Pontificia Universidad Católica del Perú
Escuela de Posgrado

Teoría de Galois de ecuaciones diferenciales lineales

Tesis para Optar el Grado de
Magíster en Matemáticas

Autor
Suzanne Maria Huaringa Mosquera

Asesor
Percy Braulio Fernández Sanchez

Jurado
Roland Rabanal
Christian Valqui

Lima - Perú
Abril-2020

Teoría de galois de ecuaciones diferenciales lineales

Suzanne Maria Huaringa Mosquera[1]

Tesis presentada a consideración del Cuerpo Docente de la Escuela de Posgrado, de la PUCP, como parte de los requisitos para obtener el grado académico de Magíster en Matemática.

Miembros de Jurado:

Dr. Percy Fernández

(Asesor)

Dr. Christian Valqui

(presidente)

Dr. Roland Rabanal

(miembro)

Lima - Perú

Abril-2020

[1]Proyecto DGI: (PAIP 2017)

... a mi familia

Agradecimientos

A todos los profesores que me enseñaron en la maestría en matemática en la PUCP.

A mi asesor, el doctor Percy Fernández, por ayudarme y enseñarme durante todo el tiempo del desarrollo de la tesis, por su gran paciencia y apoyo, por haberme enseñado durante la maestría diferentes cursos de álgebra los cuales me motivaron a aprender sobre esa rama de la matemática.

Al profesor Roland Rabanal por su gran ayuda en las correcciones de la tesis, por haberle dedicado el tiempo de leerla, por su paciencia y sus consejos.

A mi padre, el profesor Zacarías Huaringa por su apoyo en todo momento, en especial desde que inicié la maestría. A mi madre por su cariño y motivación.

A toda mi familia, en especial a mi abuela Corina por ser el soporte que construyó a toda la familia.

A la Dirección de Gestión de la Investigación de la PUCP, por haberme apoyado en la elaboración de esta tesis a través del proyecto PAIP 2017.

Resumen

En teoría de Galois clásica, las raíces de un polinomio $f(X) \in K[X]$, sus raíces generan una extensión E del cuerpo K, llamado el cuerpo de descomposición E de $f(X)$. En el presente trabajo estudiaremos su análogo en teoría de Galois diferencial. Si dotamos a un anillo de una operacion llamada derivación (que verifica las propiedades básicas de la derivada usual) llamaremos a este par, anillo diferencial. Veremos que dado un cuerpo diferencial K y un operador diferencial lineal homogéneo $\mathcal{L}$ definido sobre el, sus soluciones generan una extension diferencial E del cuerpo diferencial K, dicha extensión es llamada de Picard-Vessiot. Mostraremos con detalle la construcción de una extensión de Picard-Vessiot [1] y veremos que en efecto siempre es posible realizarla. También veremos que es única salvo $K-$isomorfismo diferencial.

Palabras clave: Extensión de Picard-Vessiot, extensión de Galois, anillo diferencial.

Abstract

In classic Galois Theory the roots of a polynomial f(X) K [X] generate an extension E of the field K, called the splitting field E of $f(X)$. In this thesis we will study the analogous in Differential Galois Theory. If we endow a ring with a map called derivation (wich verifies the basic properties of the usual derivative), we will call this pair a differential ring. We will see that given a differential field K and a homogeneous linear differential operator $\mathcal{L}$ defined over it, its solutions generate a differential extension E of the differential field K. Such extension is called a Picard-Vessiot extension. We will show with detaill the results given in [1], in particular, the construction of a Picard-Vessiot extension and we will see that in fact it is always possible to realize this extension. We also prove the uniqueness of this extension modulo $K-$differential isomorphism.

Keywords: Picard-Vessiot Extension, Galois extension, differential ring.

Índice general

Introducción **1**

1. Preliminares **4**

1.1. Conceptos básicos y ejemplos 4

1.1.1. Variedades en un espacio afín 4

1.1.2. Grupos algebraicos 8

1.2. Acciones de grupos algebraicos sobre variedades 10

1.2.1. Linealización de grupos algebraicos afines 10

1.2.2. Caracteres y semi-invariantes 15

1.2.3. Cocientes en grupos algebraicos 15

1.3. Descomposición de grupos algebraicos 18

2. Cuerpos diferenciales **28**

2.1. Anillos diferenciales 28

2.2. Extensiones diferenciales 32

2.3. El anillo de operadores diferenciales 35

2.3.1. Ecuaciones diferenciales lineales homogéneas 36

2.3.2. El wronskiano 36

2.3.3. Independencia lineal sobre constantes 40

2.3.4. El álgebra universal de soluciones 43

3. La extensión de Picard-Vessiot **47**

3.1. Definición con un operador diferencial, existencia y unicidad 47

3.1.1. Existencia 52

3.1.2. Unicidad 57

3.1.3. La existencia y la unicidad, revisados 63

3.2. Caracterización de extensiones de Picard-Vessiot 69

3.2.1. Extensión de Galois finita 72

4. Teorema fundamental de la teoría de Picard-Vessiot 75

4.1. Grupo de Galois diferencial 75

4.1.1. Ejemplos de grupos de Galois diferenciales 79

4.2. El grupo de Galois diferencial como grupo algebraico lineal 83

4.3. El Teorema fundamental 98

Bibliografía 117

Introducción

El presente trabajo es una introducción al estudio de la teoría de Galois diferencial. Dado un cuerpo K, una derivación sobre K es una aplicación $d : K \to K$ que verifica

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

Un cuerpo provisto de una derivación se llama cuerpo diferencial. Al agregar esta estructura diferencial sobre un cuerpo, sea crea una teoría análoga a la clásica.

La teoría de Galois diferencial es la teoría de soluciones de ecuaciones diferenciales sobre un cuerpo diferencial base, o más bien de la naturaleza de una extensión diferencial generada por estas soluciones, de una forma muy parecida como la teoría de Galois clásica es la teoría de extensiones generadas por soluciones de ecuaciones polinomiales de una variable, pero ahora con la propiedad adicional de que los correspondientes grupos de Galois diferencial (de automorfismos de la extensión que fijan el cuerpo base y conmutan con la derivación) tienen estructura de grupo algebraico.

En el capítulo 1 mostraremos algunos resultados de Geometría Algebraica que ayudarán en la demostración de los resultados en los siguientes capítulos. Definiremos y estudiaremos los grupos algebraicos, sus propiedades y como actúan sobre variedades. Concluiremos este capítulo estudiando la descomposición de Jordan Chevalley de un morfismo.

En el capítulo 2 presentaremos la noción de una derivación sobre un anillo, seguido de algunas propiedades algebraicas. Definiremos los elementos de una estructura diferencial, como extensiones de cuerpos diferenciales, morfismos diferenciales, ideales diferenciales.

Dado un cuerpo diferencial K definiremos su cuerpo de constantes, $C_K = \{a \in K : d(a) = 0\}$. Luego introduciremos los elementos con los cuales trabajaremos

durante el resto de esta tesis: los operadores diferenciales lineales. Terminaremos este capítulo mostrando un ejemplo que induce a preguntar sobre la manera de crear una extensión diferencial de K que contenga soluciones de un operador definido sobre K, pero que no agregue constantes.

En el capítulo 3 mostraremos la construcción de dicha extensión, llamada extensión de Picard-Vessiot, y veremos que es posible encontrarla (y es única salvo $K-$isomorfismo diferencial) siempre que C_K sea algebraicamente cerrado. De hecho, mostraremos algunos ejemplos en donde no se tiene existencia o unicidad salvo isomorfismo de una extensión de Picard-Vessiot. Esto muestra la importancia de la hipótesis de que C_K sea algebraicamente cerrado.

Finalmente, en el capítulo 4 definimos el análogo diferencial al grupo de Galois clásico de una extensión de cuerpos: el grupo de Galois diferencial. En particular, el grupo de Galois diferencial de una extensión de Picard-Vessiot tiene estructura de grupo algebraico. Presentaremos el análogo al teorema fundamental de la teoría de Galois clásica, que es el teorema fundamental de la teoría de Picard-Vessiot.

En lo posible hemos tratado de manejar los resultados de manera accesible, cuyos prerequisitos requieran herramientas de Álgebra Básica y Geometría Algebraica.

Lista de Simbolos

$\wedge^k(V)$	—	$k-$ésima potencia exterior del espacio vectorial V.
P_n	—	Espacio de permutaciones.
$V \simeq W$	—	Isomorfismo entre las variedades algebraicas V y W.
$S \otimes_K T$	—	Producto tensorial de $K-$álgebras.
$\mathbb{G}_m$	—	Grupo multiplicativo de un cuerpo.
$\mathbb{G}_a$	—	Grupo aditivo de un cuerpo.
$\overline{K}$	—	Clausura algebraica de un cuerpo K.
$\mathrm{trdeg}[L:K]$	—	Grado de trascendencia de la extensión $K \subset L$.
$\overline{H}^G$	—	Clausura de Zariski del subgrupo H en el grupo G.
$\mathrm{Frac}(A)$	—	Cuerpo de fracciones del dominio A.
$K\langle S\rangle$	—	Cuerpo diferencial generado por S sobre K, página 33
L^G	—	Subcuerpo de L fijado por G, un grupo de automorfismos de L.

Capítulo 1

Preliminares

En esta sección haremos un repaso del concepto de variedad algebraica, definiremos lo que es un grupo algebraico y daremos algunos ejemplos. Veremos que un grupo algebraico lineal es una variedad afin y recíprocamente que un grupo algebraico afin es un subgrupo cerrado de algún grupo general lineal.

1.1. Conceptos básicos y ejemplos

1.1.1. Variedades en un espacio afín

A menos que sea especificado de otra manera, C denotará un cuerpo algebraicamente cerrado de característica cero. Sea $C[X_1, \dots X_n]$ el anillo de polinomios en n indeterminadas sobre C. El conjunto $C \times \cdots \times C$ será llamado **n-espacio afín** y denotado por $\mathbb{A}^n_C$ ó solo $\mathbb{A}^n$. Una variedad afín es el conjunto de ceros comunes en $\mathbb{A}^n_C$ de una colección finita de polinomios en $C[X_1, \dots X_n]$.

A cada ideal I de $C[X_1, \dots X_n]$ le asociaremos el conjunto $\mathcal{V}(I)$ de sus ceros comunes en $\mathbb{A}^n_C$. Por el teorema de la base de Hilbert, la $C-$álgebra $C[X_1, \dots X_n]$ es Noetheriana, luego cada ideal de $C[X_1, \dots X_n]$ tiene un conjunto finito de generadores, por lo tanto $\mathcal{V}(I)$ es una variedad afin. A cada subconjunto $S \subset \mathbb{A}^n_C$ le asociamos la colección $\mathcal{I}(S)$ de polinomios que se anulan en S.

Las siguientes proposiciones son sencillas de probar. Podría consultarse el interesante libro [2].

Proposición 1.1. *Sean S, S_1, S_2 subconjuntos de $\mathbb{A}_C^n$, e I_1, I_2 ideales de $C[X_1, \ldots, X_n]$, entonces se cumplen:*

a) Si $S_1 \subset S_2$, entonces $\mathcal{I}(S_1) \supset \mathcal{I}(S_2)$.

b) Si $I_1 \subset I_2$, entonces $\mathcal{V}(I_1) \supset \mathcal{V}(I_2)$.

c) $\mathcal{I}(S) = C[X_1, \ldots, X_n]$ sí y sólo si $S = \emptyset$.

Proposición 1.2. *La correspondencia $\mathcal{V}$ satisface las siguientes igualdades:*

a) $\mathbb{A}_C^n = \mathcal{V}(0), \emptyset = \mathcal{V}(C[X_1, \ldots, X_n])$.

b) Sean I, J ideales de $C[X_1, \ldots, X_n]$, entonces $\mathcal{V}(I) \cup \mathcal{V}(J) = \mathcal{V}(I \cap J)$.

c) Sea $\{I_\alpha\}$ una colección arbitraria de ideales de $C[X_1, \ldots, X_n]$, entonces

$$\bigcap_\alpha \mathcal{V}(I_\alpha) = \mathcal{V}(\sum_\alpha I_\alpha).$$

A partir de las proposiciones anteriores se obtiene que las variedades afines en $\mathbb{A}_C^n$ satisfacen los axiomas de los conjuntos cerrados en un espacio topológico. De este modo el complemento de cada variedad afín es un abierto en la llamada **Topologia de Zariski**.

Dado un ideal I de un anillo comutativo A, el radical $\sqrt{I}$ de I está definido por

$$\sqrt{I} = \{a \in A : a^r \in I \quad \text{para algún} \quad r \geq 1\}.$$

Así, un **ideal radical** es un ideal que es igual a su radical, es decir $I = \sqrt{I}$. Consecuentemente, un ideal I del anillo A es radical sí y sólo si, el anillo cociente A/I no tiene elementos nilpotentes distintos de cero. Algunos ejemplos de ideales radicales son los ideales primos y los ideales de la forma $\mathcal{I}(S)$ donde $S \subset \mathbb{A}_C^n$.

Para un ideal I de $C[X_1, \ldots, X_n]$, es fácil ver que $\sqrt{I} \subset \mathcal{I}(\mathcal{V}(I))$. Cuando el cuerpo C es algebraicamente cerrado tenemos $\sqrt{I} = \mathcal{I}(\mathcal{V}(I))$.

Recordemos que un espacio topológico no vacío X es reducible si puede ser escrito como unión de dos subconjuntos cerrados propios. Se dice que X es **irreducible** si no es reducible, ó equivalentemente si todos los subonjuntos abiertos no vacíos de X son densos. Para subconjuntos de $\mathbb{A}_C^n$ la irreducibilidad es caracterizada en términos de su ideal correspondiente mediante la siguiente proposición.

Proposición 1.3. *Un conjunto cerrado V de $\mathbb{A}_C^n$ es irreducible sí y sólo si su ideal $\mathcal{I}(V)$ es primo.*

La demostración se encuentra en la proposición 1.1.13. de [2].

Si V es cerrado en $\mathbb{A}_C^n$, cada polinomio $f(X_1, \ldots, X_n) \in C[X_1, \ldots, X_n]$ define una función f sobre V con valores en C. Pero diferentes polinomios podrian definir la misma función. Sin embargo, es claro que tenemos una correspondencia inyectiva entre las funciones polinomiales sobre V y el anillo de clases residuales $C[X_1, \ldots, X_n]/\mathcal{I}(V)$ que se denota por $C[V]$ y lo llamaremos el anillo de coordenadas de V. Es un álgebra finitamente generada sobre C y es reducida (es decir, no tiene elementos nilpotentes distintos de cero) pues $\mathcal{I}(V)$ es un ideal radical.

Sean $V \subset \mathbb{A}_C^n$ y $W \subset \mathbb{A}_C^m$ variedades afines, una aplicación $\varphi : V \to W$ es un **morfismo de variedades afines** si para $x = (x_1, \ldots, x_n) \in V$ se tiene que $\varphi(x_1, \ldots, x_n) = (\varphi_1(x), \ldots, \varphi_m(x))$ para ciertos $\varphi_i \in C[V]$. A un morfismo de variedades $\varphi : V \to W$ podemos asociarle el morfismo de $C-$álgebras $\varphi^* : C[W] \to C[V]$ definido por $\varphi^*(f) = f \circ \varphi$. El morfismo $\varphi : V \to W$ es un **isomorfismo**, si existe un morfismo $\psi : W \to V$ tal que $\psi \circ \varphi = id_V$ y $\varphi \circ \psi = id_W$, ó equivalentemente $\varphi^* : C[W] \to C[V]$ es un isomorfismo de $C-$álgebras (con inversa ψ^*). En este caso denotaremos por $V \simeq W$.

Con frecuencia necesitaremos considerar aplicaciones sobre una variedad afín irreducible V, que no están definidas en todo punto, por lo tanto introducimos el siguiente concepto.

Definición 1.4. a) Si V es una variedad afin irreducible, un **mapeo racional** $\varphi : V \to \mathbb{A}_C^n$ es una $n-$upla $(\varphi_1, \ldots, \varphi_n)$ de funciones racionales $\varphi_1, \ldots, \varphi_n \in C(V)$. Diremos que φ es **regular** en un punto $P \in V$ si todos los φ_i son regulares en P y $\mathrm{dom}(\varphi) = \bigcap_{i=1}^{n} \mathrm{dom}(\varphi_i)$

b) Para una variedad $W \subset \mathbb{A}_C^n$, un mapeo racional $\varphi : V \to W$ es una n-upla $(\varphi_1, \ldots, \varphi_n)$ de funciones racionales $\varphi_1, \ldots, \varphi_n \in C(V)$ tales que $\varphi(P) = (\varphi_1(P), \ldots, \varphi_n(P)) \in W$ para todo $P \in \mathrm{dom}(\varphi)$.

Un mapeo racional $\varphi : V \to W$ es llamado **dominante** si $\varphi(\mathrm{dom}(\varphi))$ es un subconjunto denso en W con la topología de Zariski.

Sea $V \subset \mathbb{A}^n_C$ una variedad afín, y L un cuerpo algebraicamente cerrado que contiene C. Denotaremos por V_L a la variedad afín contenida en $\mathbb{A}^n_L$ definida por $V_L = \mathcal{V}(I_L)$ donde $I_L = \mathcal{I}(V)L[X_1, \ldots, X_n]$. Llamamos a V_L la variedad obtenida de V por **extensión de escalares** a L. El anillo de coordenadas de V_L es $L[V] = L \otimes C[V]$. Es claro que si V y W son variedades afines sobre C con $V \simeq W$ entonces $V_L \simeq W_L$.

Proposición 1.5. *Sean K, L cuerpos algebraicamente cerrados con $K \subset L$. Sean V, W variedades algebraicas afines definidas sobre K y V_L, W_L las variedades obtenidas de V y W por extensión de escalares a L. Si $V_L \simeq W_L$ entonces $V \simeq W$.*

La demostración se encuentra en la proposición 1.1.29. de [2].

Proposición 1.6. *Sea $\varphi : X \to Y$ un morfismo de variedades. Entonces $\varphi(X)$ contiene un subconjunto abierto no vacío de su clausura $\overline{\varphi(X)}$.*

La demostración se encuentra en la proposición 2.2.13. de [2].

Ahora introduciremos la noción de **dimensión de una variedad afín**. Si X es un espacio topológico noetheriano, definimos la dimensión de X como el supremo de todos los enteros n tales que existe una cadena $Z_0 \subset Z_1 \subset \cdots \subset Z_n$ de subconjuntos cerrados irreducibles distntos de X. Definimos la dimensión de una variedad afín como su dimensión vista como espacio topológico. Claramente la dimensión de una variedad afín es el máximo de las dimensiones de sus componentes irreducibles.

Proposición 1.7. *Sea X una variedad irreducible, sea Y un subconjunto irreducible propio cerrado de X. Entonces* $\dim Y < \dim X$.

La demostración se encuentra en la proposición 2.2.14. de [2].

Definición 1.8. Diremos que un conjunto es **constructible** si es una unión finita de conjuntos localmente cerrados. Recordemos que un subconjunto de un espacio topológico es localmente cerrado si es la intersección de un conjunto abierto con un conjunto cerrado.

El siguiente teorema nos muestra que los morfismos de variedades preservan la propiedad de un conjunto de ser constructible.

Teorema 1.9 (Teorema de Chevalley)**.** *Sea $\varphi : X \to Y$ un morfismo de variedades. Si S es un subconjunto constructible de X entonces $\varphi(S)$ es un subconjunto constructible de Y. En particular $\varphi(X)$ es un conjunto constructible.*

Prueba. Dado que un subconjunto localmente cerrado de una variedad es una variedad, es suficiente probar que $\varphi(X)$ es constructible. Podemos asumir que Y es irreducible. Trabajaremos por inducción sobre $\dim Y$.

Para $\dim Y = 0$ no hay nada que probar. Podemos asumir que φ es dominante. Por la proposición 1.6, existe un conjunto abierto U de Y contenido en $\varphi(X)$. Sean $W_1, \ldots, W_t$ las componentes irreducibles de $Y \backslash U$, por proposición 1.7 tenemos $\dim W_i < \dim Y$. Por hipótesis de inducción las restricciones de φ a $Z_i = \varphi^{-1}(W_i)$, $i = 1, \ldots, t$, tienen imágenes constructibles en W_i y por tanto constructibles en Y. Luego $\varphi(X)$ es la unión de U y una cantidad finita de $\varphi(Z_i)$ y por lo tanto $\varphi(X)$ es constructible. □

1.1.2. Grupos algebraicos

Definición 1.10. Un **grupo algebraico** sobre C es una variedad algebraica G definida sobre C, dotada de una estructura de grupo para el cual las aplicaciones $\mu : G \times G \to G$, donde $\mu(x, y) = xy$ y $\nu : G \to G$, donde $\nu(x) = x^{-1}$, son morfismos de variedades.

Dado un grupo algebraico G, diremos que H es un **subgrupo cerrado** de G si H es subgrupo de G y es un cerrado de la topologia de Zariski. Luego tenemos que un subgrupo cerrado de un grupo algebraico es un grupo algebraico, es decir H hereda la estructura de grupo algebraico de G.

Ejemplo 1.11. El grupo aditivo $\mathbb{G}_a(C) = (C, +)$ es la línea afín $\mathbb{A}^1$ con las operaciónes de grupo $\mu(x, y) = x + y$, $\nu(x) = -x$ y elemento neutro $e = 0$. El grupo multiplicativo $\mathbb{G}_m(C) = (C^*, .)$ es el conjunto C^* con las operaciónes de grupo $\mu(x, y) = xy$, $\nu(x) = -x$ y elemento neutro $e = 1$.

Ejemplo 1.12. El **grupo general lineal** $\mathrm{GL}(n, C)$ es el grupo de matrices inversibles $n \times n$ con entradas en C dotado con el producto de matrices. Notemos que podemos identificar el conjunto de matrices cuadradas $n \times n$ sobre C con el espacio afín de dimensión n^2, luego $\mathrm{GL}(n, C)$ es el complemento del conjunto de ceros del polinomio determinante $\det(X_{ij})$, es decir es una variedad afín. El anillo de coordenadas de $\mathrm{GL}(n, C)$ está generado por la restricción de las n^2 funciones coordenadas X_{ij} y la función $1/\det(X_{ij})$. Observamos de las fórmulas del producto e inversión de una matriz, que estas aplicaciones son dadas globalmente por funciones

racionales en las coordenadas X_{ij}, luego son morfismos de variedades. Así el grupo general lineal $\mathrm{GL}(n, C)$ es un grupo algebraico.

Diremos que G es un **grupo algebraico lineal** si G es un subgrupo cerrado de algún $\mathrm{GL}(n, C)$.

Ejemplo 1.13. Consideremos los siguientes subgrupos cerrados de $\mathrm{GL}(n, C)$:

(1) $\mathrm{SL}(n, C) = \{A \in \mathrm{GL}(n, C) : \det A = 1\}$ (grupo especial lineal)

(2) $\mathrm{T}(n, C) = \{(a_{ij}) \in \mathrm{GL}(n, C) : a_{ij} = 0, i > j\}$ (grupo triangular superior)

(3) $\mathrm{U}(n, C) = \{(a_{ij}) \in \mathrm{GL}(n, C) : a_{ii} = 1, a_{ij} = 0, i > j\}$ (grupo unipotente triangular superior)

(4) $\mathrm{D}(n, C) = \{(a_{ij}) \in \mathrm{GL}(n, C) : a_{ij} = 0, i \neq j\}$ (grupo diagonal)

Entonces todos estos son ejemplos de grupos algebraicos lineales.

Lema 1.14. *Sea E un subconjunto constructible de un espacio topológico X. Entonces E contiene un subconjunto denso abierto de su clausura.*

La demostración se encuentra en el lema 3.3.1. de [2].

