math. Studies 160 Princeton Univ. Press (2006) 112, 129

[14] Milnor J. W. – On Lattès maps. Dynamics on the Riemann sphere, 9–43, Eur. Math. Soc., Zürich, 2006.,

[15] van der Put, M. & Singer, M.F. – Galois theory of difference equations. Lecture Notes in Mathematics, 1666. Springer-Verlag, Berlin, 1997. viii+180 pp. 112, 118

[16] Ramis, J.-P. – About the growth of entire functions solutions of linear algebraic q-difference equations. Ann. Fac. Sci. Toulouse Math. (6) 1 (1992), no. 1, 53–94. 113

[17] Ritt, J. F. – Permutable rational functions. Trans. Amer. Math. Soc. 25 (1923), no. 3, 399–448. 113

[18] Ritt, J. F. – Transcendental transcendency of certain functions of Poincaré. Math. Ann. 95 (1926), no. 1, 671–682. 112

[19] Ritt, J. F. – Meromorphic functions with addition or multiplication theorems. Trans. Amer. Math. Soc. 29 (1927), no. 2, 341–360. 113

[20] Sharpe, R. W. – Differential geometry. Cartan's generalization of Klein's Erlangen program. With a foreword by S. S. Chern. Graduate Texts in Mathematics, 166. Springer-Verlag, New York, 1997. xx+421 pp. 122

[21] Umemura, H. – Differential Galois theory of infinite dimension. Nagoya Math. J. 144 (1996), 59–135. 124