Proposición 1.15. *Sea H un subgrupo de un grupo algebraico G y $\overline{H}$ su clausura.*

a) $\overline{H}$ es un subgrupo de G.

b) Si H es constructible, entonces $H = \overline{H}$.

La demostración se encuentra en la proposición 3.3.2. de [2].

Un **morfismo de grupos algebraicos** es un homomorfismo de grupos que es también un morfismo de variedades algebraicas.

Proposición 1.16. *Sea $\varphi : G \to G'$ un morfismo de grupos algebraicos, entonces*

a) $\mathrm{Ker}(\varphi)$ es un subgrupo cerrado de G

b) $\mathrm{Im}(\varphi)$ es un subgrupo cerrado de G'

La demostración se encuentra en la proposición 3.3.4. de [2].

1.2. Acciones de grupos algebraicos sobre variedades

En el estudio de grupos algebraicos es usual obtener información de sus acciones sobre sí mismos o sobre otras variedades naturalmente asociadas. Ahora veremos diversos resultados para este estudio y usaremos algunos de ellos para probar que todo grupo algebraico afín es isomorfo a un subgrupo cerrado de algún $\mathrm{GL}(n, C)$.

1.2.1. Linealización de grupos algebraicos afines

Sea G un grupo algebraico y V una variedad afín, si el morfismo

$$\begin{aligned} \varphi : G \times V &\to V \\ (x, v) &\mapsto \varphi(x, v) \end{aligned}$$

satisface las condiciones

1) $\varphi(y, \varphi(x, v)) = \varphi(yx, v)$ para todo $x, y \in G$ y $v \in V$,

2) $\varphi(e, v) = v$ para todo $v \in V$,

diremos que φ es una **acción** de G sobre V o que G **actúa sobre** V y usaremos la notación

$$\varphi(x, v) = x.v.$$

A partir de esta acción, podemos definir

$$\begin{aligned} \widetilde{\varphi} : G \times C[V] &\to C[V] \\ (x, f) &\mapsto x.f \end{aligned}$$

donde

$$(x.f)(v) = f(x^{-1}.v), \qquad \text{para todo } v \in V.$$

Luego es fácil verificar que $\widetilde{\varphi}$ satisface las condiciones de una acción. Así, la acción de G sobre V induce una acción de G sobre el anillo de coordenadas $C[V]$. Llamaremos a $x.f$ la **traslación** de f por x.

En particular, cuando $V = G$ podemos considerar dos acciones diferentes de G sobre si mismo. La acción de G por traslaciones a izquierda

$$\begin{aligned} G \times G &\to G \\ (x, y) &\mapsto xy \end{aligned}$$

y la acción de G por traslaciones a derecha

$$G \times G \to G$$
$$(x, y) \mapsto yx^{-1}.$$

Luego tenemos dos acciones diferentes de G sobre su anillo de coordenadas $C[G]$ asociadas a las acciones anteriores.

Para la acción de G sobre si mismo por traslaciones a izquierda corresponde la acción

$$G \times C[G] \to C[G]$$
$$(x, f) \mapsto \lambda_x(f) : y \to f(x^{-1}y)$$

y para la acción de G sobre si mismo por traslaciones a derecha,

$$G \times C[G] \to C[G]$$
$$(x, f) \mapsto \rho_x(f) : y \to f(yx)$$

Podemos usar traslaciones a derecha para caracterizar los miembros en un subgrupo cerrado:

Lema 1.17. *Sea H un subgrupo cerrado de un grupo algebraico G, I el ideal de $C[G]$ que se anula sobre H, entonces*

$$H = \{x \in G : \rho_x(I) \subset I\}$$

Prueba. Sea $x \in H$ y $f \in I$, probaremos que $\rho_x(f) \in I$. Sea entonces $y \in H$, tenemos $\rho_x(f)(y) = f(yx)$ y como $f \in I$ se tiene que $f(yx) = 0$.

Recíprocamente, sea $x \in G$ tal que $\rho_x(I) \subset I$, entonces para todo $f \in I$ se tiene que $\rho_x(f) \in I$. Luego para $e \in H$ tendremos $f(x) = f(ex) = \rho_x(f)(e) = 0$. Así $f(x) = 0$ para todo $f \in I$, es decir $x \in \mathcal{V}(I)$ y como H es cerrado $\mathcal{V}(I) = \mathcal{V}(\mathcal{I}(H)) = H$. □

Lema 1.18. *Sea G un grupo algebraico y V una variedad afin, ambas definidas sobre el cuerpo algebraicamente cerrado C. Supongamos que G actúa sobre V y sea F un $C-$subespacio vectorial de dimensión finita del anillo de coordenadas $C[V]$ entonces:*

a) Existe un subespacio de dimensión finita E de $C[V]$ y contiene a F que es estable bajo la acción de G.

b) F es estable bajo la acción de G si y solo sí $\varphi^*F \subset C[G] \otimes_C F$, donde $\varphi : G \times V \to V$ esta dada por $\varphi(x, v) = x^{-1}.v$.

Prueba.

a) Primero probaremos el resultado para el caso $\dim F = 1$. Sea $F = \langle f \rangle$ donde $f \in C[V]$. Sea

$$\begin{aligned} \psi : G \times V &\to V \\ (x, v) &\mapsto x.v \end{aligned}$$

el morfismo que nos da la acción de G sobre V, y

$$\begin{aligned} \psi^* : C[V] &\to C[G \times V] = C[G] \otimes C[V] \\ f &\mapsto \psi^* f = f \circ \psi \end{aligned}$$

el morfismo correspondiente entre sus anillos de coordenadas.

Sea $\psi^* f = \sum_{i=1}^{m} g_i \otimes h_i \in C[G] \otimes C[V]$ (notemos que esta expresión no es única). Para $x \in G$ y $v \in V$ tenemos

$$(x.f)(v) = f(x^{-1}.v) = f\left(\psi(x^{-1}, v)\right) = (\psi^* f)(x^{-1}, v) = \sum_{i=1}^{m} g_i(x^{-1}) h_i(v).$$

Luego $x.f = \sum_{i=1}^{m} g_i(x^{-1}) h_i$, así cada traslación $x.f$ está contenida en el $C-$espacio vectorial de dimensión finita de $C[V]$ generado por las funciones h_i. De la acción de G sobre $C[V]$ tenemos que $y.(x.f) = (yx).f$ y $e.f = f$ para todo $f \in C[V]$.

Así, el $C-$espacio vectorial $E = \langle x.f : x \in G \rangle$ es de dimensión finita, contiene a f y es $G-$estable.

Ahora para el caso general, sea $\dim F = n$ y sea $\{f_1, \ldots, f_n\} \subset C[V]$ una base de F sobre C. Hemos probado antes que para cada $F_i = \langle f_i \rangle$ existe $E_i = \langle x.f_i : x \in G \rangle$ espacio vectorial $G-$estable de dimensión finita que contiene a f_i. Sea $E = \bigoplus_{i=1}^{n} E_i$, entonces E es un espacio vectorial $G-$estable de dimesión finta que contiene a F.

b) Igual que para la parte a), primero probaremos el resultado para el caso $\dim F = 1$ es decir $F = \langle f \rangle$ donde $f \in C[V]$. Si $\varphi^* F \subset C[G] \otimes_C F$ entonces

$\varphi^* f = \sum g_i \otimes h_i \in C[G] \otimes_C F$ luego $h_i \in F$. Así, dados $x \in G$ y $v \in V$ tenemos

$$(x.f)(v) = f(x^{-1}.v) = f(\varphi(x,v)) = (\varphi^* f)(x,v) = \sum g_i(x)h_i(v)$$

entonces $x.f = \sum g_i(x)h_i \in F$ es decir, F es $G-$estable. Ahora para el caso general, sea $\dim F = n$ y sea $\{f_1, \ldots, f_n\} \subset C[V]$ una base de F sobre C. Sea $f = \sum_{j=1}^{n} c_j f_j$ donde $c_j \in C$. Dado $x \in G$ tenemos que $x.f = \sum_{j=1}^{n} c_j(x.f_j)$ y por lo antes visto tenemos que cada $x.f_j \in F_j = \langle f_j \rangle$, así $x.f \in \bigoplus_{j=1}^{n} F_j = F$.

Probaremos ahora el recíproco: sea $\{f_1, \ldots, f_n\} \subset C[V]$ una base de F sobre C y la extendemos a una base $\{f_1, \ldots, f_n\} \cup \{\psi_1, \ldots, \psi_m\}$ de $C[V]$, entonces dada $f \in F$ podemos expresar $\varphi^* f$ como

$$\varphi^* f = \sum_{i=1}^{n} r_i \otimes f_i + \sum_{j=1}^{m} s_j \otimes \psi_j.$$

Como F es $G-$estable entonces

$$x.f = \sum_{i=1}^{n} r_i(x) f_i + \sum_{j=1}^{m} s_j(x)\psi_j \in F$$

luego $s_j(x) = 0$ para todo $x \in G$ por lo tanto $s_j = 0$. Así

$$\varphi^* f = \sum_{i=1}^{n} r_i \otimes f_i$$

es decir $\varphi^* F \subset C[G] \otimes_C F$.

Así, el lema queda demostrado. □

Observación 1.19. *Sea G un grupo algebraico y consideremos la acción de G en si mismo por traslaciones a derecha. Por la demostración de la parte a) del lema anterior tenemos que para cada $x \in G$, el $C-$espacio vectorial de $C[G]$ generado por la traslación $\rho_x(f)$ es de dimensión finita, $G-$estable y contiene a f. Además, si $F_f = \langle \rho_x(f) : x \in G \rangle$, entonces tenemos*

$$C[G] = \bigcup_{f \in C[G]} F_f.$$

Así, podemos expresar el anillo de coordenadas de un grupo algebraico como unión de subespacios de dimensión finita y estables por la acción de G.

Sabemos que cualquier subgrupo cerrado de $\mathrm{GL}(n, C)$ es un grupo algebraico lineal, ahora veremos que el recíproco también es cierto, para eso construiremos un subespacio de dimensión finita de $C[G]$ sobre el cual G actúa por traslaciones.

Teorema 1.20. *Sea G un grupo algebraico afin. Entonces G es isomorfo a un subgrupo cerrado de algún* $\mathrm{GL}(n, C)$.

Prueba. Sean $f_1, \ldots, f_n$ generadores de $C[G]$ como $K-$álgebra y sea F el subespacio vectorial generado por los f_i sobre C.

Consideremos la acción de G en si mismo por traslaciones a derecha, entonces por el lema 1.18 parte a) existe un subespacio de dimensión finita $E \subset C[V]$ que es $G-$estable y contiene a F. Podemos asumir que los f_i son una base de E sobre C.

Definimos $\varphi : G \times G \to G$ por $\varphi(x, y) = x^{-1}.y = yx$, entonces por el lema 1.18 parte b) tenemos $\varphi^* \subset C[G] \otimes_C E$ pues E es $G-$estable. De este modo $\varphi^* f_i \in C[G] \otimes_C E$. Sea

$$\varphi^* f_i = \sum_j m_{ij} \otimes f_j \quad \text{donde } m_{ij} \in C[G]$$

entonces

$$\rho_x(f_i)(y) = f_i(yx) = f_i(\varphi(x, y)) = \varphi^* f_i(x, y) = \sum_j m_{ij}(x) \otimes f_j(y)$$

luego

$$\rho_x(f_i) = \sum_j m_{ij}(x) \otimes f_j$$

es decir, la matriz de $\rho_{x|_F}$ en la base $\{f_i\}$ es $(m_{ij}(x))$. En este contexto, la aplicación

$$\psi : G \to GL(n, C)$$
$$x \mapsto (m_{ij}(x))$$

es un morfismo de grupos algebraicos. Por la proposición 1.16, la imagen $\psi(G) = G'$ es un subgrupo cerrado de $GL(n, C)$. Probaremos entonces que $\psi : G \to G'$ es un isomorfismo de variedades, para esto veremos que $\psi^* : C[G'] \to C[G]$ es un isomorfismo.

Notamos que $f_i(x) = f_i(ex) = \sum_j m_{ij}(x) f_j(e)$ es decir $f_i = \sum_j f_j(e) m_{ij}$. Esto nos muestra que los m_{ij} también son un conjunto de generadores de $C[G]$, entonces ψ^* es inyectiva. Por otro lado

$$\psi^*(X_{ij|_{G'}})(x) = (X_{ij|_{G'}} \circ \psi)(x) = (X_{ij|_{G'}})(m_{ij}(x)) = m_{ij}(x)$$

entonces $\psi^*(X_{ij|_{G'}}) = m_{ij}$ luego ψ^* es sobreyectiva. $\square$

1.2.2. Caracteres y semi-invariantes

Definición 1.21. Sea G un grupo algebraico, un **caracter** de G es un morfismo de grupos algebraicos $G \to \mathbb{G}_m$.

Si χ_1, χ_2 son caracteres de un grupo algebraico G, también lo es su producto definido por $(\chi_1\chi_2)(x) = \chi_1(x)\chi_2(x)$. Con este producto el conjunto $X(G)$ de todos los caracteres de G tiene estructura de grupo conmutativo. El elemento identidad es el caracter χ_0 tal que $\chi_0(x) = 1$ para todo $x \in G$.

Si G es un subgrupo cerrado de $GL(V)$, para cada $\chi \in X(G)$ definimos $V_\chi = \{v \in V : x.v = \chi(x)v \text{ para todo } x \in G\}$. Evidentemente V_χ es un subespacio $G-$estable de V.Cualquier elemento distinto de cero de V_χ es llamado un semi-invariante de G de peso χ. Reciprocmente, si v es un vector distinto de cero que genera una linea $G-$estable en V, entonces es claro que $x.v = \chi(x)v$ define un caracter χ de G.

En general, si $\varphi : G \to GL(V)$ es una **representación racional**, es decir una aplicación racional que es un homomorfismo de grupos, entonces definiremos los semi-invariantes de G como los semi-invariantes de $\varphi(G)$.

Lema 1.22. *Sea $\varphi : G \to GL(V)$ una representación racional. Entonces los subespacios V_χ, $\chi \in X(G)$ están en suma directa. En particular sólo una cantidad finita de ellos son distintos de cero.*

La demostración se encuentra en el lema 3.6.5. de [2].

Lema 1.23. *Sea $\varphi : G \to GL(V)$ una representación racional y sea H un subgrupo normal cerrado de G. Entonces cada elemento de $\varphi(G)$ permuta los espacios V_χ para $\chi \in X(H)$.*

La demostración se encuentra en el lema 3.6.6. de [2].

1.2.3. Cocientes en grupos algebraicos

El propósito de esta sección es probar que si G es un grupo algebraico lineal y H es un subgrupo normal cerrado de G, entonces el cociente G/H tiene la estructura natural de grupo algebraico lineal, con anillo de coordenadas $C[G/H] \simeq C[G]^H$.

Si V es un $C-$espacio vectorial de dimensión finita, entonces $GL(V)$ actúa sobre potencias exteriores de V por $x.(v_1 \wedge \cdots \wedge v_k)$. Si M es un subespacio $d-$dimensional

de V, es espacialmente útil observar la acción sobre $L = \wedge^d M$, que es un subespacio de dimensión 1 de $\wedge^d V$.

Lema 1.24. *Sea $x \in GL(V)$, M un subespcio de V de dimensión d y $L = \wedge^d M$, entonces $xL = L$ si y sólo si $xM = M$.*

Prueba. Supongamos que $xL = L$. Sea $v_1, \ldots, v_l$ una base de $M \cap xM$, extendemos a una base $v_1, \ldots, v_d$ de M y a una base $v_1, \ldots, v_l, v_{d+1}, \ldots, v_{2d-l}$ de xM. Por hipótesis $x(v_1 \wedge \cdots \wedge v_d)$ es un múltiplo de $v_1 \wedge \cdots \wedge v_d$ pero por otro lado, también es un múltiplo de $v_1 \wedge \cdots \wedge v_l \wedge v_{d+1} \cdots \wedge v_{2d-l}$ así $l = d$ y por lo tanto $xM = M$. El recíproco es claro. □

Proposición 1.25. *Sea G un grupo algebraico y H un subgrupo cerrado de G. Entonces existe una representación racional $\varphi : G \to GL(V)$ y un subespacio L de V de dimensión 1 tal que $H = \{x \in G : \varphi(x)L = L\}$.*

Prueba. Sea I el ideal de $C[V]$ que se anula en H. Es un ideal finitamente generado. Por el lema 1.18 existe un subespacio de dimensión finita W de $C[G]$, estable por todos los ρ_x, $x \in G$, que contiene un conjunto finito de generadores de I. Sea $M = W \cap I$, entonces M genera I. Notemos que M es estable por todos los ρ_x, $x \in H$, pues por lema 1.17, $H = \{g \in G : \rho_g I = I\}$.

Probaremos que $H = \{x \in G : \rho_x M = M\}$. Si $\rho_g M = M$, como M genera I entonces $\rho_x I = I$ así $x \in H$. Ahora, sean $V = \wedge^d W$ y $L = \wedge^d M$ donde $d = \dim M$. Por el lema 1.24, tenemos la caracterización deseada de H. □

Teorema 1.26. *Sea G un grupo algebraico y H un subgrupo cerrado normal de G. Entonces existe una representación racional $\psi : G \to \mathrm{GL}(W)$ tal que $H = \mathrm{Ker}\psi$.*

Prueba. Por la proposición 1.25, existe un morfismo $\varphi : G \to GL(V)$ y una linea L tal que $H = \{x \in G : \varphi(x)L = L\}$. Como cada elemento de H actúa sobre L por multiplicación escalar, esta acción tiene asociado un caracter $\chi_0 : H \to \mathbb{G}_m$. Consideremos la suma en V de todos los V_χ distintos de cero para todos los caracteres χ de H. Por lema 1.22, esta suma es directa y contiene a L. Es más, por lema 1.23, $\varphi(G)$ permuta los V_χ. Así, podemos asumir que V es la suma de los V_χ.

Sea W el subespacio de $\mathrm{End}(V)$ cuyos elementos dejan estable V_χ para todo $\chi \in X(H)$. Existe un isomorfismo natural entre W y $\oplus\mathrm{End}(V_\chi)$. Ahora $\mathrm{GL}(V)$

actúa sobre $\mathrm{End}(V)$ por conjugación. Como $\varphi(G)$ permuta los v_χ y W estabiliza a cada uno de estos, entonces el subgrupo $\varphi(G)$ estabiliza a W. Luego podemos definir el morfismo de grupos $\psi : G \to \mathrm{GL}(W)$ dado por

$$\psi(x)(y) = \varphi(x)_{|W} y \varphi(x)^{-1}_{|W},$$

así ψ es una representación racional. Veamos que $\mathrm{Ker}(\psi) = H$. Sea $x \in H$, entonces $\psi(x)$ actúa como escalar sobre cada V_χ, luego la conjugación por $\psi(x)$ no tiene efecto sobre W, así $x \in \mathrm{Ker}(\psi)$. Reciprocamente, sea $x \in G$ tal que $\psi(x) = id_W$. Entonces $\psi(x)$ estabiliza todos los V_χ y conmuta con $\mathrm{End}(V_\chi)$, pero el centro de $\mathrm{End}(V_\chi)$ es el conjunto de escalares, luego $\psi(x)$ actúa sobre cada V_χ como escalar. En particular, $\psi(x)$ estabiliza $L \subset V_{\chi_0}$, así $x \in H$. □

Corolario 1.27. *El cociente G/H puede ser dotado de una estructura de grupo algebraico afin, dotado de un epimorfismo $\pi : G \to G/H$.*

Prueba. Consideremos la representación $\psi : G \to \mathrm{GL}(W)$ con núcleo H dada por el teorema 1.26 e imagen $Y = \mathrm{Im}(\psi)$. Por el teorema 1.9 tenemos que Y es un conjunto constructible y como es un subgrupo de $\mathrm{GL}(W)$, por la proposición 1.15 se tiene que Y es un subgrupo cerrado de $GL(W)$. Luego tenemos el isomorfismo de grupos $G/H \simeq Y$ entonces podemos trasladar la estructura de grupo algebraico lineal de Y a G/H. Es más, ψ induce un epimorfismo de grupos algebraicos $\pi : G \to G/H$. □

Definición 1.28. Sea G un grupo algebraico y H un subgrupo algebraico cerrado de G. Un **cociente de Chevalley** de G por H es una variedad X junto con un morfismo sobreyectivo $\pi : G \to X$ tal que las fibras de π son exactamente los cocientes de H en G.

En el corolario 1.27 hemos establecido que existe un cociente de Chevalley de un grupo algebraico lineal G por un subgrupo normal cerrado H. Sin embargo, no está claro si los cocientes de Chevalley son únicos salvo isomorfismo, ni si ellos satisfacen la propiedad universal usual de cocientes. Estas propiedades caracterizan los cocientes categóricos que definiremos a continuación:

Definición 1.29. Sea G un grupo algebraico y H un subgrupo cerrado de G. Un **cociente categórico** de G por H es una variedad X junto con un epimorfismo $\pi : G \to X$ que es constante en todos los cocientes de H en G con la siguiente

propiedad universal: dada cualquier otra variedad Y y un morfismo $\psi : G \to Y$ que es constante en todos los cocientes de H en G, existe un único morfismo $\overline{\psi} : X \to Y$ tal que $\psi = \overline{\psi} \circ \pi$.

Es claro que los cocientes categoricos son únicos salvo único isomorfismo. Queremos probar que los cocientes de Chevalley son cocientes categoricos, así obtendremos un cociente de G por H definido unicamente salvo isomorfismo y que satisface la propiedad universal.

Teorema 1.30. *Los cocientes de Chevalley son cocientes categóricos.*

La demostración se encuentra en el teorema 3.7.7. de [2].

Proposición 1.31. *Sea G un grupo algebraico lineal, H un subgrupo normal cerrado de G, entonces $C[G/H] \simeq C[G]^H$.*

Prueba. Consideremos el epimorfismo π dado por el corolario 1.27. Si un elemento $f \in C[G/H]$, entonces $\widetilde{f} = f \circ \pi \in C[G]$. Es más, cuando $x \in H$ y $y \in G$, se obtiene

$$\lambda_x(\widetilde{f})(y) = \widetilde{f}(x^{-1}y) = (f \circ \pi)(x^{-1}y) = f(\pi(x^{-1}y)) = f(\pi(y)) = \widetilde{f}(y),$$

luego $\lambda_x(\widetilde{f}) = \widetilde{f}$ y $\widetilde{f} \in C[G]^H$.

Si $f \in C[G]^H$, entonces f es un morfismo $G \to \mathbb{A}^1$ que es constante sobre los cocientes de H en G. Entonces por la propiedad unniversal del cociente G/H establecida en el teorema 1.30, existe $F \in C[G/H]$ tal que $f = F \circ \pi$. □

1.3. Descomposición de grupos algebraicos

Comenzaremos la pressente sección, estudiando la descomposición de Jordan Chevalley aditiva y multiplicativa para el caso de dimensión finita, y a partir de este estudiaremos el caso de dimensión infinita. Usaremos la versión de dimensión infinita para estudiar las traslaciones a derecha ρ_x sobre el anillo de coordenadas $C[G]$ de un grupo algebraico G.

Primero mostraremos que ρ preserva la descomposición de Jordan para $\mathrm{GL}(n, C)$, luego veremos que la descomposición de Jordan puede ser definida intrínsecamente para un grupo algebraico afin arbitrario.

Finalmente, mostraremos que los morfismos de grupos algebraicos preservan la descomposición de Jordan Chevalley.

A lo largo de esta sección, C denotará un cuerpo (algebraicamente cerrado, como mencionamos al comienzo de este capítulo), V denotará un C-espacio vectorial de dimensión finita y W un C-espacio vectorial de dimensión infinita.

Definición 1.32. Sea $x \in \mathrm{End}(V)$ donde V es un espacio vectorial de dimensión finita sobre el cuerpo C.

a) Diremos que x es **nilpotente** si $x^n = 0$ para algún $n \in \mathbb{N}$ (equivalentemente, si 0 es el único autovalor de x).

b) Diremos que x es **semisimple** si el polinomio minimal de x tiene raíces diferentes (equivalentemente, si x es diagonalizable sobre C).

c) Sea $x \in \mathrm{GL}(V)$. Diremos que x es **unipotente** si es la suma de la identidad y un endomorfismo nilpotente, ó equivalentemente, si 1 es su único autovalor.

Lema 1.33 (Descomposición de Jordan Chevalley aditiva)**.** *Sea $x \in \mathrm{End}(V)$:*

a) Existen únicos $x_s, x_n \in \mathrm{End}(V)$ tales que x_s es semisimple, x_n es nilpotente y $x = x_s + x_n$.

b) Existen polinomios $p(X), q(X) \in C[X]$ sin término independiente tales que $x_s = p(x)$, $x_n = q(x)$. Entonces x_s y x_n conmutan con cualquier endomorfismo de V que conmuta con x, y en particular conmutan entre ellos.

c) Si $W_1 \subset W_2$ son subespacios de V, y x lleva a W_2 en W_1, también lo hacen x_s y x_n.

d) Sea $y \in \mathrm{End}(V)$. Si $xy = yx$, entonces $(x+y)_s = x_s + y_s$ y $(x+y)_n = x_n + y_n$

*La descomposición $x = x_s + x_n$ es llamada **descomposición de Jordan Chevalley aditiva** de x, donde x_s es llamada la parte semisimple de x y x_n la parte nilpotente de x.*

Para la demostración de este lema se puede consultar [6].

A partir de esta descomposición aditiva, se obtiene una versión multiplicativa de la descomposición de Jordan Chevalley cuando $x \in \mathrm{End}(V)$ es un endomorfismo inversible.

En efecto, si $x \in \mathrm{GL}(V)$, sus autovalores son distintos de cero, luego x_s también es inversible. Así podemos escribir $x_u := 1 + x_s^{-1}x_n$ y obtendremos que $x = x_s + x_n = x_s(1 + x_s^{-1}x_n) = x_s.x_u$.

Lema 1.34 (Descomposición de Jordan Chevalley multiplicativa)**.** *Sea $x \in \mathrm{GL}(V)$:*

a) Existen únicos $x_s, x_u \in \mathrm{GL}(V)$ tales que x_s es semisimple, x_u es unipotente y $x = x_s x_u = x_u x_s$.

b) x_s y x_u conmutan con cualquier endomorfismo de V que conmute con x.

c) Si U es un subespacio de V estable por x, entonces U es estable por x_s y x_u.

d) Sea $y \in \mathrm{GL}(V)$. Si $xy = yx$, entonces $(xy)_s = x_s y_s$ y $(xy)_u = x_u y_u$.

La descomposición $x = x_u x_s$ es llamada ***descomposición de Jordan Chevalley multiplicativa*** *de x, donde x_s es llamada la parte semisimple de x y x_u la parte unipotente de x.*

Para la demostración de este lema se puede consultar [6].

En la sección 1.2 vimos que un grupo algebraico afin G actúa sobre si mismo por traslaciones a derecha, luego cada $x \in G$ define un morfismo $G \to G$ dado por $y \mapsto yx$, el cual induce un morfismo $\rho_x : C[G] \to C[G]$ definido por $\rho_x(f)(y) = f(yx)$.

Seria útil conocer la descomposición de Jordan Chevalley de este mapeo lineal para todo $x \in G$, sin embargo $C[G]$ en general es un $C-$espacio vectorial de dimensión infinita. Los resultados que hemos visto solo se aplican al caso de dimensión finita, por tanto extenderemos la definición al caso de dimensión infinita y mostraremos la versión de las descomposiciones de Jordan Chevalley aditiva y multiplicativa de dimensión infinita.

Definición 1.35. Sea W un $C-$espacio vectorial de dimensión infinita y sea $x \in \mathrm{End}(W)$. Si

$$W = \bigcup_{\lambda \in I} V_\lambda$$

donde los V_λ son $C-$subespacios vectoriales de dimensión finita de W tales que $x(V_\lambda) \subset V_\lambda$, entonces:

a) Diremos que x es semisimple si y sólo si $x_{|_{V_\lambda}}$ es semisimple para todo $\lambda \in I$.

b) Diremos que x es nilpotente si y sólo si $x_{|_{V_\lambda}}$ es nilpotente para todo $\lambda \in I$.

c) Si además $x \in \mathrm{GL}(V_\lambda)$ para todo $\lambda \in I$, diremos que x es unipotente si y sólo si $x_{|_{V_\lambda}}$ es unipotente para todo $\lambda \in I$.

La hipótesis que hará posible la descomposición de un endomorfismo de W es que W es la unión de subespacios estables por x y de dimensión finita, pues para el caso de dimensión finita ya tenemos el resultado dado en el lema 1.33 y podemos descomponer cada una de las restricciones:

$$x_{|V_\lambda} = (x_{|V_\lambda})_s + (x_{|V_\lambda})_n.$$

Agrupando los $(x_{|V_\lambda})_s$ y los $(x_{|V_\lambda})_n$ obtenemos los endomorfismos semisimple y nilpotente $x_s, x_n \in \mathrm{End}(W)$ tales que $x = x_s + x_n$.

Proposición 1.36 (Descomposición de Jordan Chevalley aditiva de dimensión infinita)**.** *Sean W y $x \in \mathrm{End}(W)$ en las condiciones de la definición 1.35.*

a) Existen únicos $x_s, x_n \in \mathrm{End}(W)$ tales que x_s es semisimple, x_n es nilpotente y $x = x_s + x_n$.

b) Si $V \subset W$ es estable por x, entonces V es estable por x_s y x_n.

Prueba. Como W es unión de $C-$subespacios vectoriales de dimensión finita y estables por x, para cada restricción $x_{|V_\lambda} : V_\lambda \to V_\lambda$ existe la descomposición de Jordan Chevalley aditiva. Sean $\alpha, \beta \in I$, tenemos:

$$x_{|V_\alpha} = (x_{|V_\alpha})_s + (x_{|V_\alpha})_n$$
$$x_{|V_\beta} = (x_{|V_\beta})_s + (x_{|V_\beta})_n$$

Por el lema 1.33 parte c) se tiene que la restricción de un endomorfismo semisimple es también semisimple, y de igual manera la restricción de un endomorfismo nilpotente es también nilpotente. Así

$$((x_{|V_\alpha})_s)_{|V_\alpha \cap V_\beta}, ((x_{|V_\beta})_s)_{|V_\alpha \cap V_\beta}$$

son semisimples y

$$((x_{|V_\alpha})_n)_{|V_\alpha \cap V_\beta}, ((x_{|V_\beta})_n)_{|V_\alpha \cap V_\beta}$$

son nilpotentes. Podemos descomponer $x_{|V_\alpha \cap V_\beta}$ de dos maneras:

$$(x_{|V_\alpha})_{|V_\alpha \cap V_\beta} = ((x_{|V_\alpha})_s)_{|V_\alpha \cap V_\beta} + ((x_{|V_\alpha})_n)_{|V_\alpha \cap V_\beta}$$
$$(x_{|V_\beta})_{|V_\alpha \cap V_\beta} = ((x_{|V_\beta})_s)_{|V_\alpha \cap V_\beta} + ((x_{|V_\beta})_n)_{|V_\alpha \cap V_\beta}$$

y por la unicidad de la descomposición tenemos

$$((x_{|V_\alpha})_s)_{|V_\alpha \cap V_\beta} = ((x_{|V_\beta})_s)_{|V_\alpha \cap V_\beta} \quad \text{y} \quad ((x_{|V_\alpha})_n)_{|V_\alpha \cap V_\beta} = ((x_{|V_\beta})_n)_{|V_\alpha \cap V_\beta}$$

Así podemos agrupar juntos los $(x_{|V_\lambda})_s$ (respectivamente $(x_{|V_\lambda})_n$) para obtener endomorfismos de W cuya suma es x. Estos pueden ser denotados nuevamente x_s, x_n y llamadas las partes de Jordan de x. □

Podemos hacer un proceso similar para obtener la versión multiplicativa.

Proposición 1.37 (Descomposición de Jordan Chevalley multiplicativa de dimensión infinita)**.** *Sean W y $x \in \mathrm{GL}(W)$ en las condiciones de la definición 1.35.*

a) Existen únicos $x_s, x_u \in \mathrm{GL}(V)$ tales que x_s es semisimple, x_u es unipotente, x_s, x_u conmutan entre sí, y $x = x_s x_u$.

b) Si $U \subset W$ es estable por x, entonces U es estable por x_s y x_u.

Prueba. La prueba es similar a la prueba de la proposición anterior. Es importante observar, usando el lema 1.34 parte c), que $(x_{|V_\lambda})_s$ y $(x_{|V_\lambda})_u$ dejan estable cada subespacio de U (de dimensión finita ó no) que es estable por x, luego U es estable por x_s y x_u. □

El objetivo de estudiar la descomposición de Jordan Chevalley de dimensión infinita es poder descomponer el morfismo $\rho_x : C[G] \to C[G]$. En la observación 1.19 vimos que $C[G]$ es la unión de subespacios de dimensión finita estables por ρ_x. Entonces para todo ρ_x existe la descomposición de Jordan multiplicativa. Veremos ahora que cuando $G = \mathrm{GL}(n, C)$, la descomposición de Jordan de ρ_x proviene de la descomposición de Jordan de x.

Proposición 1.38 (Descomposición de Jordan Chevalley en el grupo general lineal)**.** *Sea $x \in G = \mathrm{GL}(n, C)$ con descomposición de Jordan Chevalley*

$$x = x_s x_u,$$

entonces $\rho_x : C[G] \to C[G]$ tiene descomposición de Jordan

$$\rho_x = \rho_{x_s} \rho_{x_u}.$$

Prueba. Como $C[G]$ es la unión de subespacios de dimensión finita estables por todos los ρ_x, existen las descomposiciones de Jordan. Es más

$$\rho_x(f)(y) = f(yx) = f(yx_sx_u) = \rho_{x_u}(f)(yx_s) = \rho_{x_s}(\rho_{x_u}(f))(y) = (\rho_{x_s}\rho_{x_u})(f)(y)$$

entonces $\rho_x = \rho_{x_s}\rho_{x_u}$ y los operadores conmutan. Luego bastará probar que ρ_{x_s} es semisimple y ρ_{x_u} es unipotente.

El anillo de coordenadas $C[G]$ es el anillo de polinomios en n^2 indeterminadas X_{ij} localizado en el sistema multiplicativo de potencias de $d = \det(X_{ij})$. Veamos que $C[X_{ij}]$ es estable bajo la traslación a derecha. Sean $x, y \in G$

$$\rho_x(X_{ij})(y) = X_{ij}(yx) = \sum_{h=1}^{n} y_{ih}x_{hj} = \sum_{h=1}^{n} X_{ih}(y)x_{hj}$$

entonces $\rho_x X_{ij} = \sum_{h=1}^{n} x_{hj}X_{ih} \in C[X_{ij}]$.

Veamos ahora como actúa G sobre d. Sean $x, y \in G$

$$\rho_x(d)(y) = d(yx) = \det(y)\det(x)$$

entonces $\rho_x d = \det(x)d$, es decir el espacio vectorial generado por d es $G-$estable. Así, podremos describir la acción de ρ_x sobre $C[G]$, si se conoce la acción sobre $C[X_{ij}]$.

En particular, como d es un autovector de ρ_x en cualquier caso, tenemos que:

- Si $\rho_{x|_{C[X_{ij}]}}$ es semisimple, entonces ρ_x es semisimple.
- Si $\rho_{x|_{C[X_{ij}]}}$ es unipotente entonces su autovalor $\det(x)$ debe ser 1, así ρ_x es unipotente.

□

Si G es un subgrupo de $\mathrm{GL}(n, C)$ y $x \in G$, no necesariamente $x_s \in G$ ó $x_u \in G$. Veremos que esto sí se cumple cundo G es un subgrupo cerrado.

Corolario 1.39. *Sea G un subgrupo cerrado de $\mathrm{GL}(n, C)$ y $x \in G$, entonces x_s, $x_u \in G$.*

Prueba. Si G es cerrado y $x \in G$, por el lema 1.17 bastará probar que ρ_{x_s} y ρ_{x_u} dejan estable al ideal $\mathcal{I}(G) \subset C[\mathrm{GL}(n, C)]$. Por la proposición 1.38, $(\rho_x)_s = \rho_{x_s}$ y $(\rho_x)_u = \rho_{x_u}$. Como $\mathcal{I}(G)$ es estable por ρ_x (pues $x \in G$), por lema 1.34, $\mathcal{I}(G)$ será estable por $(\rho_x)_s$ y $(\rho_x)_u$. □

Ahora veremos que podemos considerar la descomposición de Jordan para elementos en cualquier grupo algebraico afin.

Proposición 1.40. *Sea G un grupo algebraico afín.*

a) Si $x \in G$, entonces existen únicos elementos $s, u \in G$ tales que $x = su$, s y u conmutan, ρ_s es semisimple, ρ_u es unipotente. Llamamos a s y u la parte semisimple y unipotente de x respectivamente y las denotamos por x_s y x_u.

b) Si $\psi : G \to \widetilde{G}$ es un morfismo de grupos algebraicos, entonces $(\psi(x))_s = \psi(x_s)$ y $(\psi(x))_u = \psi(x_u)$.

Prueba.

a) Por el teorema 1.20 existe un isomorfismo $\psi : G \to G'$ donde G' es un subgrupo cerrado de algún $\mathrm{GL}(n, C)$.

Sea $\psi(x) = x' = s'u'$ su descomposición de Jordan en $\mathrm{GL}(n, C)$. Por la proposición 1.38 tenemos $(\rho_{x'})_s = \rho_{s'}$ y $(\rho_{x'})_u = \rho_{u'}$.

Sea $I = \mathcal{I}(G') = \{f \in C[\mathrm{GL}(n, C)] : f_{|_{G'}} = 0\}$, por el lema 1.17 como $x' \in G'$ entonces $\rho_{x'}$ estabiliza I. Luego por observación, $(\rho_{x'})_s$ y $(\rho_{x'})_u$ también estabilizan I, y nuevamente por el lema 1.17 tenemos que $s', u' \in G'$. Así

$$x = \psi^{-1}(x') = \psi^{-1}(s'u') = \psi^{-1}(s')\psi^{-1}(u')$$

donde $\psi^{-1}(s') = x_s$ y $\psi^{-1}(u') = x_u \in G$.

b) Consideremos ψ como una composición de morfismos:

$$G \xrightarrow{\psi} \psi(G) \xrightarrow{i} \widetilde{G}$$

Mostraremos que en cada uno de estos morfismos, se preservan las descomposiciones de Jordan.

Consideremos el primer paso, donde $\psi : G \to \psi(G) = G''$ es un epimorfismo. La traslación a derecha $\rho_{\psi(x)} : C[G''] \to C[G'']$ es la restricción de $\rho_x : C[G] \to C[G]$ si vemos a $C[G'']$ como subanillo de $C[G]$ vía la inyección ψ^*

$$\begin{array}{ccc} C[G''] & \xrightarrow{\rho_{\psi(x)}} & C[G''] \\ {\scriptstyle \psi^*}\downarrow & & \downarrow{\scriptstyle \psi^*} \\ C[G] & \xrightarrow[\rho_x]{} & C[G] \end{array}$$

Pero la restricción de un operador semisimple (respectivamente unipotente) a un subespacio, es del mismo tipo. Entonces ρ_{x_s} es semisimple y ρ_{x_u} es unipotente. Como $\rho_{\psi(x)} = \rho_{\psi(x_s)}\rho_{\psi(x_u)}$ entonces $(\rho_{\psi(x)})_s = \rho_{\psi(x_s)}$ y $(\rho_{\psi(x)})_u = \rho_{\psi(x_u)}$, pero por la proposición 1.38 tenemos $(\rho_{\psi(x)})_s = \rho_{(\psi(x))_s}$ y $(\rho_{\psi(x)})_u = \rho_{(\psi(x))_u}$. Así $(\psi(x))_s = \psi(x_s)$ y $(\psi(x))_u = \psi(x_u)$.

Luego la proposición queda demostrada. □

Ejemplo 1.41. Consideremos el subgrupo de $\mathrm{GL}(2, C)$:

$$G = \left\{ \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} : a \in C \right\}$$

y el isomorfismo

$$\begin{aligned} \varphi : (\mathbb{G}_a(C), +) &\to (G, \cdot) \\ a &\mapsto \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \end{aligned}$$

Entonces tenemos que todo elemento de $\mathbb{G}_a(C)$ es unipotente.

Ejemplo 1.42. Consideremos el subgrupo de $\mathrm{GL}(2, C)$:

$$G = \left\{ \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} : a \in C \right\}$$

y el isomorfismo

$$\begin{aligned} \varphi : (\mathbb{G}_m(C), \cdot) &\to (G, \cdot) \\ a &\mapsto \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} \end{aligned}$$

Entonces tenemos que todo elemento de $\mathbb{G}_m(C)$ es semisimple.

Ejemplo 1.43. No existen homomorfismos no triviales de $\mathbb{G}_a$ en $\mathbb{G}_m$. En efecto, supongamos que existe un homomorfismo no trivial $\psi : \mathbb{G}_a \to \mathbb{G}_m$. Sea $x \in \mathbb{G}_a$, por el ejemplo 1.41 tenemos que x es unipotente, entonces por la proposición 1.40 b) tendremos que $\psi(x) \in \mathbb{G}_m$ es también unipotente. Sin embargo, en el ejemplo 1.42 vimos que todo elemento de $\mathbb{G}_m$ es semisimple. Como el único elemento que es unipotente y semisimple a la vez es la identidad, ψ es el homomorfismo trivial $\psi(x) = 1$. Así obtenemos $X(\mathbb{G}_a) = 1$.

Ejemplo 1.44. Un subgrupo cerrado H del grupo unipotente triangular superior $U(n, C)$ no tiene caracteres no triviales. En efecto, un caracter no trivial de H induciria un caracter no trivial de $\mathbb{G}_a$ en $\mathbb{G}_m$.

La proposición 1.40 nos dice que en cualquier grupo algebraico afín, los subconjuntos

$$G_s = \{x \in G : x = x_s\} \quad \text{y} \quad G_u = \{x \in G : x = x_u\}$$

quedan intrinsecamente definidos y su intersección es el elemento neutro e. La parte b) de esta proposición nos dice que los morfismos de grupos algebraicos preservan los conjuntos G_s y G_u. Es más, como el conjunto de matrices unipotentes en GL(n, C) es el conjunto de ceros del polinomio $(x-1)^n = 0$, entonces G_u es un conjunto cerrado. Sin embargo, en general G_s no es un subconjunto cerrado de G.

Definición 1.45. Denotaremos por $\mathcal{T}(n, C)$ (respectivamente $\mathcal{D}(n, C)$) el anillo de matrices triangulares superiores (respectivamente matrices diagonales) en $M(n, C)$. Un subconjunto M de $M(n, C)$ se dice **triangularizable** (respectivamente **diagonalizable**) si existe $x \in GL(n, C)$ tal que

$$xMx^{-1} \subset \mathcal{T}(n, C)$$

(respectivamente $xMx^{-1} \subset \mathcal{D}(n, C)$).

El siguiente lema será de utilidad en la demostración del teorema de correspondencia de la teoría de Picard-Vessiot.

Lema 1.46. *Si $M \subset M(n, c)$ es un conjunto conmutativo de matrices, entonces M es triangularizable. Si $N \subset M$ es un subconjunto de matrices diagonalizables, entonces N puede ser diagonalizado al mismo tiempo.*

Prueba. Sea $V = C^n$. Probaremos el resultado por inducción sobre n. Si M consiste sólo de homotecias el resultado es trivial. De lo contrario es posible escoger $x \in M$ y $\lambda \in C$ tales que $0 \neq W = \text{Ker}(x - \lambda I) \neq V$. Es fácil probar que W es $M-$estable. Por inducción, existe $v_1 \in W$ tal que Cv_1 es $M-$estable. Aplicando la hipótesis inductiva a la acción de M sobre V/Cv_1 obtenemos $v_2, \ldots v_n \in V$ que forman una base de V/Cv_1, tales que cada subespacio $Cv_1 + \cdots + Cv_i$ $(1 \leq i \leq n)$. Luego la base $v_1, \ldots, v_n$ triangulariza M.

Ahora, si N no consiste sólo de homotecias, podemos suponer $x \in N$. Como x es diagonalizble entonces $V = W \oplus W'$ donde la suma w' de autoespacios restantes de x es distinta de cero. Como vimos antes, ambos W y W' son $M-$estables. Por hipótesis de inducción podemos encontrar bases de W y W' que triangularizan M mientras simultaneamente diagonalizan N. □

Teorema 1.47 (Estructura de grupos conmutativos)**.** *Sea G un grupo algebraico lineal comutativo. Entonces G_s, G_u son subgrupos cerrados y*

$$\begin{aligned} \varphi : G_s \times G_u &\to G \\ (x, y) &\mapsto xy \end{aligned}$$

es un isomorfismo de grupos algebraicos cuya inversa es la descomposición de Jordan.

Prueba. Como G es conmutativo, por el lema 1.34 parte d), tenemos que G_s y G_u son subgrupos de G. Por el teorema 1.20 existe un isomorfismo $\psi : G \to G'$, donde G' es un subgrupo cerrado de algún $\mathrm{GL}(n, C)$. Luego por la proposición 1.40, tenemos $\psi(G_u)$ es el conjunto de matrices unipotentes de $\mathrm{GL}(n, C)$ en G', es decir

$$\psi(G_u) = G' \cap \{x' \in G' : (x' - id)^n = 0\}$$

luego G_u es cerrado. Por otro lado, como G' es un conjunto conmutativo de matrices, por lema 1.46 existe $g \in \mathrm{GL}(n, C)$ tal que $gG'g^{-1} \subset \mathcal{T}(n, C)$ y como $\psi(G_s)$ es un subconjunto de matrices diagonalizables de G' entonces $g\psi(G_s)g^{-1} \subset \mathcal{D}(n, C)$. Así $\varphi(G_s) = G' \cap g\psi(G_s)g^{-1}$ luego G_s es cerrado, es más, φ es un morfismo de grupos algebraicos.

Ahora veremos que φ^{-1} es un morfismo de grupos algebraicos. Hay que probar que $x \mapsto x_s$ y $x \mapsto x_u$ son morfismos. Como $x_u = x_s^{-1}x$, bastará probar que $x \mapsto x_s$ es un morfismo, luego $x \mapsto x_u$ también lo será. Sea $x \in G$, entonces x_s es la parte diagonal de x, luego $x \mapsto x_s$ es un morfismo. □

Capítulo 2

Cuerpos diferenciales

En este capítulo presentaremos algunas definiciones y resultados sobre teoría de Galois diferenciable.

2.1. Anillos diferenciales

Definición 2.1. Sea A un anillo, una **derivación** de A es un mapeo $d_A : A \to A$ tal que

i) $d_A(a+b) = d_A(a) + d_A(b)$

ii) $d_A(ab) = d_A(a)b + ad_A(b)$

Definición 2.2. Un **anillo diferencial** es un anillo conmutativo con identidad dotado de una derivación.

Ejemplo 2.3. $A = C^\infty(\mathbb{R})$ con $d(f) = f'$ la derivada usual, es un anillo diferencial.

Escribiremos (A, d_A) para referirnos al anillo diferencial A dotado de la derivación d_A, ó sólo A cuando la derivación se sobreentienda.

Escribiremos en el segundo caso, $d_A(a) = a'$ y a'' , ..., $a^{(n)}$ para las derivadas sucesivas. En un anillo diferencial podemos verificar lo siguiente:

- Por inducción se comprueba que $(a^n)' = na^{n-1}a'$
- Debido a la linealidad de la derivación se verifica que $(1_A)' = 0$.
- Por la segunda condición de derivación tenemos que, si $a \in A$ es inversible con inversa a^{-1} entonces $(a^{-1})' = -a'/a^2$.

Definición 2.4. Un cuerpo diferencial es un anillo diferencial que es un cuerpo.

Definición 2.5. Sea A un anillo diferencial, definimos el **cuerpo de constantes** de A como:

$$C_A = \{a \in A : a' = 0\}$$

Si K es un cuerpo, se verifica que C_K es también un cuerpo.

Proposición 2.6. *Si A es un dominio de integridad, una derivación d_A de A se extiende al cuerpo de fracciones* $\mathrm{Frac}(A)$ *de forma única.*

Prueba. Definimos:

$$\begin{aligned} \hat{d} \quad : \quad & Frac(A) \to Frac(A) \\ & \frac{a}{b} \ \mapsto \ \hat{d}\left(\frac{a}{b}\right) = \frac{d_A(a)b - ad_A(b)}{b^2} \end{aligned}$$

- Veamos que $\hat{d}$ está bien definida:
  Sea $\dfrac{c}{d} \in \left[\dfrac{a}{b}\right]$ entonces existe $k \in A$ tal que $c = ak$ y $d = bk$. Luego:

$$\begin{aligned} \hat{d}\left(\frac{c}{d}\right) = \hat{d}\left(\frac{ak}{bk}\right) &= \frac{d_A(ak)(bk) - (ak)d_A(bk)}{(bk)^2} \\ &= \frac{\left(d_A(a)k + ad_A(k)\right)bk - ak(d_A(b)k + bd_A(k))}{b^2k^2} = \frac{d_A(a)b - ad_A(b)}{b^2} \end{aligned}$$

  Asi, la definición de $\hat{d}\left(\dfrac{a}{b}\right)$ es independiente de la elección del representante de la clase de equivalencia.

- Veamos que $\hat{d}$ es una derivación: Sean $\dfrac{a}{b}, \dfrac{c}{d} \in Frac(A)$

$$\begin{aligned} \hat{d}\left(\frac{a}{b} + \frac{c}{d}\right) = \hat{d}\left(\frac{ad + bc}{bd}\right) &= \frac{D_A(ad + bc)bd - (ad + bc)D_A(bd)}{(bd)^2} \\ &= \frac{d_A(a)b - ad_A(b)}{b^2} + \frac{d_A(c)d - cd_A(d)}{d^2} = \hat{d}\left(\frac{a}{b}\right) + \left(\frac{c}{d}\right) \\ \hat{d}\left(\frac{a}{b}.\frac{c}{d}\right) = \hat{d}\left(\frac{ac}{bd}\right) &= \frac{(ac)'bd - acd_A(bd)}{b^2d^2} \\ &= \left(\frac{d_A(a)ab - ad_A(b)}{b^2}\right)\frac{c}{d} + \frac{a}{b}\left(\frac{d_A(c)d - cd_A(d)}{d^2}\right) \\ &= \hat{d}\left(\frac{a}{b}\right)\frac{c}{d} + \frac{a}{b}\hat{d}\left(\frac{c}{d}\right) \end{aligned}$$

- Veamos que $\hat{d}$ extiende a d

$$\hat{d}\left(\frac{a}{1}\right) = \frac{d_A(a)1 - ad_A(1)}{1^2} = d_A(a)$$

- Veamos la unicidad: supongamos que existe otra derivación $\tilde{d}$ de Fracc(A) tal que $\tilde{d}_{|A} = d_A$.

$$\tilde{d}\left(\frac{a}{b}\right) = \tilde{d}\left(\frac{a}{1}.\frac{1}{b}\right) = \tilde{d}\left(\frac{a}{1}\right).\frac{1}{b} + \frac{a}{1}.\tilde{d}\left(\frac{1}{b}\right) = d_A(a).\frac{1}{b} + ad\frac{1}{b}$$
$$= a'.\frac{1}{b} + a(b^{-1})' = \frac{a'}{b} + a\left(\frac{-b'}{b^2}\right) = \frac{a'b - ab'}{b^2}$$

□

Ejemplo 2.7. Sea A un anillo conmutativo con unidad. Si definimos la derivación trivial: $d(a) = 0$ para todo $a \in A$, entonces A es un anillo diferencial.
Sea d es una derivación sobre $\mathbb{Z}$ ó $\mathbb{Q}$, tenemos que $d(1) = 0$, luego:

- Dado $n \in \mathbb{Z} : d(n) = d((n-1)+1) = d(n-1) + d(1) = \ldots = d(1) = 0.$
- Sea $\frac{m}{n} \in \mathbb{Q} : d\left(\frac{m}{n}\right) = d(m).\frac{1}{n} + m.d\left(\frac{1}{n}\right) = m\frac{(-d(n))}{n^2} = 0$

entonces la única derivación posible sobre $\mathbb{Z}$ y $\mathbb{Q}$ es la trivial.

Ejemplo 2.8. Sea Ω un conjunto abierto y conexo de $\mathbb{C}$, entonces

$$A(\Omega) = \{f : \Omega \to \mathbb{C} / f \text{ es analítica en } \Omega\}$$

con la derivación usual "d" es un anillo diferencial. Como $A(\Omega)$ es un dominio de integridad, podemos extender "d" al cuerpo de fracciones de $A(\Omega)$, que es el cuerpo de funciones meromorfas $M(\Omega)$.

Observación 2.9. Si $f(X) = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n$, denotaremos:

$$f^{(d)}(X) = a_0' + a_1'X + a_2'X^2 + \cdots + a_n'X^n$$
$$f'(X) = a_1 + 2a_2X + 3a_3X^2 + \cdots + na_nx^{n-1}.$$

Ejemplo 2.10. Sea (A, d) un anillo diferencial, podemos dotar al anillo de polinomios $A[X]$ de una derivación que extiende a la derivación de A.

Sea $f(X) = \sum_{i=0}^{n} a_iX^i \in A[X]$ y sea D la derivación sobre $A[X]$, entonces:

$$D\left(\sum_{i=0}^{n} a_iX^i\right) = \sum_{i=0}^{n}[D(a_i)X^i + a_iD(X^i)]$$
$$= \sum_{i=0}^{n}[d(a_i)X^i + a_iiX^{i-1}D(X)]$$
$$= \sum_{i=0}^{n} a_i'X^i + \left(\sum_{i=0}^{n} ia_iX^{i-1}\right)D(X)$$
$$= f^{(d)}(X) + f'(X)D(X).$$

Luego la derivación D esta totalmente determinada por $D(X)$. Entonces extendemos la derivación de A a una sobre $A[X]$, asignando un valor arbitatrio a X' en $A[X]$. Analogamente, si A es un cuerpo, podemos extender la derivación de A al cuerpo

$$A(X) = \left\{ \frac{f(X)}{g(X)} : f, g \in A[X], g \neq 0 \right\}.$$

- Si A es un anillo diferencial, mediante iteración, podemos dotar de una estructura diferencial al anillo $A[X_1, \ldots, X_n]$. En efecto, si A es un anillo diferencial entonces por lo visto anteriormente, podemos extender su derivación a $A[X_1]$. Luego extender esta derivación a $A[X_1, X_2] = (A[X_1])[X_2]$ y asi por inducción es posible extender a una derivación sobre $A[X_1, X_2, \ldots, X_n] = (A[X_1, \ldots, X_{n-1}])[X_n]$.

- Si A es un cuerpo diferencial entonces mediante iteración podemos dotar de una estructura diferencial al cuerpo

$$A(X_1, \ldots, X_n) = \left\{ \frac{P(X_1, \ldots, X_n)}{Q(X_1, \ldots, X_n)} : P, Q \in A[X_1, \ldots, X_n], Q \neq 0 \right\}.$$

Ejemplo 2.11. Sea A un anillo diferencial. Consideremos el anillo

$$A[X_i],\ i = 0, 1, 2, \ldots$$

Definimos: $X_i' = X_{i+1}$ (por ejemplo en $(A[X_2], d) : d(X_2) = X_2' = X_3$). Por notación escribiremos $X = X_0$ y $X^{(n)} = X_n$. Llamamos a este procedimiento la **adjunción** de una indeterminada diferencial. Denotamos con $A\{X\}$ al anillo diferencial resultante:

$$A\{X\} = \{p(X, X', \ldots, X^{(n)}, \ldots) : p \in A[X_1, \ldots, X_n, \ldots]\}.$$

Si A es un cuerpo diferencial, entonces $A\{X\}$ es un dominio de integridad diferencial y su derivación se extiende de manera única al cuerpo cociente. Denotaremos el cuerpo cociente de $A\{X\}$ como

$$A\langle X \rangle = \left\{ \frac{p(X, X', X'', \ldots)}{q(X, X', X'', \ldots)} : p, q \in A\{X\} \right\}.$$

Ejemplo 2.12. Si A es un anillo diferencial, definimos

$$\begin{aligned} D : M_{n\times n}(A) &\longrightarrow M_{n\times n}(A) \\ [a_{ij}] &\longmapsto D([a_{ij}]) = [a_{ij}'] \end{aligned}$$

entonces $(M_{n\times n}(A), D)$ *no* es un anillo diferenciable, es un anillo no conmutativo con derivación D.

Definición 2.13. Sea (A, d_A) un anillo diferencial y sea $I \subset A$ un ideal de A. Diremos que I es un ideal diferencial si: $a \in I$ implica $a' \in I$, es decir, $d(I) \subset I$.

Proposición 2.14. *Si I es un ideal diferencial de un anillo diferencial A, la aplicación dada por:*

$$\begin{aligned} \widetilde{d} : \frac{A}{I} &\longrightarrow \frac{A}{I} \\ \overline{a} &\longmapsto \widetilde{d}(\overline{a}) = \overline{d_A(a)} \end{aligned}$$

define una derivación en el anillo cociente A/I.

Prueba. Veamos que $\tilde{d}$ está bien definida: si $\overline{a} = \overline{b}$ entonces $a - b \in I$ luego

$$d_A(a) - d_A(b) = d_A(a - b) \in I$$

pues I es un ideal diferencial, así $\overline{d_A(a)} = \overline{d_A(b)}$.
Veamos que es una derivación:

- $\widetilde{d}\left(\overline{a} + \overline{b}\right) = \widetilde{d}\left(\overline{a + b}\right) = \overline{d_A(a + b)} = \overline{d_A(a) + d_A(b)} = \widetilde{d}(a) + \widetilde{d}(b)$
- $\widetilde{d}\left(\overline{a}\overline{b}\right) = \widetilde{d}\left(\overline{ab}\right) = \overline{d_A(ab)} = \overline{d_A(a)b + ad_A(b)} = \widetilde{d}(\overline{a})\overline{b} + \overline{a}\widetilde{d}(\overline{b})$

□

Definición 2.15. Sean (A, d_A) y (B, d_B) anillos diferenciales, $f : A \to B$ es un morfismo diferencial si:

1) $f(a + b) = f(a) + f(b)$

2) $f(ab) = f(a)f(b)$, para todo $a, b \in A$

3) $f(1_A) = 1_B$

4) $d_B\left(f(a)\right) = f\left(d_A(a)\right)$, para todo $a \in A$

2.2. Extensiones diferenciales

Definición 2.16. Sean (A, d_A) y (B, d_B) anillos diferenciales tales que $A \subset B$. Diremos que $A \subset B$ es una **extensión diferencial** si $d_A = (d_B)_{|_A}$, es decir, $d_B(a) = d_A(a)$, para todo $a \in A$.

- Si $S \subset B$ es un conjunto: $A\{S\}$ es el menor subanillo de B que contiene a A, a S y las derivadas de todos los ordenes de los elementos de S. Es la A-subalgebra diferencial de B generada por S sobre A.

- Si $K \subset L$ es una extensión de cuerpos diferenciales, $S \subset L$ subconjunto, entonces $K\langle S\rangle$ es el subcuerpo diferencial de L generado por S sobre K. Si S es finito diremos que la extensión $K \subset K\langle S\rangle$ es finitamente generada diferencialmente. Es decir, con las notaciones del ejemplo 2.11, se obtiene que

$$K\langle S\rangle = \left\{ \frac{p(s, s', s'', \ldots)}{q(s, s', s'', \ldots)} : p, q \in K\{S\}, s \in S \right\}.$$

Proposición 2.17. *Si K es un cuerpo diferencial, $K \subset L$ una extensión de cuerpos algebraica separable, entonces la derivación de K se extiende de manera única a L. Es más, todo K-automorfismo de L es diferencial.*

Prueba. Primero veamos el caso en que la extensión $K \subset L$ es finita. Como $K \subset L$ es separable, por el teorema del elemento primitivo existe $\alpha \in L$ tal que $L = K(\alpha)$. Sea

$$p(X) = Irr(\alpha, K)(X) = \sum_{i=0}^{n-1} a_i X^i + X^n, a_i \in K$$

el polinomio irreducible de α en $K[X]$. Definimos

$$\begin{aligned} \varphi : & K[X] \longrightarrow K(\alpha) = L \\ & h(X) \longmapsto h(\alpha) \end{aligned}$$

Como α es algebraico sobre K, tenemos que $K(\alpha) = K[\alpha]$, luego φ es sobreyectiva. Es fácil ver que $Ker(\varphi) = \langle p(X)\rangle$, luego por el primer teorema de isomorfismo para anillos

$$\frac{K[X]}{\langle p(X)\rangle} \simeq L,$$

donde el isomorfismo inducido por φ es

$$\begin{aligned} \overline{\varphi} : & \frac{K[X]}{\langle P(X)\rangle} \longrightarrow K(\alpha) \\ & \overline{h(X)} \longmapsto h(\alpha) \end{aligned}$$

Si logramos encontrar una derivación $\tilde{d}$ sobre $\dfrac{K[X]}{\langle P(X)\rangle}$, podremos definir una derivación d_L sobre L. En efecto, si consideramos el diagrama:

$$\begin{array}{ccc} K(\alpha) & \xrightarrow{\overline{\varphi}^{-1}} & \dfrac{K[X]}{\langle P(X)\rangle} \\ {\scriptstyle d_L}\downarrow & & \downarrow{\scriptstyle \tilde{d}} \\ K(\alpha) & \xleftarrow[\overline{\varphi}]{} & \dfrac{K[X]}{\langle P(X)\rangle} \end{array} .$$

Podremos definir una aplicación sobre L:

$$d_L = \overline{\varphi} \circ \tilde{d} \circ \overline{\varphi}^{-1}. \tag{2.2.1}$$

Por la proposición 2.14 bastará dotar a $K[X]$ de una derivación $\hat{d}$ de tal manera que $\langle p(X)\rangle$ sea un ideal diferencial, así tendremos la derivación sobre $\dfrac{K[X]}{\langle p(X)\rangle}$:

$$\tilde{d}\left(\overline{p(X)}\right) = \overline{\hat{d}\,(p(X))}.$$

Como vimos en el ejemplo 2.10, dado $h(X) \in K\,[X]$

$$\hat{d}\,(h(X)) = h^{(d)}(X) + h'(X)\hat{d}(X)$$

luego bastará definir adecuadamente $\hat{d}(X)$. De la ecuación 2.2.1 evaluando en α:

$$d_L(\alpha) = \overline{\varphi} \circ \tilde{d} \circ \overline{\varphi}^{-1}(\alpha) = \overline{\varphi} \circ \tilde{d}(\overline{X}) = \overline{\varphi}\left(\overline{\hat{d}(X)}\right) = \hat{d}(\alpha) \tag{2.2.2}$$

Veamos como definir adecuadamente $\hat{d}(X)$ de tal manera que se verifique 2.2.2 y $\langle p(X)\rangle$ sea un ideal diferencial. Observemos que, si d_L es la derivación sobre L que extiende a la derivación de K:

$$0 = d_L\,(p(\alpha)) = p^{(d)}(\alpha) + p'(\alpha)d_L(\alpha).$$

Entonces

$$d_L(\alpha) = \frac{-p^{(d)}(\alpha)}{p'(\alpha)}.$$

Luego por (2.2.2) tendremos

$$\hat{d}(\alpha) = \frac{-p^{(d)}(\alpha)}{p'(\alpha)}. \tag{2.2.3}$$

Como $char(K) = 0$ entonces $p'(X) \neq 0$, y como $p(X)$ es irreducible entonces $mcd\,(p(X), p'(X)) = 1$, luego por la identidad de Bézout existen $r(X), q(X) \in K\,[X]$ tales que

$$p(X)r(X) + p'(X)q(X) = 1$$

evaluando en α:

$$p(\alpha)r(\alpha) + p'(\alpha)q(\alpha) = 1$$

luego

$$q(\alpha) = \frac{1}{p'(\alpha)}$$

entonces por (2.2.3)

$$\hat{d}(\alpha) = -p^{(d)}(\alpha)q(\alpha)$$

Definiremos entonces $\hat{d}(X) = -p^d(X)q(X)$. Comprobaremos que con esta definición $\langle p(X)\rangle$ es un ideal diferencial. Sea $h(X) \in \langle p(X)\rangle$ entonces $h(X) = p(X)h_1(X)$ donde $h_1(X) \in K[X]$ así

$$\hat{d}\left(h(X)\right) = \hat{d}\left(p(X)\right)h_1(X) + p(X)\hat{d}\left(h_1(X)\right).$$

Luego sólo basta ver que el primer sumando está en el ideal $\langle p(X)\rangle$:

$$\begin{aligned}
\hat{d}\left(p(X)\right) =& p^{(d)}(X) + p'(X)\hat{d}(X) \\
=& p^{(d)}(X) + p'(X)\left(-p^{(d)}(X)q(X)\right) \\
=& p^{(d)}(X)\left(1 - p'(X)q(X)\right) \\
=& p^{(d)}(X)p(X)r(X) \in \langle p(X)\rangle.
\end{aligned}$$

Así, $\hat{d}\left(p(X)\right) \in \langle p(X)\rangle$ y $\langle p(X)\rangle$ es un ideal diferencial.

Veamos el caso general, cuando $K \subset L$ es algebraica. Sea $\alpha \in L$ entonces $\alpha \in K(\alpha)$ y como la extensión $K \subset K(\alpha)$ es finita, existe una derivación $d_{K(\alpha)}$ que extiende a la derivación de K. Luego definiremos $d_L(\alpha) = d_{K(\alpha)}(\alpha)$.

Finalmente, si σ es un $K-$automorfismo de L, es fácil probar que $\sigma^{-1}D\sigma$ es también una derivación de L que extiende la derivación de K por unicidad tenemos que $\sigma^{-1}D\sigma = D$, luego $D\sigma = \sigma D$, así σ es un automorfismo diferencial. □

2.3. El anillo de operadores diferenciales

Definición 2.18. Sea K un cuerpo diferencial con derivación no trivial d. Un **operador diferencial lineal** $\mathcal{L}$ con coeficientes en K es un polinomio en d:

$$\mathcal{L} = a_0 + a_1 d + a_2 d^2 + \cdots + a_n d^n, a_i \in K.$$

Si $a_n \neq 0$ diremos que $\mathcal{L}$ tiene grado n. Si $a_n = 1$ diremos que $\mathcal{L}$ es mónico.

El anillo de operadores diferenciales lineales con coeficientes en K es el anillo de polinomios $K[d]$ en la variable d con coeficientes en K. Este anillo no es conmutativo:

$$(da)(y) = d(ay) = a'y + ay' = (a' + ad)(y)$$

luego $da = a' + ad$. A cada operador diferencial $\mathcal{L} = a_0 + a_1 d + \cdots + a_n d^n$ le asociamos la ecuación difeencial lineal

$$\mathcal{L}(Y) = a_0 + a_1 Y + \cdots + a_n Y^{(n)} = 0.$$

2.3.1. Ecuaciones diferenciales lineales homogéneas

De ahora en adelante, K denotará un cuerpo de característica cero: $char(K) = 0$.

Consideraremos ecuaciones diferenciales lineales homogeneas sobre un cuerpo diferencial K, con cuerpo de constantes C:

$$\mathcal{L}(Y) = a_0 Y + a_1 Y' + a_2 Y'' + \cdots + a_{n-1} Y^{(n-1)} + Y^{(n)} = 0, \quad a_i \in K. \tag{2.3.1}$$

Si $K \subset L$ es una extensión diferencial, el conjunto de soluciones de $\mathcal{L}(Y) = 0$ en L es un C_L - espacio vectorial, donde C_L denota el cuerpo de constantes de L.

En efecto:

- Si α y β son soluciones de $\mathcal{L}(Y) = 0$, $\mathcal{L}(\alpha) = 0$ y $\mathcal{L}(\beta) = 0$. Como $\mathcal{L}$ es lineal, $\mathcal{L}(\alpha + \beta) = \mathcal{L}(\alpha) + \mathcal{L}(\beta) = 0$.
- Si α es solución de $\mathcal{L}(Y) = 0$ y $a \in C_L$, notamos que $(a\alpha)^{(n)} = a\alpha^{(n)}$, luego: $\mathcal{L}(a\alpha) = a\mathcal{L}(\alpha) = 0$

Veamos que la dimensión del espacio de soluciones de $\mathcal{L}(Y) = 0$ es a lo mas el orden n de $\mathcal{L}$.

2.3.2. El wronskiano

En esta sección definiremos el determinante wronskiano y lo usaremos para discutir cuál debería ser el mínimo número de soluciones de una ecuación del tipo (2.3.1).

Definición 2.19. Sean $y_1, \ldots, y_n \in K$, donde K es un cuerpo diferencial. El determinante:

$$W = W(y_1, \ldots, y_n) = \begin{vmatrix} y_1 & y_2 & \ldots & y_n \\ y_1' & y_2' & \ldots & y_n' \\ \vdots & \vdots & & \vdots \\ y_1^{(n-1)} & y_2^{(n-1)} & \ldots & y_n^{(n-1)} \end{vmatrix}$$

es el **wronskiano** de $y_1 \ldots y_n$.

Sea $\underline{y} = (y_1, \ldots, y_n)$ la fila de n entradas de elementos de un cuerpo diferencial K, entonces para cualquier $1 \leq i \leq n$ definimos

$$\underline{y}^{(i)} = (y_1^{(i)}, \ldots, y_n^{(i)}),$$

donde $z^{(i)}$ significa la composición de la derivación $(d \circ \cdots \circ d)(z)$ (i veces). Luego el wronskiano podra ser expresado como

$$W\left(\underline{y}\right) = det\left(\underline{y}^{(0)}, \ldots, \underline{y}^{(n-1)}\right),$$

donde $\underline{y}^{(0)} = \underline{y}$. Por otro lado, también es conveniente usar la siguiente notación:

$$A = \begin{bmatrix} y^{(0)} \\ \underline{y}^{(1)} \\ \vdots \\ \underline{y}^{(n-1)} \end{bmatrix}$$

luego $W\left(\underline{y}\right) = \det(A)$. Veamos algunos ejemplos:

Ejemplo 2.20. Sea K un cuerpo diferencial, y sean $y_1, \ldots y_n \in K$ tales que $y_i' = a_i y_i$ donde $a_i' = 0$ para todo $i = 1, \ldots, n$. Sea $\underline{y} = (y_1, \ldots, y_n)$, entonces $\underline{y}^{(i)} = \left(a_1^{(i)} y_1, \ldots, a_n^{(i)} y_n\right)$, así

$$W\left(\underline{y}\right) = \begin{vmatrix} y_1 & y_2 & \ldots & y_n \\ a_1 y_1 & a_2 y_2 & \ldots & a_n y_n \\ \vdots & \vdots & & \vdots \\ a_1^{n-1} y_1^{(n-1)} & a_2^{n-1} y_2^{(n-1)} & \ldots & a_n^{n-1} y_n^{(n-1)} \end{vmatrix}$$

$$= y_1 y_2 \ldots y_n \begin{vmatrix} 1 & 1 & \ldots & 1 \\ a_1 & a_2 & \ldots & a_n \\ \vdots & \vdots & & \vdots \\ a_1^{n-1} & a_2^{n-1} & \ldots & a_n^{n-1} \end{vmatrix}$$

el determinante de la derecha es el determinante de Vandermonde, el cual distinto de cero siempre que los a_i sean todos diferentes. En ese caso $W\left(\underline{y}\right) \neq 0$.

Ejemplo 2.21. Calcularemos la derivada de un determinante. Sea K un cuerpo diferencial, y sean $x_{ij} \in K$ para todo $i, j = 1, \ldots, n$. Usaremos la fórmula de Leibniz para el determinante de una matriz cuadrada. Sea $A = [x_{ij}]$,

$$\det(A) = \sum_{\sigma \in P_n} (-1)^{\sigma} x_{1\sigma(1)} \ldots x_{n\sigma(n)},$$

donde la suma se calcula sobre todas las permutaciónes σ del grupo simétrico P_n. Para cada $\sigma \in P_n$

$$\left(x_{1\sigma(1)} \ldots x_{n\sigma(n)}\right)' = \sum_{i=1}^{n} x_{1\sigma(1)} \ldots x_{i\sigma(i)} \ldots x_{n\sigma(n)}$$

luego si denotamos $\underline{x_i} = (x_{i1}, \ldots, x_{in})$ obtendremos

$$(\det(A))' = \sum_{i=1}^{n} \det\left(\ldots, \underline{x_i'}, \ldots\right).$$

Ejemplo 2.22. Veamos ahora el cálculo de la derivada de un wronskiano. Sea $\underline{y} = (y_1, \ldots, y_n)$ entonces

$$W\left(\underline{y}\right) = \det\left(\underline{y}^{(0)}, \ldots, \underline{y}^{(n-1)}\right)$$

luego por el ejemplo anterior

$$\begin{aligned}
\left(W\left(\underline{y}\right)\right)' &= \sum_{i=1}^{n} \det\left(\ldots, \underline{y}^{(i-1)\prime}, \ldots\right) \\
&= \sum_{i=1}^{n} \det\left(\ldots, \underline{y}^{(i)}, \ldots\right) \\
&= \det\left(\underline{y}', \underline{y}', \underline{y}^{(2)}, \ldots, \underline{y}^{(n-1)}\right) + \det\left(\underline{y}, \underline{y}^{(2)}, \underline{y}^{(2)}, \ldots, \underline{y}^{(n-1)}\right) \\
&+ \ldots + \det\left(\underline{y}, \underline{y}', \underline{y}^{(2)}, \ldots, \underline{y}^{(n-2)}, \underline{y}^{(n)}\right)
\end{aligned}$$

y todos los términos de esta suma son cero pues las matrices tienen una fila repetida, excepto por el último. Así obtenemos la forma de la derivada del wronskiano

$$\left(W\left(\underline{y}\right)\right)' = \det\left(\underline{y}, \underline{y}', \underline{y}^{(2)}, \ldots, \underline{y}^{(n-2)}, \underline{y}^{(n)}\right).$$

Consideremos la ecuación $Y^{(n)} - \sum_{i=1}^{n-1} a_i Y^{(n-i)} = 0$. Si todos los y_i son soluciones de esta ecuación tendremos

$$y_j^{(n)} = \sum_{i=1}^{n-1} a_i y_j^{(n-i)}$$

para todo $j = 1, \ldots, n$, luego

$$\underline{y}^{(n)} = \sum_{i=1}^{n-1} a_i \underline{y}^{(n-i)}.$$

Entonces

$$\begin{aligned}
\left(W\left(\underline{y}\right)\right)' &= \det\left(\underline{y}, \underline{y}', \underline{y}^{(2)}, \ldots, \underline{y}^{(n-2)}, \underline{y}^{(n)}\right) \\
&= \det\left(\underline{y}, \underline{y}', \underline{y}^{(2)}, \ldots, \underline{y}^{(n-2)}, \sum_{i=1}^{n-1} a_i \underline{y}^{(n-i)}\right) \\
&= \det\left(\underline{y}, \underline{y}', \underline{y}^{(2)}, \ldots, \underline{y}^{(n-2)}, a_1 \underline{y}^{(n-1)}\right) \\
&= a_1 \det\left(\underline{y}, \underline{y}', \underline{y}^{(2)}, \ldots, \underline{y}^{(n-2)}, \underline{y}^{(n-1)}\right) \\
&= a_1 W\left(\underline{y}\right).
\end{aligned}$$

Ejemplo 2.23. Sea A un anillo diferencial, y $A\{Y\}$ el anillo de polinomios diferenciales sobre A (ejemplo 2.11). Sean $y_1, \ldots, y_n \in A$ y consideremos

$$\mathcal{L}(Y) = W\left(Y, y_1, \ldots, y_n\right).$$

Entonces L es un operador diferencial lineal homogéneo de orden n con coeficientes en A. Notamos que $\mathcal{L}(y_i) = 0$ para todo $i = 1 \ldots, n$ pues en cada caso la matriz correspondiente tiene una columna repetida. Para ayudarnos en resultados posteriores, será conveniente considerar la forma explícita de $\mathcal{L}$ obtenida por expansión de cofactores a lo largo de la primera columna.

$$W(Y, y_1 \ldots y_n) = \begin{vmatrix} Y & y_1 & y_2 & \ldots & y_n \\ Y' & y_1' & y_2' & \ldots & y_n' \\ \vdots & \vdots & & \vdots & \\ Y^{(n)} & y_1^{(n)} & y_2^{(n)} & \ldots & y_n^{(n)} \end{vmatrix} = \sum_{i=o}^{n} a_i Y^{(i)}$$

donde $a_i = (-1)^i \det(\ldots, \underline{y}^{(i-1)}, \underline{y}^{(i+1)}, \ldots)$ y $\underline{y} = (y_1, \ldots, y_n)$. En particular, notamos que $a_n = W\left(\underline{y}\right)$.

Proposición 2.24. *Sea $\mathcal{L}(Y) = 0$ una ecuación diferencial lineal homogénea de grado n sobre el cuerpo diferencial K y sea $\{y_1, \ldots, y_n\}$ una base del espacio solución de $\mathcal{L}(Y) = 0$ en una extensión diferencial L de K. Sea $z_j = \sum_{i=1}^{n} c_{ij} y_i$ para todo $j = 1, \ldots, n$ con $c_{ij} \in C_K$. Entonces*

$$W(z_1, \ldots, z_n) = \det(c_{ij}).W(y_1, \ldots, y_n).$$

Prueba. Como $c_{ij} \in C_K$, derivando z_j tenemos:

$$z_j^{(k)} = \sum_{i=1}^{n} c_{ij} y_i^{(k)}, \;\; k = 1, \ldots, n-1.$$

Luego se verifica que el siguiente producto

$$\begin{bmatrix} y_1 & y_2 & \cdots & y_n \\ y_1' & y_2' & \cdots & y_n' \\ \vdots & \vdots & & \vdots \\ y_1^{(n-1)} & y_2^{(n-1)} & \cdots & y_n^{(n-1)} \end{bmatrix} \begin{bmatrix} c_{11} & c_{12} & \cdots & c_{1n} \\ c_{21} & c_{22} & \cdots & c_{2n} \\ \vdots & \vdots & & \vdots \\ c_{n1} & c_{n2} & \cdots & c_{nn} \end{bmatrix}$$

es igual a la matriz

$$\begin{bmatrix} z_1 & z_2 & \cdots & z_n \\ z_1' & z_2' & \cdots & z_n' \\ \vdots & \vdots & & \vdots \\ z_1^{(n-1)} & z_2^{(n-1)} & \cdots & z_n^{(n-1)} \end{bmatrix}.$$

Por lo tanto, tomando determinantes, se obtiene lo deseado. □

2.3.3. Independencia lineal sobre constantes

En esta sección estableceremos que un conjunto de elementos en un cuerpo diferencial cuyo wronskiano es distinto de cero, es linealmente independiente sobre el cuerpo de constantes de dicho cuerpo. Comenzaremos observando que el conjunto de soluciones de una ecuación diferencial que tiene más elementos que el orden de la ecuación tiene wronskiano igual a cero:

Proposición 2.25. *Sea $\mathcal{L}(Y) = 0$ una ecuación diferencial lineal homogenea de grado n sobre un cuerpo diferencial K. Si $y_1, \ldots, y_{n+1}$ son soluciones de $\mathcal{L}(Y) = 0$ en una extensión diferencial L de K, entonces $W(y_1, y_2, \ldots, y_n, y_{n+1}) = 0$.*

Prueba. Sea $\mathcal{L}(Y) = a_0 Y + a_1 Y' + \cdots + a_n Y^{(n)}$ con $a_i \in K$. Como $\mathcal{L}(y_i) = 0$ para todo $i = 1, \ldots, n+1$ entonces:

$$y_i^{(n)} = (-a_0) Y_i + (-a_1) Y_i' + \cdots + (-a_{n-1}) Y_i^{(n-1)} = 0$$

para todo $i = 1, \ldots, n+1$.

Sean $u_i = (y_1^{(i)}, \ldots y_{n+1}^{(i)})$ las filas del wronskiano, como u_n es combinación lineal de $u_0, u_1, \ldots, u_{n-1}$ entonces $W(y_1, \ldots, y_{n+1}) = 0$. □

Corolario 2.26. *La ecuación $\mathcal{L}(Y) = 0$ tiene a lo más n soluciones en L, linealmente independientes en C_L.*

La proposición 2.25 nos da una condición necesaria para que el wronskiano sea cero. La siguiente proposición nos da una condición necesaria y suficiente.

Proposición 2.27. *Sea K un cuerpo diferencial con C su cuerpo de constantes, y sean $y_1, \ldots, y_n \in K$. Entonces $y_1, \ldots, y_n$ son linealmente indendientes sobre C, si y sólo si, $W(y_1, \ldots, y_n) \neq 0$.*

Prueba. Supongamos que $y_1, \ldots, y_n$ son linealmente dependientes sobre C. Entonces existen $c_1, c_2, \ldots c_n \in C$ no todos simultaneamente cero, tales que

$$\sum_{i=1}^{n} c_i y_i = 0. \tag{2.3.2}$$

Derivando (2.3.2):

$$\sum_{i=1}^{n} c_i y_i' = \sum_{i=1}^{n} (c_i y_i' + c_i' y_i) = \left(\sum_{i=1}^{n} c_i y_i \right)' = 0.$$

Si seguimos derivando (2.3.2) tendremos que

$$\sum_{i=1}^{n} c_i y_i^{(k)} = 0$$

para todo $k = 0, 1, \ldots, n-1$. Sean $w_i = (y_i, y_i', \ldots, y_i^{(n-1)})$ las columnas del wronskiano, entonces:

$$\sum_{i=1}^{n} c_i w_i = 0$$

y por hipótesis los $c_i \in C$ no son todos ceros, asi $\{w_1, \ldots w_n\}$ es un conjunto linealmente dependiente, por lo tanto $W(y_1, \ldots, y_n) = 0$.

Para el recíproco, trabajaremos por inducción sobre n. El caso $n = 1$ es trivial. Como hipótesis inductiva asumiremos que para todos $z_1, \ldots, _{n-1} \in K$ tales que son C_K-linealmente independientes entonces $W(z_1, \ldots, _{n-1}) \neq 0$. Sean $y_1, \ldots, y_n \in K$ elementos C_K-linealmente independientes pero con $W(y_1, \ldots, y_n) = 0$. Entonces sus columnas $\{w_1, \ldots, w_n\}$ forman un conjunto linealmente dependiente, luego existen $c_1, \ldots, c_n \in K$ no todos cero tales que $\sum_{i=1}^{n} c_i w_i = 0$, es decir

$$\sum_{i=1}^{n} c_i y_i^{(k)} = 0 \tag{2.3.3}$$

para todo $k = 0, \ldots, n-1$. Supongamos que algún $c_j \neq 0$, dividiendo (2.3.3) entre c_j y cambiando los índices podemos asumir sin pérdida de generalidad que $c_1 = 1$. Derivando (2.3.3) para $k = 0, \ldots, n-2$:

$$\sum_{i=1}^{n} c_i y_i^{(k+1)} + \sum_{i=1}^{n} c_i' y_i^{(k)} = 0$$

Por (2.3.3), el primer sumando es cero. Para el segundo, como $c_1 = 1$

$$\sum_{i=2}^{n} c_i' y_i^{(k)} = 0 \tag{2.3.4}$$

para todo $k = 0, \ldots, n-2$. El subconjunto $\{y_2, \ldots, y_n\}$ es C_K-linealmente independiente, luego por la hipótesis inductiva $W(y_2, \ldots, y_n) \neq 0$. Así el sistema (2.3.4) tiene solución trivial $c_i' = 0$ para todo $i = 2, \ldots, n$, entonces $c_i \in C_K$ para todo $i = 1, \ldots, n$ pero por (2.3.3) para $k = 0$

$$\sum_{i=1}^{n} c_i y_i = 0.$$

Sin embargo $c_1 \neq 0$ lo cual contradice la hipótesis de que $\{y_1, \ldots, y_n\}$ es un conjunto C_K-linealmente independiente. □

Usando las proposiciones 2.25 y 2.27, podremos describir la estructura del conjunto de soluciones de una ecuación diferencial lineal.

Teorema 2.28. *Sea K un cuerpo diferencial y sea $\mathcal{L}$ un operador diferencial lineal homogéneo mónico de orden n sobre K. Sea $K \subset L$ una extensión diferencial de cuerpos y sea V el conjunto de soluciones de $\mathcal{L} = 0$ en L. Entonces V es un espacio vectorial sobre C_L con dimensión a lo más n.*

Prueba. Consideremos la aplicación

$$\begin{aligned} \psi : L &\to L \\ y &\mapsto \mathcal{L}(y). \end{aligned}$$

Es fácil ver que es una C_L-transformación lineal, luego su núcleo $V = \mathrm{Ker}(\psi)$ es un C_L-espacio vectorial. Por la proposición 2.25, cualesquiera $n+1$ elementos de V tendrán wronskiano igual a cero. Por la proposición 2.27, estos elementos serán linealmente dependientes sobre C_L. Así V es un espacio vectorial de dimensión finita a lo más n. □

2.3.4. El álgebra universal de soluciones

El teorema anterior nos brinda una cota superior del tamaño del conjunto de soluciones de una ecuación diferencial lineal. Usaremos la siguiente terminología para esta situación:

Definición 2.29. Sea $\mathcal{L}$ un operador diferencial lineal homogéneo de grado n sobre un cuerpo diferencial K y sea $K \subset L$ una extensión diferencial de cuerpos. Diremos que $\mathcal{L} = 0$ tiene un **conjunto fundamental de soluciones en** L si el conjunto de soluciones tiene dimensión n sobre C_L. Esto es, si existen $y_1, \ldots, y_n \in L$ soluciones de $\mathcal{L} = 0$ que son C_L-linealmente independientes.

A lo largo de este trabajo sólo consideramos ecuaciones diferenciales lineales homogéneas, pues a una ecuación diferencial lineal no homogénea le podemos asociar una homogénea. En efecto, sea

$$\mathcal{L}(Y) = Y^{(n)} + a_{n-1}Y^{(n-1)} + \cdots + a_1 Y' + a_0 Y = b, \;\; b \neq 0. \tag{2.3.5}$$

Derivando (2.3.5) tenemos $d(\mathcal{L}(Y)) = b'$, y multiplicando (2.3.5) por b'/b tenemos $\dfrac{b'}{b}\mathcal{L}(Y) = b'$. Restando ambas expresiones obtenemos un operador homogéneo:

$$\begin{aligned}
\overline{\mathcal{L}}(Y) &= d(\mathcal{L}(Y)) - \frac{b'}{b}\mathcal{L}(Y) \\
&= \left(a_0' - \frac{b'}{b}a_0\right) Y + \left(a_0 + b\left(\frac{a_0}{b}\right)' a_1\right) Y' + \cdots + \left(a_{n-1} - \frac{b'}{b}\right) Y^{(n)} + Y^{(n+1)} \\
&= 0.
\end{aligned}$$

Es fácil verificar que si $y_1, \ldots, y_n$ es un conjunto fundamental de soluciones de $\mathcal{L}(Y) = 0$ y y_0 es una solución particular de $\mathcal{L}(Y) = b$ entonces $y_0, y_1, \ldots, y_n$ es un conjunto fundamental de soluciones de $\overline{\mathcal{L}}(Y) = 0$.

El teorema 2.28 tiene otra consecuencia importante: como pone límites en cuanto al tamaño del conjunto de soluciones de una ecuación diferencial, podemos usarlo para mostrar que un conjunto fundamental de soluciones de una ecuación determina dicha ecuación.

Corolario 2.30. *Sea K un cuerpo diferencial y sean $\mathcal{L}_1$ y $\mathcal{L}_2$ dos operadores diferenciales lineales homogéneos de orden n sobre K. Sea $\{y_1, \ldots, y_n\} \subset K$ un conjunto C_K-linealmente independiente tal que $\mathcal{L}_i(y_j) = 0$ para $i = 1, 2$ y $j = 1, \ldots, n$. Entonces*

$$\mathcal{L}_1 = \mathcal{L}_2 = \frac{W(Y, y_1, \ldots, y_n)}{W(y_1, \ldots, y_n)}.$$

Prueba. Sean $\mathcal{L}_1(Y) = \sum_{i=0}^{n} a_i Y^{(i)}$ y $\mathcal{L}_2(Y) = \sum_{i=0}^{n} b_i Y^{(i)}$ donde $a_n = b_n = 1$. Sea j el mayor subíndice tal que $a_j \neq b_j$, probaremos que no existe tal j. Supongamos que existe, y consideremos el operador

$$\mathcal{L}(Y) = (a_j - b_j)^{-1}(\mathcal{L}_1 - \mathcal{L}_2)(Y) = \sum_{i=0}^{j-1}(a_i - b_i)Y^{(i)} + Y^{(j)}$$

Entonces $\mathcal{L}$ es un operador diferencial lineal homogéneo de grado $j < n$. Como $\mathcal{L}(y_i) = 0$, $i = 1, \ldots, n$ y $\{y_1, \ldots, y_n\} \subset K$ un conjunto C_K-linealmente independiente, por teorema 2.28 la dimensión del conjunto de soluciones de $\mathcal{L} = 0$ sobre C_K es a lo más n, que es mayor que el orden del operador $\mathcal{L}$ lo cual es una contradicción. Así no existe tal j que verifica la propiedad mencionada entonces tendremos $a_i = b_i$ para todo $i = 1 \ldots, n$ luego $\mathcal{L}_1 = \mathcal{L}_2$.

Usando el mismo razonamiento, como

$$\mathcal{L}_3(Y) = \frac{W(Y, y_1, \ldots, y_n)}{W(y_1, \ldots, y_n)}$$

es un operador diferencial lineal homogéneo mónico sobre K de orden n y $\mathcal{L}_3(y_i) = 0$, $i = 1, \ldots, n$ entonces $\mathcal{L}_3 = \mathcal{L}_1 = \mathcal{L}_2$. □

El teorema 2.28 también nos dice que dado un operador $\mathcal{L}$ de orden n sobre un cuerpo diferencial K, para obtener un cuerpo diferencial L tal que $K \subset L$ podriamos agregar a lo más n soluciones C_K-linealmente independientes a K. Ahora veremos como construir de manera natural un conjunto fundamental de soluciones linealmente independientes sobre su cuerpo de constantes.

Definición 2.31. Sea K un cuerpo diferencial y sea $\mathcal{L}(Y) = \sum_{i=0}^{n-1} a_i Y^{(i)} + Y^{(n)}$ un operador diferencial lineal hmogéneo sobre K. Consideremos el anillo de polinomios en n^2 indeterminadas

$$K\left[Y_{ij}, 0 \leq i \leq n-1, 1 \leq j \leq n\right]$$

y extendemos la derivación de K a $K\left[Y_{ij}\right]$ definiendo:

$$Y'_{ij} = Y_{i+1,j}, \quad 0 \leq i \leq n-2, \tag{2.3.6}$$

$$Y'_{n-1,j} = -a_{n-1}Y_{n-1,j} - \cdots - a_1 Y_{1j} - a_0 Y_{0j} \tag{2.3.7}$$

Sea $R = K\left[Y_{ij}\right]\left[W^{-1}\right]$ la localización de $K\left[Y_{ij}\right]$ por el conjunto de potencias de $W = \det(Y_{ij})$. La derivación de $K\left[Y_{ij}\right]$ se extiende de manera única a R. La $K-$álgebra diferencial R es llamada **álgebra universal de soluciones** de $\mathcal{L}$.

Observación 2.32. *Veamos algunas propiedades del álgebra universal de soluciones R de*

$$\mathcal{L}(Y) = a_0 Y + a_1 Y' + \cdots + a_{n-1} Y^{(n-1)} + Y^{(n)}$$

- *Por la forma en que hemos definido la derivación sobre $K[Y_{ij}]$, hemos construido soluciones de $\mathcal{L}(Y) = 0$. En efecto, por* (2.3.6) *tenemos $Y_{0j}^{(i)} = Y_{ij}$. Combinando esto con 2.3.7 tendremos*

$$\mathcal{L}(Y_{0j}) = a_0 Y_{0j} + a_1 Y'_{0j} + \cdots + a_{n-1} Y_{0j}^{(n-1)} + Y_{0j}^{(n)} = 0, j = 1, \ldots, n \quad (2.3.8)$$

  luego $\{Y_{01}, \ldots, Y_{0n}\}$ son soluciones de $\mathcal{L} = 0$ en $K[Y_{ij}]$.

- *La derivación que hemos definido sobre $K[Y_{ij}]$ está bien definida. En efecto, si consideramos*

$$\begin{aligned} \varphi : K\{X_1, \ldots, X_n\} &\to K[Y_{ij}] \\ X_i &\to Y_{0i} \end{aligned}$$

  entonces por 2.3.8 tenemos que $\mathrm{Ker}(\varphi)$ *es el ideal diferencial generado por los $\mathcal{L}(Y_{0i})$:*

$$I = \langle \mathcal{L}(Y_{01}), \ldots, \mathcal{L}(Y_{0n}) \rangle$$

  así $K\{X_1, \ldots, X_n\}/I \simeq K[Y_{ij}]$ y ya vimos antes que si K es un cuerpo diferencial, se puede dotar de una derivación al cuerpo $K\{X_1, \ldots, X_n\}$ y por tanto al anillo cociente por un ideal diferencial.

- *Tenemos que $\mathcal{L}(Y_{0i}) = 0$, y es claro que*

$$W = \det(Y_{ij}) = W(Y_{01}, \ldots, Y_{0n}) \neq 0$$

  en $K[Y_{ij}]$, por tanto $\{Y_{01}, \ldots, Y_{0n}\}$ es un conjunto fundamental de soluciones de $\mathcal{L} = 0$ en $K[Y_{ij}]$. Para no perder esta propiedad, localizamos $K[Y_{ij}]$ con W, pues así W es un elemento inversible de R entonces $\{Y_{01}, \ldots, Y_{0n}\}$ es un conjunto fundamental de soluciones de $\mathcal{L} = 0$ en R.

Antes de terminar esta sección, veamos el siguiente ejemplo que aparece publicado en el libro [5].

Ejemplo 2.33. En este ejemplo trabajaremos en el cuerpo de fracciones de series de potencias en la indeterminada z, con la derivación d donde $d(z) = 1$ y d trivial sobre $\mathbb{C}$. Sea $f(z) = e^z$ la serie exponencial usual, entonces $d(f) = f$. Consideremos el cuerpo diferencial $K = \mathbb{C}\langle f \rangle$ y el operador $\mathcal{L}(Y) = Y' - Y = 0$. Como vimos en la definición 2.31, $R = F[Y]$ es álgebra universal de soluciones de $\mathcal{L}$ con la derivación definida como $Y' = Y$, es decir, hemos creado una solución de $\mathcal{L}$, pero de cierta forma esta construcción es superflua, pues el operador $\mathcal{L}$ ya tenía la solución $f \in F$. Observamos que

$$d\left(\frac{Y}{f}\right) = \frac{fd(Y) - Yd(f)}{f^2} = 0.$$

Entonces al agregar la solución Y hemos creado también una nueva constante: $Y/f \in C_R$ y obviamente $Y/f \notin C_R$. Estudiaremos de manera más profunda esta situación en el siguiente capítulo.

Capítulo 3

La extensión de Picard-Vessiot

3.1. Definición con un operador diferencial, existencia y unicidad

Para empezar, consideremos K un cuerpo diferencial, $\mathcal{L}$ un operador diferencial lineal homogéneo de orden n definido sobre K y L una extensión diferencial de K en la que $\mathcal{L}$ tiene un conjunto fundamental de soluciones. Esto es, existen $y_1, \ldots, y_n \in L$ con $\mathcal{L}(y_i) = 0$ y $W(y_1, \ldots, y_n) \neq 0$. En este contexto, $V = \{y \in L : \mathcal{L}(y) = 0\}$ es el espacio vectorial de las soluciones de $\mathcal{L}(Y) = 0$ en L, $L_1 = K\langle y_1, \ldots, y_n\rangle$ es un subcuerpo diferencial de L y C_1 es su cuerpo de constantes. Como $W(y_1, \ldots, y_n) \neq 0$, entonces $\{y_1, \ldots, y_n\}$ es una C_1-base del espacio vectorial $V_1 = V \cap L_1$ y así V_1 (las soluciones de $\mathcal{L} = 0$ en L_1) también tiene dimensión n sobre C_1. Consideremos ahora $\{z_1, \ldots, z_n\}$ un conjunto fundamental de soluciones de $\mathcal{L}$ en L_1, con al menos un elemento diferente de los $y_1, \ldots, y_n$. Entonces $z_i \in V_1$ y $W(z_1, \ldots, z_n) \neq 0$. Analogamente, para el subcuerpo diferencial $L_0 = K\langle z_1, \ldots, z_n\rangle$ y para C_0 su cuerpo de constantes se cumple que $W(z_1, \ldots, z_n) \neq 0$, entonces $\{z_1, \ldots, z_n\}$ es una C_0-base del espacio vectorial $V_0 = V \cap L_0$, y así V_0 también tiene dimensión n sobre C_0, donde $\{z_1, \ldots, z_n\}$ también es una base de V_1 como C_1-espacio vectorial, por lo tanto V_0 genera a V_1 sobre C_1: $V_1 = C_1\langle V_0\rangle$.

Sin embargo, es posible que $L_0 \neq L_1$. Por ejemplo, si $\mathcal{L} = 0$ tiene un conjunto fundamental de soluciones $z_i \in K$ y L es el cuerpo de fracciones del álgebra de soluciones de $\mathcal{L}$ como en la definición 2.31 con soluciones $y_i = Y_{0i}$. Entonces $L_1 = K\langle y_1, \ldots, y_n\rangle = L$ contiene propiamente a $L_0 = K\langle z_1, \ldots, z_n\rangle = K$.

Observemos que cuando L_0 es un subcuerpo propio de L_1, entonces V_0 es un subconjunto propio de V_1 pues L_1 es generado como cuerpo diferencial por V_1 sobre K, mientras que L_0 esta generado como cuerpo diferencial por V_0 sobre K. Luego, como V_0 genera a V_1 sobre C_1, entonces C_0 debe estar contenido propiamente en C_1, por lo tanto C_K está contenido propiamente en C_1. De este análisis, podemos concluir que para obtener una extensión diferencial L_1 de K que contenga un conjunto fundamental de soluciones de $\mathcal{L} = 0$ y que sea minimal en el sentido de la inclusión, es necesario que su cuerpo de constantes C_1 sea minimal respecto a los cuerpos de constantes de todas las subextensiones de K que esten contenidas en L_1 en las que $\mathcal{L} = 0$ tenga un conjunto fundamental de soluciones. Una forma de lograr la minimalidad sería construir la extensión L_1 de tal manera que no tuviese nuevas constantes. Como veremos luego, esto es posible de lograr. Otra observación del análisis realizado es que agregar soluciones superfluas de $\mathcal{L} = 0$ a K siempre implica la existencia de nuevas constantes:

Proposición 3.1. *Sea $\mathcal{L}$ un operador diferencial lineal homogéneo mónico sobre el cuerpo diferencial K, y sea $K \subset L$ una extensión diferencial de cuerpos que contiene un conjunto total de soluciones de $\mathcal{L} = 0$. Si $K \subset F \subset L$ con $F \neq L$ y F también contiene un conjunto total de soluciones de $\mathcal{L} = 0$, entonces existe $x \in C_L$ tal que $x \notin F$.*

Prueba. Podemos suponer sin pérdida de generalidad que $L = K\langle y_1, \ldots, y_n \rangle$ y $F = K\langle z_1, \ldots, z_n \rangle$ donde $y_i \notin F$ (pues $F \subsetneq L$). Sea V el espacio vectorial de soluciones de $\mathcal{L} = 0$ en L. Por hipótesis $F = K\langle V \cap F \rangle \subsetneq K\langle V \rangle = L$ luego $V \cap F \subsetneq V$, y como $C_L\langle V \cap F \rangle = V$ entonces $C_F \subsetneq C_L$. □

Ahora estamos listos para definir una extensión de Picard - Vessiot, que es análogo del cuerpo de descomposición de un polinomio.

Definición 3.2. Sea K un cuerpo diferencial y sea $\mathcal{L}(Y) = 0$ un operador diferencial lineal homogéneo de orden n sobre K. Diremos que L es una **extensión de Picard-Vessiot de K para $\mathcal{L}$** si:

1. $L = K\langle y_1, \ldots, y_n \rangle$ donde $\{y_1, \ldots, y_n\}$ es un conjunto fundamental de soluciones de $\mathcal{L}(Y) = 0$ en L.

2. $C_K = C_L$.

Ejemplo 3.3. Consideremos el cuerpo diferencial $\mathbb{C}(z)$ dotado de la derivación usual $\dfrac{d}{dz}$ y consideremos el operador diferencial

$$\mathcal{L}(y) = y^{(n)} + a_{n-1}(z)y^{(n-1)} + \cdots + a_1(z)y' + a_0(z)y = 0.$$

Como $a_i(z) \in \mathbb{C}(z)$, estas son funciones meromorfas definidas sobre $\mathbb{C}\setminus\{z_{i0}, \ldots, z_{iN_i}\}$. Sabemos que si tomamos un conjunto abierto acotado simplemente conexo $U \subset \mathbb{C}\setminus\left\{z_{01}, \ldots, z_{0N_0} \ldots, z_{n-1,1}, \ldots, z_{n-1,N_{n-1}}\right\}$ y condiciones iniciales, entonces existen n únicas soluciones holomorfas linealmente independientes de $\mathcal{L}(y) = 0$ defnindas sobre U. Sea este conjunto fundamental de soluciones $\{f_1(z), \ldots, f_n(z)\}$. Podemos pensar en estas soluciones en el anillo $Hol(U)$ de funciones holomorfas sobre U. Entonces tenemos la extensión diferencial $\mathbb{C}(z) \subset \mathbb{C}(z)\langle f_1(z), \ldots, f_n(z)\rangle = L$ considerando la derivación usual sobre L, y pensando en L como un subcuerpo del cuerpo de funciones meromorfas $Mer(U)$ definidas sobre U. Así $\mathbb{C}(z) \subset \mathbb{C}(z)\langle f_1(z), \ldots, f_n(z)\rangle$ donde $\{f_1(z), \ldots, f_n(z)\}$ es un conjunto fundamental de soluciones de $\mathcal{L}(y) = 0$ en L. Finalmente, veamos que $C_K = C_L$. Sea $f(z) \in C_L$, como $L \subset Mer(U)$ entonces $f(z)$ es constante, es decir $f(z) \in C_K = \mathbb{C}$. Por lo tanto $\mathbb{C}(z)\langle f_1(z), \ldots, f_n(z)\rangle$ es una extensión de Picard-Vessiot de $\mathbb{C}(z)$ para $\mathcal{L}(y) = 0$.

Ahora veremos algunos ejemplos de extensiones de Picard-Vessiot con algunas condiciones necesarias. Asumiremos que trabajamos con cuerpos diferenciales cuyo cuerpo de constantes es algebraicamente cerrado, pues esto asegura la existencia y unicidad de una extensión de Picard-Vessiot tal como describimos completamente en las secciones respectivas (3.1.1 y 3.1.2).

Ejemplo 3.4. Sea K un cuerpo diferencial y sea $\alpha' = a \in K$ tal que a no es una derivada en K, es decir $a \neq x'$ para todo $x \in K$ (entonces $\alpha \notin K$). Consideremos la extensión $K \subset K\langle\alpha\rangle = L$. Diremos que L es obtenido de K por **adjunción de una integral**. Probaremos que:

- α es trascendente sobre K
- $K \subset L$ es una extensión de Picard-Vessiot para el operador diferencial

$$\mathcal{L}(Y) = Y'' - \frac{a'}{a}Y' \tag{3.1.1}$$

Supongamos que α es algebraico sobre K y sea

$$p(X) = X^n + \sum_{i=0}^{n-1} b_i X^{n-i}$$

su polinomio irreducible sobre K. Entonces:

$$p(\alpha) = \alpha^n + \sum_{i=0}^{n-1} b_i \alpha^{n-i} = \alpha^n + b_1\alpha^{n-1} + \cdots + b_{n-1}\alpha + b_n = 0$$

derivando,

$$n\alpha^{n-1}\alpha' + b_1'\alpha^{n-1} + b_1(n-1)\alpha^{n-2}\alpha' + \cdots + b_n' = 0$$

luego

$$(n\alpha' + b_1')\alpha^{n-1} + \sum_{i=0}^{n-2} \lambda_i \alpha^i = 0.$$

Entonces, por minimalidad de $p(X) : na + b_1' = 0$ luego $a = \left(-\frac{b_1}{n}\right)'$ lo cual es una contradicción. Asi, α no es algebraico.

En el operador diferencial (3.1.1) se cumple $\mathcal{L}(1) = 0$ y $\mathcal{L}(\alpha) = \alpha'' - \frac{a'}{a}\alpha' = 0$. Observamos que el conjunto $\{1, \alpha\}$ es C_K - linealmente independiente. Veamos que $K\langle 1, \alpha\rangle = K(\alpha)$ no contiene nuevas constantes. Supongamos que existe un elemento $l \in C_L$ tal que $l \notin C_K$. Entonces l es de la forma

$$\frac{f(\alpha)}{g(\alpha)}, \text{ donde } f(X), g(X) \in K[X]$$

Podemos asumir $(f(X), g(X)) = 1$ con g mónico de grado mayor ó igual a 1, minimal. Entonces

$$0 = \left(\frac{f(\alpha)}{g(\alpha)}\right)' = \frac{f(\alpha)'g(\alpha)\alpha' - f(\alpha)g(\alpha)'\alpha'}{g(\alpha)^2}. \tag{3.1.2}$$

Supongamos que $g(\alpha) \notin C_L$, es decir $g(\alpha)' \neq 0$ entonces de (3.1.2)

$$\frac{f(\alpha)'}{g(\alpha)'} = \frac{f(\alpha)}{g(\alpha)} \in C_L$$

pero $gr(g') < gr(g)$ lo cual contradice $(f(X), g(X)) = 1$. Así $g(\alpha) \in C_L$. Sea

$$g(\alpha) = \sum_{i=0}^{n} b_i \alpha^{n-i}, b_i \in K.$$

Derivando obtenemos

$$0 = g(\alpha)' = b_0'\alpha^n + (nb_0a + b_1')\alpha^{n-1} + \cdots + b_{n-1}'\alpha.$$

Como α es trascendental, todos los coeficientes de esta ecuación son cero entonces $b_0' = nb_0a + b_1' = 0$, luego

$$a' = \left(-\frac{b_1}{nb_0}\right)' = \frac{-nb_0b_1' + b_1nb_0'}{n^2b_0^2} = \frac{-nb_0b_1'}{n^2b_0^2} = \frac{-b_1'}{nb_0} \in K$$

lo cual contradice la hipótesis, pues a no es la derivada de ningún elemento de K. Luego L es una extensión de Picard Vessiot de K para $\mathcal{L}$.

Ejemplo 3.5. Sea K un cuerpo diferencial y sea $\alpha'/\alpha = a \in K\setminus\{0\}$. Consideremos la extensión $L = K\langle\alpha\rangle$. Diremos que L es obtenido de K por **adjunción de la exponencial de una integral**. Asumiremos que $C_K = C_L$. Consideremos el operador $\mathcal{L}(Y) = Y' - aY$, entonces $\mathcal{L}(\alpha) = 0$ y el conjunto $\{\alpha\}$ es C_K-linealmente independiente, luego $K \subset L$ es una extensión de Picard-Vessiot.
Estudiemos la extensión L. Supongamos que α es algebraico sobre K. Sea

$$p(X) = X^n + \sum_{i=0}^{n-1} a_i X^i$$

su polinomio irreducible. Evaluando en α y derivando

$$0 = p(\alpha)' = p^{(d)}(\alpha) + p'(\alpha)\alpha' = p^{(d)}(\alpha) + p'(\alpha)a\alpha = an\alpha^n + \sum_{i=0}^{n-1}(a_i' + aia_i)\alpha i.$$

Por minimalidad, $p(\alpha)$ divide a $p(\alpha)'$. Comparando el término de grado n tenemos que $p(\alpha)' = anp(\alpha)$, luego comparando los demás términos tenemos $a_i' + aia_i = ana_i$, entonces $a_i' = a(n-i)a_i$ para todo $i = 0, \ldots, n-1$. Así

$$\left(\frac{\alpha^{n-i}}{a_i}\right)' = \frac{a_i(\alpha^{n-i})' - a_i'\alpha^{n-i}}{a_i^2} = \frac{a_i(n-i)\alpha^{n-i-1}\alpha' - a(n-i)a_i\alpha^{n-i}}{a_i^2} = 0.$$

En particular para $i = 0$ tenemos $(\alpha^n/a_0)' = 0$ luego $\alpha^n = ca_0$ para algún $c \in C_L = C_K$. Luego $\alpha^n \in K$.
Entonces la extensión $L = K\langle\alpha\rangle$ puede ser algebraica con $\alpha^n \in K$ ó puramente trascendental con grado de trascendencia 1.

En los ultimos ejemplos hemos mostrado extensiones de Picard-Vessiot de K que son puramente trascendentales con grado de trascendencia 1, a pesar de que en el ejemplo 3.4 se obtiene a partir de un operador de grado 2 y en el ejemplo 3.5 a partir de un operador de grado 1. En el siguiente ejemplo veremos que un operador de grado n puede tener una extensión de Picard-Vessiot puramente trascendental de grado 1.

Ejemplo 3.6. Sea $K = \mathbb{C}(z)$ y consideremos el subcuerpo L de series de potencias $\mathbb{C}((z))$ generado por la serie exponencial e^z, es decir $L = K(e^z)$. Sea el operador

$$\mathcal{L}(Y) = \sum_{m=0}^{n} \binom{n}{m} (-1)^m Y^{n-m}.$$

Entonces $\left\{e^z, ze^z, \ldots, z^{k-1}e^z\right\}$ es un conjunto C_K linealmente independiente de soluciones de $\mathcal{L}(Y) = 0$ en L, y genera L como cuerpo diferencial sobre K. obviamente $C_K = C_L$. Así L es una extensión de Picard-Vessiot de K para $\mathcal{L}$.

3.1.1. Existencia

En el caso cuando K es un cuerpo diferencial con cuerpo de constantes C, algebraicamente cerrado; probaremos que existe una extension de Picard-Vessiot L de K para una ecuación diferencial lineal homogenea $\mathcal{L}$ definida sobre K y que es única salvo K-isomorfismo diferencial.

La idea para la prueba de existencia es construir una K-álgebra diferencial que contenga un conjunto completo de soluciones de la ecuación diferencial

$$\mathcal{L}(Y) = a_0Y + a_1Y' + \cdots + a_{n-1}Y^{(n-1)} + Y^{(n)} = 0, \quad a_i \in K$$

y luego llevar al cociente mediante un ideal diferencial maximal para obtener una extensión sin agregar constantes.

Construcción:

- Como vimos en la observación 2.32, el álgebra universal de soluciones

  $$R = K\left[Y_{ij}\right]\left[W^{-1}\right]$$

  de $\mathcal{L} = 0$, contiene un conjunto fundamental de soluciones de $\mathcal{L} = 0$. Pero R no es un cuerpo, es un anillo diferencial, de hecho es una $K-$álgebra diferencial y en general tiene demasiadas constantes.

- Si P es un ideal diferencial maximal de R, en la proposición 3.7 se probará que P es un ideal primo. Por tanto R/P es un dominio de integridad.

- Sea $L =$ el cuerpo de fracciones de R/P, en la proposición 3.8 se probará que L tiene el mismo cuerpo de constantes que K, esto es, $C_L = C_K$.

Así, L es extensión de Picard-Vessiot de K para $\mathcal{L}(Y) = 0$.

Proposición 3.7. *Sea K un cuerpo diferencial y $K \subset R$ una extensión de anillos diferenciales. Si I es un ideal maximal diferencial de R, entonces I es un ideal primo.*

Prueba. Como I es un elemento maximal en el conjunto de ideales diferenciales propios de R, el cociente R/I no posee ideales diferenciales no triviales. Probaremos que R/I es un dominio de integridad. Supongamos que R/I tiene divisores de cero, entonces existen $a, b \in R/I, a \neq 0, b \neq 0$ tales que $ab = 0$.

Así tenemos

$$d^k(a)b^{k+1} = 0, \quad \text{para todo} \quad k \in \mathbb{N}.$$

En efecto, procediendo por inducción:

Si $k = 1$: $ab = 0$ entonces $d(ab) = ad(b) + d(a)b = 0$, multiplicando por b tenemos $abd(b) + d(a)b^2 = 0$ luego $d(a)b^2 = 0$.

Si suponemos $d^k(a)b^{k+1} = 0$, derivando

$$d^{k+1}(a)b^{k+1} + d^k(a)(k+1)b^k d(b) = d(d^k(a)b^{k+1}) = 0.$$

Multiplicando por b

$$d^{k+1}(a)b^{k+2} + d^k(a)(k+1)b^{k+1}d(b) = 0.$$

De la hipótesis inductiva, el segundo sumando es igual a cero, así $d^{k+1}(a)b^{k+2} = 0$ y la afirmación queda probada.

Ahora, sea J el ideal diferencial generado por a, esto es, el ideal generado por a y sus derivadas.

Supongamos que b no es nilpotente, es decir $b^k \neq 0$, para todo $k \in \mathbb{N}$. Por la afirmación anterior, todos los elementos de J son divisores de cero. En efecto, sea $c \in J$, entonces $c = \sum_{k=0}^{n} \alpha_k d^k(a)$ para algunos $n \in \mathbb{N}$ y $\alpha_k \in R/I$. Luego bastará escoger b^{n+1}, y por la afirmación:

$$\left(\sum_{k=0}^{n} \alpha_k d^k(a) \right) b^{n+1} = 0.$$

Luego, $1 \notin J$, entonces $J \neq R/I$. Y como $a \neq 0$, $a \in J$, entonces J no es el ideal nulo. Así, J es un ideal diferencial propio de R/I, que es una contradicción. Entonces b es nilpotente.

Como b fue tomado como divisor de cero arbitrario, tenemos que todos los divisores de cero en R/I son nilpotentes, en particular a es nilpotente, entonces existe $m \in \mathbb{N}$ tal que $a^m = 0$. Sea $n = \min\{m \in \mathbb{N} / a^m = 0\}$.

$$na^{n-1}d(a) = d\left(a^n\right) = d(0) = 0. \tag{3.1.3}$$

Recordemos que asumimos que $\text{char}(K) = 0$. Como K es subanillo de R, $\text{char}(R) = 0$, y se prueba facilmente que $\text{char}\left(R/I\right) = 0$. Entonces $na^{n-1} \neq 0$ para todo $n \in \mathbb{N}$, y por 3.1.3, $d(a)$ es un divisor de cero.

Así, hemos probado que la derivada de un divisor de cero, es también un divisor de cero, entonces a y todas sus derivadas son divisores de cero y por tanto nilpotentes. Luego J es un ideal diferencial de elementos nilpotentes, entonces $1 \notin J$ y $J \neq R/I$, es decir, J es un ideal diferencial propio de R/I, que es una contradicción. Así, R/I no tiene divisores de cero. □

Existen ideales maximales que no son ideales diferenciales. Sea el anillo $R = K[X]$, $I = \langle X \rangle$ es un ideal maximal de R pero $X' = 1 \in d(I)$ y $1 \notin I$. Luego I no es un ideal diferencial.

Proposición 3.8. *Sea K un cuerpo diferencial con cuerpo de constantes C_K algebraicamente cerrado y sea $K \subset R$ una extension de anillos diferenciales, donde R es un dominio de integridad finitamente generado como K-algebra, que no tiene ideales diferenciales propios. Sea $L = Frac(R)$ el cuerpo de fracciones de R. Entonces $C_L = C_K$.*

Prueba. La demostración se presenta en tres partes complementarias.

1. Primero probaremos que los elementos de $C_L \backslash C_K$ no son algebraicos sobre K. Sea $\alpha \in C_L \backslash C_K$. Supongamos que α es algebraico sobre K, es decir $\alpha \in \overline{K}$. De la prueba de la proposición 3.15, tenemos que si $P(X) = a_0 + a_1 X + \cdots + a_{n-1}X^{n-1} + X^n$ es el polinomio irreducible de α sobre K,

$$0 = \alpha' = \frac{-P^d(\alpha)}{P'(\alpha)},$$

donde $P^d(X)$ y $P'(X)$ son como en la observación 2.9. Luego $P^d(\alpha) = 0$, es decir, α es raíz de $P^d(X) \in K[X]$ que tiene grado $n-1$, entonces por minimalidad de $P(X)$:

$$P^d(X) = a_0' + a_1' X + \cdots + a_{n-1}' X^{n-1} = 0.$$

Como C_K es algebraicamente cerrado, K es infinito, entonces las funciones polinomiales coinciden con el conjunto de polinomios sobre K. Así $a_i' = 0$, para todo $i = 1, \ldots, n-1$ y como $a_n = 1 \in C_K$, $P(X) \in C_K[X]$. Como α es raíz de $P(X)$ y C_K es algebraicamente cerrado: $\alpha \in C_K$, lo cual es una contradicción.

2. Probaremos que $C_L \subset R$.

   Sea $b \in C_L$, entonces $b \in L$ y $b' = 0$. Sea $b = f/g$ con $f, g \in R$ y $g \neq 0$. Consideremos el conjunto $J = \{h \in R : hb \in R\}$. Dado $h \in J$ tenemos que $h'b = (hb)' - hb' \in R$, luego $h' \in J$. Así J es un ideal diferencial, pero por hipótesis R no contiene ideales diferenciales propios, entonces $J = R$ o $J = 0$. Como $gb = f \in R$ tenemos que $g \in J$ luego $J \neq 0$, así $J = R$. Como $1 \in R = J$ entonces $b \in R$.

3. Probaremos que $C_L \subset C_K$. Para lograr esto, inicialmente veremos que para cualquier $b \in C_L$, existe $c \in C_K$ tal que $b - c$ no es inversible en R. Luego tendremos que el ideal $\langle b - c \rangle = R(b - c) \neq R$, y por hipótesis de R, no solo se obtiene $R(b - c) = 0$, sino también $b = c$. Es decir, $b \in C_K$ y así se obtien la inclusión $C_L \subset C_K$

   Sea $\overline{K}$ la clausura algebraica de K, primero pasamos a la extension escalar $\overline{R} = R \otimes_K \overline{K}$ (extensión de R al cuerpo $\overline{K}$) que es un anillo con identidad $1 \otimes_K 1$. En este contexto, es útil considerar el siguiente diagrama de extension de anillos para usar la propiedades básicas de la geometría algebraíca en cuerpos algebraicamente cerrados.

$$\begin{array}{ccc} R & \longmapsto & R \otimes_K \overline{K} \\ \Big| & & \Big| \\ K & \longmapsto & \overline{K} \end{array} .$$

   En otras palabras, estamos considerando la siguiente identificación natural que se construye con el producto tensorial.

$$\begin{aligned} \varphi : R &\longrightarrow \overline{R} = R \otimes_K \overline{K} \\ x &\longmapsto x \otimes_K 1 \end{aligned}$$

   De este modo, si $b \otimes_K 1 - c \otimes_K 1 = (b - c) \otimes_K 1$ no es una unidad en $\overline{R}$, entonces $b - c$ no es una unidad en R. Así podemos pasar este problema a $\overline{R}$, es decir reemplazaremos:

$$\begin{aligned} R &\longmapsto R \otimes_K \overline{K} \\ K &\longmapsto K \otimes_K \overline{K} \simeq \overline{K} \\ b &\longmapsto b \otimes_K 1 = \overline{b} \end{aligned} \tag{3.1.4}$$

De (3.1.4) podemos asumir que K es algebraicamente cerrado.
Sea V la variedad algebraica afín con anillo de coordenadas $\overline{R}$:

$$\overline{K}[V] = \overline{R}.$$

Entonces $\overline{b} \in \overline{R}$ define una función sobre V con valores en $\overline{K}$:

$$\overline{b} \in \overline{R} \simeq \frac{\overline{K}[X_1, ..., X_n]}{\mathcal{I}(V)},$$

entonces existe $f(X_1, ..., X_n) \in \overline{K}[X_1, ..., X_n]$ tal que $\overline{b} = \overline{f} = f + I(V) = f|_V$.
Luego tenemos:

$$f : V \longrightarrow \overline{K} = \mathbb{A}^1.$$

Por el teorema de Chevalley (teorema 1.9), $f(V)$ es constructible en la línea afín $\mathbb{A}^1$ entonces es un conjunto finito de puntos ó el complemento de un conjunto finito de puntos.
Si $f(V)$ es el complemento de un conjunto finito: como C_K es algebraicamente cerrado, es infinito; luego existe $v \in V$ tal que $f(v) \in C_K$, es decir

$$f(v) = c \otimes_K 1 \in C_K \otimes_K \overline{K} \subset K \otimes_K \overline{K} \simeq \overline{K}$$

donde $c \in C_K$. Así se tiene que $(f - c \otimes_K 1)(v) = f(v) - c \otimes_K 1 = 0$, luego $b \otimes_K 1 - c \otimes_K 1 \in \mathfrak{m}_v$, donde $\mathfrak{m}_v$ es el ideal maximal que define v. Luego $b - c$ no es inversible en R.
Si $f(V)$ es finito: como R es un dominio, $\mathcal{I}(V)$ es primo; entonces V es irreducible (conexo) y $f(V)$ es conexo, es decir es un solo punto. Entonces existe $a \in K$ tal que $f(V) = \{a \otimes_K 1\}$, luego f es constante y $b \in K$. Como $b \in C_L$, y hemos concluido que $b \in K$ tenemos $b \in C_K$. Por lo tanto $C_L \subset C_K$.

Se concluye la proposición. □

Teorema 3.9. *Sea K un cuerpo diferencial con cuerpo de constantes algebraicamente cerrado C. Sea $\mathcal{L}(Y) = 0$ una ecuación diferencial lineal homogénea definida sobre K. Sea R el álgebra universal de soluciones para $\mathcal{L}$ y sea P un ideal diferencial maximal de R. Entonces P es un ideal primo y el cuerpo de fracciones L del dominio R/P es una extensión de Picard-Vessiot de K para $\mathcal{L}$.*

Prueba. $R = K[Y_{ij}][W^{-1}]$ es diferencialmente generado sobre K por las soluciones de $\mathcal{L}(Y) = 0$ y por W^{-1}, entonces R/P también es diferencialmente

generado sobre K. Como P es un ideal diferencial maximal de R, por la proposición 3.7 , P es primo, entonces R/P es un dominio de integridad, luego tiene sentido considerar su cuerpo de fracciones. Como P es un ideal diferencial maximal, R/P no tiene ideales diferenciales propios. Luego por la proposición 3.8 tenemos $C_K = C_L$, es más, L es diferencialmente generado sobre K por las soluciones de $\mathcal{L}(Y) = 0$, y el Wronskiano inverso de R es también inversible en R/P y en particular es distinto de cero en L, entonces $\mathcal{L}(Y) = 0$ tiene un conjunto total de soluciones en L. Entonces $L|K$ es una extensión de Picard-Vessiot para $\mathcal{L}$. □

3.1.2. Unicidad

En esta sección se presentan algunos condiciones para garantizar la unicidad de la extensión que estamos estudiando. Especificamente, el resultado aparece en el teorema 3.16, donde puede verse que la unicidad sólo es posible salvo isomorfismos, para lo cual la siguiente proposición es de vital importancia.

Proposición 3.10. *Sean L_1, L_2 extensiones de Picard-Vessiot de K para un operador diferencial lineal homogéneo $\mathcal{L}$ de orden n y sea $K \subset L$ una extensión diferencial con $C_L = C_K$. Sean $\sigma_1 : L_1 \to L$, $\sigma_2 : L_2 \to L$ dos K-morfismos diferenciales. Entonces $\sigma_1(L_1) = \sigma_2(L_2)$.*

Prueba. Sea $V_1 = \{y \in L_1 : \mathcal{L}(Y) = 0\}$. Como $\mathcal{L}$ es de grado n sobre K y L_1 es una extensión de Picard-Vessiot de K, entonces $\dim_{C_K} V_1 = n$.

$$\begin{array}{ccccc} L_1 & \xrightarrow{\sigma_1} & L & \xleftarrow{\sigma_2} & L_2 \\ & \searrow & \downarrow & \swarrow & \\ & & K & & \end{array}$$

Sea $V = \{y \in L : \mathcal{L}(Y) = 0\}$. Como $\mathcal{L}$ tiene grado n, por el corolario 2.26 , tiene a lo más n soluciones C_K-linealmente independientes, entonces

$$\dim_{C_K} V \leq n.$$

Ahora veremos que $\sigma_i(V_i) \subset V, i = 1, 2$. En efecto, sea $y \in V_1$, $\mathcal{L}(y) = 0$ y $y \in L_1$. Como σ_1 es un morfismo, $\mathcal{L}(\sigma_1(y)) = 0$, por otro lado, $\sigma_1(y) \in \sigma_1(L_1) \subset L$, asi $\sigma_1(y) \in V$. Analogamente $\sigma_2(V_2) \subset V$ y se obtiene

$$n = \dim_{C_K} V_1 = \dim_{C_K}[\sigma_1(V_1)] \leq \dim_{C_K} V.$$

Entonces $\sigma_1(V_1) = \sigma_2(V_2) = V$. Como L_1 y L_2 son extensiones de Picard-Vessiot de L entonces $L_1 = K\langle V_1\rangle$ y $L_2 = K\langle V_2\rangle$. Luego, $\sigma_1(L_1) \subset \sigma_2(L_2)$. El otro contenido es análogo. □

Corolario 3.11. *Sea $K \subset L \subset M$ una extensión de cuerpos diferenciales, L una extensión de Picard-Vessiot de K con $C_M = C_k$. Entonces para todo K-automorfismo diferencial $\sigma : M \to M$: $\sigma(L) = L$.*

Prueba. Consideremos el diagrama (donde id es la inclusión $id : L \hookrightarrow M$).

$$\begin{array}{ccccc} L & \xrightarrow{\sigma_1 = id} & M & \xleftarrow{\sigma_2 = \sigma} & M \\ & \searrow & \downarrow & \swarrow & \\ & & K & & \end{array}$$

Por la proposición anterior se obtiene

$$\begin{aligned} \sigma_1(L) &= \sigma_2(L) \\ i(L) &= \sigma_{|L}(L) \\ L &= \sigma(L) \end{aligned}$$

Por lo tanto, el corolario se cumple. □

Corolario 3.12. *Sea K un cuerpo diferencial con C_K algebraicamente cerrado. Si L es una extensión de Picard-Vessiot algebraica de K, entonces L es una extensión algebraica normal de K.*

Prueba. Sea $\overline{K}$ una clausura algebraica de K con $K \subset L \subset \overline{K}$ y sea el monomorfismo $\sigma : L \to \overline{K}$ tal que $\sigma_{|_K} = id_K$, probaremos que $\sigma(L) = L$. Como $\overline{K}$ es una extensión algebraica de K, por proposición 2.17 se tiene que $\overline{K}$ es una extensión diferencial de K y todo $K-$automorfismo de $\overline{K}$ es diferencial.

Sea $\alpha \in C_{\overline{K}}$ y sea $p(X)$ el polinomio irreducible de α sobre K, usando la notación de la observación 2.9:

$$0 = (p(\alpha))' = p^{(d)}(\alpha) + p'(\alpha)\alpha' = p^{(d)}(\alpha).$$

Como $p^{(d)}[X] \in C_K[X]$ y C_K es algebraicamente cerrado entonces $\alpha \in C_K$. Así $C_{\overline{K}} = C_K$, luego por el corolario 3.11 se tiene $\sigma(L) = L$. □

Ejemplo 3.13. Consideremos la extensión diferencial $K = \mathbb{R}(x, e^{3x}) \subset \mathbb{R}(x, e^x) = L$ con la derivación usual. Sea $F = \mathbb{R}(x)$ entonces $K = F(e^{3x})$ y $L = F(e^x)$. Sea

$$p(\lambda) = \lambda^3 - e^{3x} \in K[\lambda]$$

entonces $p(e^x) = 0$, luego la extensión es algebraica pero

$$p(\lambda) = \lambda^3 - e^{3x} = (\lambda - e^x)(\lambda^2 + \lambda e^x + e^{2x})$$

es decir, $p(\lambda)$ no se factoriza en términos lineales sobre $L[\lambda]$ luego la extensión no es normal. Ahora, si consideramos el operador diferencial lineal $\mathcal{L}(Y) = Y - Y'$ se tiene que $\mathcal{L}(e^x) = 0$ luego $K\langle e^x \rangle = K(e^x)$ es una extensión de Picard - Vessiot de K para $\mathcal{L}$, pero $K(e^x) = \mathbb{R}(x, e^{3x}, e^x) = \mathbb{R}(x, e^x) = L$.

Sin embargo esto no contradice el corolario anterior pues $C_K = \mathbb{R}$ no es algebraicamente cerrado.

Ejemplo 3.14. Consideremos la extensión diferencial $\mathbb{Q}(x) \subset \mathbb{Q}(x)(\sqrt[n]{x})$ con la derivación usual, donde $n \geq 2$. Sea

$$p(\lambda) = \lambda^n - x \in \mathbb{Q}(x)[\lambda]$$

entonces $p(\sqrt[n]{x}) = 0$, luego la extensión es algebraica pero

$$p(\lambda) = (\lambda - \sqrt[n]{x})(\lambda^{n-1} + \lambda^{n-2}\sqrt[n]{x} + \cdots + \lambda\sqrt[n]{x^{n-2}} + \sqrt[n]{x^{n-1}})$$

es decir, $p(\lambda)$ no se factoriza en términos lineales sobre $\mathbb{Q}(x)(\sqrt[n]{x})[\lambda]$ luego la extensión no es normal. Consideremos el operador diferencial lineal

$$\mathcal{L}(Y) = Y' - \frac{1}{nx}Y,$$

se tiene que $\mathcal{L}(\sqrt[n]{x}) = 0$ luego $\mathbb{Q}(x)\langle \sqrt[n]{x} \rangle = \mathbb{Q}(x)(\sqrt[n]{x})$ es una extensión de Picard Vessiot de $\mathbb{Q}(x)$ para $\mathcal{L}$. Esto no contradice el corolario 3.12 pues $C_{\mathbb{Q}(x)} = \mathbb{Q}$ no es algebraicamente cerrado.

Para estudiar el teorema de la unicidad via K - isomorfismo de una extensión de Picard-Vessiot seran necesarias las derivaciones en productos tensoriales, las cuales se ilustran en el siguiente ejemplo.

Ejemplo 3.15. Sea R un anillo diferencial, y sean S y T dos $R-$álgebras diferenciales. Definimos

$$\begin{aligned} D : S \otimes_R T &\to S \otimes_R T \\ s \otimes_R t &\mapsto d_S(s) \otimes_R t + s \otimes_R d_T(t). \end{aligned}$$

Es fácil verificar que se cumplen las propiedades de derivación dadas en la definición 2.1. Veamos que está bien definida.

Primero consideremos el caso en que R está dotada de la derivación trivial, entonces dados $r \in R$ y $s \in S$:

$$d_S(rs) = d_S(r)s + rd_S(s) = d_R(r)s + rd_S(s) = rd_S(s),$$

luego d_S y analogamente d_T son $R-$lineales, así D está bien definida.

Para el caso general, sea C el cuerpo de constantes de R, entonces por lo visto en el caso anterior, D está bien definida sobre $S \otimes_C T$. Consideremos el conjunto

$$X = \{r \otimes_C 1 - 1 \otimes_C r : r \in R\}$$

entonces

$$\begin{aligned} D\left(r \otimes_C 1 - 1 \otimes_C r\right) &= D\left(r \otimes_C 1\right) - D\left(1 \otimes_C r\right) \\ &= d_S(r) \otimes_C 1 + r \otimes_C d_T(1) - d_S(1) \otimes_C r - 1 \otimes_C d_T(r) \\ &= d_S(r) \otimes_C 1 - 1 \otimes_C d_T(r) \end{aligned}$$

luego $D(X) \subset X$, así $\langle X \rangle$ es un ideal diferencial de $S \otimes_C T$ y por el ejemplo 2.14, $\dfrac{S \otimes_C T}{\langle X \rangle}$ es un anillo diferencial con derivación

$$\widehat{D}\left(\overline{s \otimes_C t}\right) = \overline{D\left(s \otimes_C t\right)}.$$

Definimos

$$\begin{aligned} \psi : S \otimes_C T &\to S \otimes_R T \\ s \otimes_C t &\mapsto s \otimes_R t \end{aligned}$$

Claramentte ψ es sobreyectva, luego por el primer teorema de isomorfismo de anillos $\dfrac{S \otimes_C T}{\langle X \rangle} \simeq S \otimes_R T$ donde el isomorfismo inducido por ψ es

$$\begin{aligned} \overline{\psi} : \frac{S \otimes_C T}{\langle X \rangle} &\to S \otimes_R T \\ \overline{s \otimes_C t} &\mapsto s \otimes_R t \end{aligned}$$

Luego podemos definir una derivación sobre $S \otimes_R T$ considerando el diagrama:

$$\begin{array}{ccc} S \otimes_R T & \xrightarrow{\overline{\psi}^{-1}} & \dfrac{S \otimes_C T}{\langle X \rangle} \\ {\scriptstyle D}\downarrow & & \downarrow{\scriptstyle \widehat{D}} \\ S \otimes_R T & \xleftarrow[\overline{\psi}]{} & \dfrac{S \otimes_C T}{\langle X \rangle} \end{array}$$

luego

$$\begin{aligned} D\left(s \otimes_R t\right) &= \overline{\psi} \circ \widehat{D} \circ \overline{\psi}^{-1}\left(s \otimes_R t\right) \\ &= \overline{\psi} \circ \widehat{D}\left(\overline{s \otimes_C t}\right) \\ &= \overline{\psi}\left(\overline{D\left(s \otimes_C t\right)}\right) \\ &= \overline{\psi}\left(\overline{d_S(s) \otimes_C t + s \otimes_C d_T(t)}\right) \\ &= \overline{\psi}\left(\overline{d_S(s) \otimes_C t} + \overline{s \otimes_C d_T(t)}\right) \\ &= d_S(s) \otimes_R t + s \otimes_R d_T(t) \end{aligned}$$

Para concluir esta sección, se presenta el resultado más importante sobre la unicidad de la extension de Picard-Vessiot.

Teorema 3.16. *Sea K un cuerpo diferencial con C_K algebraicamente cerrado y $\mathcal{L}(Y) = 0$ una ecuación diferencial lineal homogenea sobre K. Sean L_1, L_2 extensiones Picard-Vessiot de K para $\mathcal{L}$. Entonces existe un $K-$isomorfismo diferencial de L_1 en L_2.*

Prueba. Podemos asumir que L_1 es la extensión Picard-Vessiot de K construida en el teorema 3.9 , es decir, L_1 es el cuerpo de fracciones de R/P donde $R = K\left[Y_{ij}\right]\left[W^{-1}\right]$ es el álgebra universal de soluciones de $\mathcal{L}$ y P es un ideal diferencial maximal de R. Construiremos una extensión diferencial E/K con $C_E = C_K$, y morfismos K- diferenciales $\varphi_1 : L_1 \to E$, $\varphi_2 : L_2 \to E$ y aplicaremos la proposición 3.10.

Notemos que $R/P = K\left[y_{ij}, w^{-1}\right]$ donde y_{ij} y w^{-1} son las clases de Y_{ij} y W^{-1}.

Consideremos el anillo $A = (R/P) \otimes_K L_2$.

$$A = (R/P) \otimes_K L_2 = K\left[y_{ij}, w^{-1}\right] \otimes_K L_2 = (K \otimes_K L_2)\left[y_{ij}, w^{-1}\right] = L_2\left[y_{ij}, w^{-1}\right].$$

Entonces A es finitamente generado como L_2-álgebra, con derivación:

$$\begin{aligned} d : (R/P) \otimes_K L_2 &\longrightarrow (R/P) \otimes_K L_2 \\ x \otimes y &\longmapsto dx \otimes y + x \otimes dy \end{aligned}$$

Sea Q un ideal diferencial maximal propio de A y consideremos su imagen inversa $I = \{a \in R/P : a \otimes 1 \in Q\}$ en R/P por la aplicación

$$\begin{aligned} \phi : R/P &\longrightarrow A \\ a &\longmapsto a \otimes 1 \end{aligned}$$

Recordemos que como P es un ideal diferencial maximal, R/P no tiene ideales diferenciales propios. Entonces $I = 0$, o bien $I = R/P$.

Si $I = R/P$ tenemos $1 \in I$ entonces $1 \otimes 1 \in Q$ luego $Q = A$, lo cual no es posible pues Q es un ideal diferencial maximal. Entonces $I = 0$ y la aplicación

$$\begin{aligned} \varphi : R/P &\longrightarrow A/Q \\ a &\longmapsto \overline{a \otimes 1} = (a \otimes 1) + Q \end{aligned}$$

es inyectiva. En efecto, si $\varphi(a) = \varphi(b)$ entonces $a \otimes 1 + Q = b \otimes 1 + Q$ luego $(a - b) \otimes 1 = (a \otimes 1) - (b \otimes 1) \in Q$, así $a - b \in I = 0$ y $a = b$.

Consideremos ahora

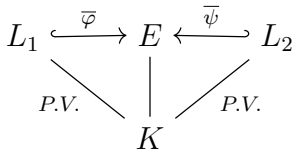
$$\begin{aligned} \psi : L_2 &\longrightarrow A/Q \\ b &\longmapsto \overline{1 \otimes b} = (1 \otimes b) + Q. \end{aligned}$$

Se prueba de manera similar que es también inyectiva.

Por la proposición 3.7 , Q es primo y por tanto A/Q es un dominio de integridad. Sea E su cuerpo de fracciones. Como sabemos, un morfismo entre dominios induce un morfismo entre sus respectivos cuerpos de fracciones, luego φ induce un morfismo $\overline{\varphi} : L_1 \longrightarrow E$. Por otro lado, sea $\nu : A/Q \longrightarrow E$ la aplicación canónica entre el dominio A/Q y su cuerpo de fracciones, y llamemos $\overline{\psi} = \nu \circ \psi$.

Así tenemos que, el cuerpo diferencial L_2 esta contenido en el dominio A/Q que es finitamente generado como L_2 álgebra (pues A es finitamente generado como L_2 álgebra) y A/Q no tiene ideales diferenciales propios (pues Q es un ideal diferencial maximal). Entonces, por la proposición 3.8 : $C_E = C_{L_2}$. Y como L_2 es una extensión de Picard-Vessiot de K, $C_{L_2} = C_K$. Luego $C_E = C_K$.

Entonces tenemos:



Luego, por la proposición 3.10 : $\overline{\varphi}(L_1) = \overline{\psi}(L_2)$. Entonces podemos definir un isomorfismo $f : L_1 \longrightarrow \overline{\varphi}(L_1) = \overline{\psi}(L_2) \longrightarrow L_2$ □

3.1.3. La existencia y la unicidad, revisados

El sigueinte teorema se obtiene como una aplicación directa de los resultados anteriores. En esta sección analizaremos la necesidad de la clausura de cuerpo de constantes para obtener la existencia (ejemplo 3.18) y la unicidad (ejemplo 3.23).

Teorema 3.17. *Sea K un cuerpo diferencial con C_K algebraicamente cerrado y sea $\mathcal{L}(Y) = 0$ definido sobre K. Entonces existe una extensión de Picard - Vessiot L de K para $\mathcal{L}$ y es única salvo K-isomorfismo diferencial.*

En los ejemplos a continuación veremos que si C_K no es algebraicamente cerrado, entonces no siempre es posible obtener existencia ó unicidad salvo isomorfismo de una extensión de Picard-Vessiot.

El siguiente ejemplo es dado por Seidenberg, se puede consultar [11].

Ejemplo 3.18. Sea $K = \mathbb{R}\langle a \rangle$ donde $a = \dfrac{i}{2}\operatorname{sen} 2x$ y K está equipado con la derivación usual sobre el anillo de funciones analíticas.

Como $a' = i\cos 2x$ y $a'' = -2i\operatorname{sen} 2x = -4a$ entonces $K = \mathbb{R}(a, a')$. Notemos que a es trascendental sobre $\mathbb{R}$, y considerando el polinomio:

$$p(X) = X^2 + 4a^2 + 1 \in \mathbb{R}(a)[X]$$

se verifica que

$$p(a') = a'^2 + 4a^2 + 1 = -\cos 2x^2 - \sin 2x^2 + 1 = 0 \tag{3.1.5}$$

es decir a' es algebraico de grado 2 sobre $\mathbb{R}(a)$. Así

$$K = \mathbb{R}(a, a') = \mathbb{R}(a)(a') = \mathbb{R}(a)[a'].$$

Afirmación: $C_K = \mathbb{R}$. Sea $c \in C_K$, entonces c es de la forma:

$$c = p + qa \text{ donde } p, q \in \mathbb{R}(a).$$

Derivando:

$$\begin{aligned} 0 &= \frac{dp}{da}a' + \frac{dq}{da}a'^2 + qa'' \\ &= \frac{dp}{da}a' - (4a^2+1)\frac{dq}{da} - 4aq \end{aligned}$$

entonces tenemos

$$\frac{dp}{da} = 0, \tag{3.1.6}$$

$$(4a^2+1)\frac{dq}{da} + 4aq = 0. \tag{3.1.7}$$

De (3.1.6): $p \in \mathbb{R}$. Supongamos que $q \neq 0$, entonces podemos escribirlo de la forma

$$q = (4a^2+1)^r \frac{m}{n}$$

donde $r \in \mathbb{Z}$, $m, n \in \mathbb{R}[a]$ no son divisibles por $4a^2+1$. Entonces reemplazando en (3.1.7) obtenemos

$$(4a^2+1)\left[r(4a^2+1)^{r-1}(8a)\frac{m}{n} + (4a^2+1)^r\left(\frac{dm}{da}n - m\frac{dn}{da}\right)\frac{1}{n^2}\right] + 4a(4a^2+1)^r\frac{m}{n} = 0,$$

y simplificando se tiene

$$(4a^2+1)\left(\frac{dm}{da}n - m\frac{dn}{da}\right) + 4a(1+2r)mn = 0.$$

Pero esto contradice la condición de que $4a^2+1$ no divide a m y n. Entonces $q = 0$, así $c = p \in \mathbb{R}$ y la afirmación queda probada.

Consideremos ahora el operador diferencial $\mathcal{L}(Y) = Y'' + Y$ definido sobre K, y sea η una solución no trivial de $\mathcal{L}(Y) = 0$. Probaremos que no es posible encontrar una extensión de Picard-Vessiot de K para $\mathcal{L}$. Para esto bastará probar que cualquier extensión diferencial de K que contenga a η agrega constantes.

Sea $u = \dfrac{\eta'}{\eta}$ entonces $K\langle u\rangle \subset K\langle \eta\rangle$. Probaremos que $K\langle u\rangle$ contiene una constante que no pertenece a $\mathbb{R}$.

Es fácil ver que

$$\left(\frac{\eta'}{\eta}\right)' + \left(\frac{\eta'}{\eta}\right)^2 + 1 = \frac{\eta''\eta - \eta'^2}{\eta^2} + \frac{\eta'^2}{\eta^2} + 1 = 0$$

luego u satisface la ecuación de Riccatti:

$$u' = -1 - u^2$$

Si $u^2 + 1 = 0$ entonces $u = \pm i$, que es una nueva constante. Si $u^2 + 1 \neq 0$ tenemos:

$$(1 + u^2)' = 2uu' = -2u(1 + u^2) \tag{3.1.8}$$

$$\begin{aligned}(a + a'u - au^2)' &= a' + a''u + a'u' - a'u^2 - 2au'u \\ &= a' - 4au - a'(1 + u^2) - a'u^2 + 2a(1 + u^2)u \\ &= -2u(a + a'u - au^2) \end{aligned} \tag{3.1.9}$$

Sea

$$c = \frac{a + a'u - au^2}{1 + u^2} \tag{3.1.10}$$

entonces de (3.1.8) y (3.1.9) se verifica que $c' = 0$. Si $c \notin \mathbb{R}$ entonces c es una nueva constante. Si $c \in \mathbb{R}$, de (3.1.10) tenemos:

$$(c + a)u^2 - a'u + (c - a) = 0.$$

Usando la fórmula general

$$u = \frac{a' \pm \sqrt{a'^2 - 4(c + a)(c - a)}}{2(c + a)}$$

entonces

$$\sqrt{a'^2 - 4(c + a)(c - a)} \in K\langle u \rangle .$$

De (3.1.5) :

$$a'^2 - 4(c + a)(c - a) = a'^2 + 4a^2 - 4c^2 = -1 - 4c^2 < 0$$

luego

$$\sqrt{-1 - 4c^2} = i\sqrt{1 + 4c^2} \in K\langle u \rangle .$$

Como $\sqrt{1 + 4c^2} \in \mathbb{R}$ entonces $i \in K\langle u \rangle$ y esta es una nueva constante.

El cuerpo $K\langle u\rangle$ en el ejemplo 3.18

En este ejemplo de Seidenberg, podemos hallar el cuerpo de constantes de $K\langle u\rangle$ y veremos que es una extensión clásica de la forma $\mathbb{R}(c,d)$ (corolario 3.21). Para dar una descripcion completa, usaremos los siguientes lemas:

Lema 3.19. *Sea K un cuerpo diferencial y la ecuación*

$$u' = p + qu - u^2 \tag{3.1.11}$$

definida sobre K. Sea u una solución de (3.1.11) y sea $L = K\langle u\rangle$. Si $C_K \subsetneq C_L$, es decir u genera una nueva constante $k \neq 0$ entonces es de la forma $\dfrac{f(u)}{g(u)}$ donde $f(u), g(u) \in K[u]$ y $\deg(f) = \deg(g)$.

Prueba. Sea un polinomio $h(u) \in K[u]$

$$h(u) = a_0 + a_1 u + \cdots + a_n u^n$$

derivando

$$\begin{aligned} h'(u) &= a_0' + a_1' u + a_1 u' + \cdots + a_n' u^n + a_n n u^{n-1} u' \\ &= a_0' + a_1' u + a_1(p + qu - u^2) + \cdots + a_n' u^n + a_n n u^{n-1}(p + qu - u^2) \end{aligned}$$

luego $\deg(h') = 1 + \deg(h) > 0$, entonces ningún polinomio puede ser constante.

Sea $k \neq 0$ una constante, como u es solución de (3.1.11), los elementos de L son de la forma $\dfrac{f(u)}{g(u)}$ donde $f(u), g(u) \in K[u]$ y podemos asumir $(f(u), g(u)) = 1$.

Supongamos que $\deg(f) > \deg(g)$ entonces

$$\frac{f}{g} = \varphi + \frac{f_1}{g} \tag{3.1.12}$$

donde $\deg(f_1) < \deg(g)$, $f_1 \neq 0$, $\varphi \neq 0$ y $\deg(\varphi) > 0$. Derivando (3.1.12):

$$0 = \varphi' + \frac{f_1' g - f_1 g'}{g^2}$$

pero

$$\begin{aligned} \deg\left(\frac{f_1' g - f_1 g'}{g^2}\right) &= \text{máx}\left\{\deg(f_1' g), \deg(f_1 g')\right\} - \deg(g^2) \\ &= \deg(f_1) + \deg(g) + 1 \leq 0 \end{aligned}$$

mientras que $\deg(\varphi) > 0$. □

Si consideramos la ecuación

$$u' = p + qu + ru^2,\ r \neq 0 \tag{3.1.13}$$

se prueba de manera similar, el mismo resultado. Si agregamos la hipótesis adicional $p \neq 0$ se verifica el siguiente resultado:

Lema 3.20. *Sea u una solución de (3.1.13) y $p \neq 0$. Si $\dfrac{f(u)}{g(u)} \neq 0$ es una constante donde $f(u), g(u) \in K[u]$ y $(f(u), g(u)) = 1$ entonces $f(0) \neq 0$ y $g(0) \neq 0$.*

Prueba. Como $\dfrac{f(u)}{g(u)} \neq 0$ es una constante entonces $\deg(f) = \deg(g)$. Haciendo $v = \dfrac{1}{u}$ la ecuación (3.1.13) se convierte en

$$v' = -r - qv - pv^2 \tag{3.1.14}$$

Sean $f_1(v) = \dfrac{f(u)}{u^{\deg(f)}}$ y $g_1(v) = \dfrac{g(u)}{u^{\deg(g)}}$ entonces

$$\frac{f_1(v)}{g_1(v)} = \frac{f(u)}{g(u)}$$

Como $p \neq 0$ la ecuación (3.1.14) tiene la forma de (3.1.13), luego se cumple $\deg(f_1) = \deg(g_1)$. Sean

$$f(u) = a_0 + a_1 u + \cdots + a_n u^n$$
$$g(u) = b_0 + b_1 u + \cdots + b_n u^n$$

entonces $f(0) = a_0$, $g(0) = b_0$ y

$$f_1(v) = a_0 v^n + a_1 v^{n-1} + \cdots + a_{n-1} v + a_n$$
$$g_1(v) = b_0 v^n + b_1 v^{n-1} + \cdots + b_{n-1} v + b_n$$

luego $\deg(f_1) = \deg(f) = n = \deg(g) = \deg(g_1)$ sí y sólo si $a_0 \neq 0$ y $b_0 \neq 0$. □

Corolario 3.21. *En el contexto del ejemplo 3.18, si se considera la constante $c \in C_{K\langle u\rangle}$ como en la ecuación (3.1.10) y*

$$d = \frac{a' - 4au - a'u^2}{1 + u^2},$$

entonces se cumple que el cuerpo de constantes de $K\langle u\rangle$ es $\mathbb{R}(c, d)$.

Prueba. Probaremos inicialmente que $d \in C_{K\langle u\rangle}$, por un calculo directo. Como

$$\begin{aligned}(a' - 4au - a'u^2)' &= a'' - 4au' - 4a'u - a''u^2 - 2a'uu' \\ &= -4a + 4a(1+u^2) - 4a'u + 4au^2 + 2a'u(1+u^2) \\ &= -2u(a' - 4au - a'u^2),\end{aligned}$$

es fácil verificar que $d' = 0$ y se obtiene que d es una constante de $K\langle u\rangle$. Por lo tanto,

$$c, d \in C_{K\langle u\rangle}$$

Por el lema 3.20, cada constante del cuerpo $K\langle u\rangle$ es de la forma $\dfrac{f(u)}{g(u)}$ donde $f(u), g(u) \in K[u]$, $f(0) \neq 0$, $g(0) \neq 0$. Sean

$$\begin{aligned}f(u) &= \alpha_0(a, a') + \alpha_1(a, a')u + \cdots + \alpha_n u^n \\ g(u) &= \beta_0(a, a') + \beta_1(a, a')u + \cdots + \beta_n u^n\end{aligned}$$

donde $\alpha_i, \beta_j \in K = \mathbb{R}(a, a')$. Consideremos la constante

$$\frac{F(u)}{G(u)} = \frac{f(u)}{g(u)} - \frac{\alpha_0(c,d)}{\beta_0(c,d)}$$

evaluando en $u = 0$

$$\frac{F(0)}{G(0)} = \frac{f(0)}{g(0)} - \frac{\alpha_0(a,a')}{\beta_0(a,a')} = 0$$

esto contradice el lema 3.20, luego la constante $\dfrac{f(u)}{g(u)} - \dfrac{\alpha_0(c,d)}{\beta_0(c,d)}$ debe ser igual a cero, entonces

$$\frac{f(u)}{g(u)} \in \mathbb{R}(c, d)$$

y obtenemos el corolario. □

Observación 3.22. *De la misma manera, para la constante*

$$4c^2 + d^2 + 1 \in C_{K\langle u\rangle},$$

evaluando en $u = 0$ obtenemos que $4a^2 + a'^2 + 1 = 0$. De este modo, las constantes c y d verifican la relación

$$4c^2 + d^2 + 1 = 0,$$

que no se verifica en un cuerpo ordenado, como $C_K = \mathbb{R}$.

Veremos ahora un ejemplo donde no hay la unicidad de una extensión Picard-Vessiot salvo $K-$isomorfismo diferencial.

Ejemplo 3.23. Sean $L_1 = \mathbb{R}\langle \operatorname{sen} x, \cos x\rangle$ y $L_2 = \mathbb{R}\langle i \operatorname{sen} x, i\cos x\rangle$ equipadas de la derivación usual sobre el anillo de funciones analíticas. Sea el operador diferencial $\mathcal{L}(Y) = Y + Y''$, se verifica facilmente que $\{\operatorname{sen} x, \cos x\}$ y $\{i \operatorname{sen} x, i\cos x\}$ son sistemas fundamentales de soluciones de $\mathcal{L}(Y) = 0$. De forma similar al ejemplo 3.18 se prueba que $C_{L_1} = C_{L_2} = \mathbb{R}$, así L_1 y L_2 son extensiones de Picard-Vessiot de $\mathbb{R}$ para $\mathcal{L}$. Supongamos que existe un $\mathbb{R}-$isomorfismo diferencial $\sigma : L_1 \to L_2$, entonces $\sigma(\operatorname{sen} x)$ es una solución de $\mathcal{L}(Y) = 0$, luego es combinación lineal de $\{i \operatorname{sen} x, i\cos x\}$ sobre $\mathbb{R}$:

$$\sigma(\operatorname{sen} x) = ai \operatorname{sen} x + bi\cos x, \quad a, b \in \mathbb{R}$$

derivando

$$\sigma(\cos x) = ai\cos x - bi \operatorname{sen} x.$$

Como $\operatorname{sen} x^2 + \cos x^2 = 1$, aplicando σ tenemos:

$$\begin{aligned} 1 = \sigma(1) &= \sigma(\operatorname{sen} x)^2 + \sigma(\cos x)^2 \\ &= (ai \operatorname{sen} x + bi\cos x)^2 + (ai\cos x - bi \operatorname{sen} x)^2 \\ &= -(a^2 + b^2) \end{aligned}$$

Luego, no existen $\mathbb{R}-$isomorfismos diferenciales de L_1 en L_2.

3.2. Caracterización de extensiones de Picard-Vessiot

El teorema 3.17 muestra que, dado un cuerpo diferencial K con cuerpo de constantes C_K algebraicamente cerrado y un operador $\mathcal{L}$ sobre K, la extensión de Picard-Vessiot de K para $\mathcal{L}$ es única salvo $K-$isomorfismo diferencial.

Pero es posible que L también sea la extensión de Picard-Vessiot de K para otros operadores.

Ejemplo 3.24. Sea $K = \mathbb{C}(x)$ el cuerpo de funciones racionales sobre $\mathbb{C}$ y sea $L = \mathbb{C}(x, e^x)$. Tenemos $C_K = \mathbb{C} = C_L$ pues $L \subset \mathbb{C}((x))$. Sean $\mathcal{L}_1(Y) = Y' - Y$ y $\mathcal{L}_2(Y) = Y'' - \dfrac{x+1}{x}Y'$. Como $L = K\langle e^x\rangle$ y $\{e^x\}$ es un conjunto fundamental de soluciones de $\mathcal{L}_1 = 0$, entonces L es una extensión Picard-Vessiot de K para $\mathcal{L}_1$. Por otro lado tenemos que $L = K\langle (x-1)e^x\rangle$ y $\{1, (x-1)e^x\}$ es un conjunto fundamental de soluciones de $\mathcal{L}_2 = 0$, entonces L es también una extensión de Picard-Vessiot de K para $\mathcal{L}_2$.

Seria útil tener una caracterización de las extensiones Picard-Vessiot que no dependa explicitamente del operador $\mathcal{L}$. La siguiente definición nos brinda dicha caracterización:

Definición 3.25. Sea $K \subset L$ una extensión de cuerpos diferenciales donde C_K es algebraicamente cerrado. Diremos que $K \subset L$ es una **extensión de Picard-Vessiot** si se verifican:

a) Existe un C_K espacio vectorial de dimensión finita $V \subset L$ que genera diferencialmente L sobre K, es decir $L = K\langle V \rangle$.

b) Existe un grupo G de automorfismos diferenciales de L con

$$G(V) = \{\sigma(v) \colon \sigma \in G, v \in V\} \subset V$$

que verifica $L^G = K$.

c) $C_K = C_L$.

Esta definición es independiente del operador diferencial, pero por medio del wronskiano se puede asociar un operador de gran utilidad.

Observación 3.26. *La extensión en la definición 3.25 nos permite contruir un operador diferencial $\mathcal{L}$ para el cual tal extension verifica la definicion 3.2. Si $\{y_1, \ldots, y_n\}$ es una C_K-base de V, entonces L es una extensión Picard-Vessiot de K para*

$$\mathcal{L}(Y) = \frac{W(Y, y_1, \ldots, y_n)}{W(y_1, \ldots, y_n)}. \tag{3.2.1}$$

La siguiente proposición utiliza un corolario del capítulo 4, que es independiente del resto del capítulo 3.

Proposición 3.27. *Sea $\widetilde{\mathcal{L}}$ un operador diferencial lineal homogéneo sobre K con C_K algebraicamente cerrado. Entonces L es una extensión Picard-Vessiot de K para $\widetilde{\mathcal{L}}$ si y solo sí $K \subset L$ es una extensión de Picard-Vessiot.*

Prueba. Si L es una extensión de Picard-Vessiot de K para $\widetilde{\mathcal{L}}$, entonces $L = K\langle z_1, \ldots, z_m \rangle$ donde $\{z_1, \ldots, z_m\}$ es un conjunto fundamental de soluciones de $\widetilde{\mathcal{L}}(Y) = 0$. Sea V el espacio vectorial de soluciones de $\widetilde{\mathcal{L}}$ entonces $L = K\langle V \rangle$. Por proposición 2.26, la dimensión de V sobre C_K es m. Sea $G = G(L|K)$, por corolario 4.4 se tiene que $L^G = K$ y es fácil ver que $G(V) \subset V$.

Reciprocamente, sea $\{y_1, \ldots, y_n\}$ una base de V sobre C_K, por proposición 2.25 $w(y_1, \ldots, y_n) \neq 0$. Sea

$$\mathcal{L}(Y) = \frac{W(Y, y_1, \ldots, y_n)}{W(y_1, \ldots, y_n)} \in L\{Y\}.$$

Probaremos que $\mathcal{L}(Y) \in K\{Y\}$. Sea $\mathcal{L}(Y) = \sum_{i=0}^{n} b_i Y^{(i)}$, por el ejemplo 2.23

$$w(Y, y_1, \ldots, y_n) = \sum_{i=0}^{n} a_i Y^{(i)}$$

donde $a_i = (-1)^i \det(\ldots, \underline{y}^{(i-1)}, \underline{y}^{(i+1)}, \ldots)$ y $\underline{y} = (y_1, \ldots, y_n)$. En particular, notamos que $a_n = W(y_1, \ldots, y_n)$. Luego

$$\mathcal{L}(Y) = \sum_{i=0}^{n} b_i Y^{(i)}$$

donde $b_i = \dfrac{a_i}{a_n}$. Como V es $G-$estable, para cualquier $\sigma \in G$ tenemos que $\sigma(y_i) \in V$, $i = 1, \ldots, n$, entonces

$$\sigma(y_i) = \sum_{j=1}^{n} c_{ji} y_j, c_{ij} \in C_K.$$

Luego por la proposición 2.24,

$$\sigma(a_i) = a_i \det(c_{ij}).$$

Luego $\sigma(b_i) = \sigma(a_n)^{-1}\sigma(a_i) = [\det(c_{ij})a_n]^{-1}[\det(c_{ij})a_i] = a_n^{-1}a_i = b_i$, entonces $b_i \in L^G$. Como $L^G = K$, los coeficientes $b_i \in K$ y se obtiene $\mathcal{L} \in K\{Y\}$. □

Por la proposición 3.27 y del ejemplo 3.24 tenemos que $L = \mathbb{C}(x, e^x)$ es una extensión de Picard-Vessiot de $K = \mathbb{C}(x)$. Usando la fórmula 3.2.1 podemos calcular el operador $\mathcal{L}$ del cual L es una extensión de Picard-Vessiot para K.

Para el conjunto fundamental de soluciones $\{e^x\}$:

$$\mathcal{L}_1(Y) = \frac{W(Y, e^x)}{W(e^x)} = \frac{\begin{vmatrix} Y & e^x \\ Y' & e^x \end{vmatrix}}{e^x} = \frac{Ye^x - Y'e^x}{e^x} = Y - Y'.$$

Para el conjunto fundamental de soluciones $\{1, (x-1)e^x\}$:

$$\mathcal{L}_2(Y) = \frac{W(Y, 1, (x-1)e^x)}{W(1, (x-1)e^x)} = \frac{\begin{vmatrix} Y & 1 & (x-1)e^x \\ Y' & 0 & xe^x \\ Y'' & 0 & (x+1)e^x \end{vmatrix}}{e^x} = -\frac{x+1}{x}Y' + Y''.$$

Como vemos, es posible que una extensión satisfaga la definición 3.25 para distintos subespacios V, es por eso que en el ejemplo 3.24 se tiene que L es una extensión de Picard-Vessiot de K para operadores distintos $\mathcal{L}_1$ y $\mathcal{L}_2$ que además tienen distinto grado.

En el ejemplo 3.5 también podría darse la posibilidad de que la extensión de Picard-Vessiot L fuese algebraica sobre K. En general, si una etensión de Picard-Vessiot $K \subset L$ es finita algebraica, donde C_K es algebraicamente cerrado, entonces por el corolario 4.4 existe un grupo G con $L^G = K$, así L debe ser necesariamente una extensión de Galois de K. Reciprocamente, mostraremos eque toda extensión de Galois finita $K \subset L$ es una extensión de Picard-Vessiot (donde L es un cuerpo diferencial usando la derivación única de L que se extiende de K establecida en la proposición 2.17).

3.2.1. Extensión de Galois finita

Veremos que una extensión de Galois finita es un ejemplo de la extensión de Picard-Vessiot. La parte más complicada es probar que una extensión algebraica no agrega nuevas constantes, lo que probará el siguiente lema:

Lema 3.28. *Sea $K \subset L$ una extensión diferencial de cuerpos y sean $x_1, \ldots, x_n \in L$ constantes algebraicamente dependientes sobre K, entonces son algebraicamente dependientes sobre C_K. En particular, si C_K es algebraicamente cerrado y L es algebraico sobre K entonces $C_L \subset C_K$.*

Prueba. Como $x_1, \ldots, , x_n$ son algebraicamente dependientes sobre K, entonces existe $f \in K[X_1, \ldots, X_n]$, $f \neq 0$ con $f(x_1, \ldots, x_n) = 0$.

Sea $\beta = \{u_s\}$ una base de K sobre C_K. Entonces β es una base libre del anillo de polinomios $K[X_1, \ldots, X_n]$ como $C_K[X_1, \ldots, X_n]-$módulo. Luego existen $h_1, \ldots, h_m \in C_K[X_1, \ldots, X_n]$ tales que $f = \sum_{s=1}^{m} h_s u_s$.

Como β es una base, el subconjunto $\{u_1, \ldots, u_m\}$ es C_K-linealmente independiente, entonces por la proposición 2.25 su wronskiano es diferente de cero.

Como los $u_i \in K \subset L$, nuevamente por la proposición 2.25 tenemos que el conjunto $\{u_1, \ldots, u_m\}$ es C_L- linealmente independiente.

Luego, como

$$\sum_{s=1}^{m} h_s(x_1, \ldots, x_n) u_s = f(x_1, \ldots, x_n) = 0$$

y $h_s(x_1, \ldots, x_n) \in C_L$ entonces $h_s(x_1, \ldots, x_n) = 0$ para todo $s \in \{1, \ldots, m\}$. Como $f \neq 0$ entonces $h_{s_0} \neq 0$ para algún $s_0 \in \{1, \ldots, m\}$, así $h_{s_0}(x_1, \ldots, x_n) = 0$ es la relación de dependencia lineal sobre C_K buscada.

En particular, si C_K es algebraicamente cerrado y L es algebraico sobre K veremos que $C_L \subset C_K$.

Sea $\alpha \in C_L$, como la extensión $L|K$ es algebraica, entonces existe $p(X) \in K[X]$ tal que $p(\alpha) = 0$. Sea $p(X) = a_0 + a_1X + \cdots + a_nX^n$ entonces

$$p(\alpha) = a_0(1) + a_1(\alpha) + \cdots + a_n(\alpha^n) = 0.$$

Como $\alpha' = 0$ entonces $(\alpha^r)' = 0$ para todo $r \in \{1, \ldots, n\}$. Luego los elementos $1, \alpha, \alpha^2, \ldots, \alpha^n \in L$ son constantes algebraicamente dependientes sobre K, y por lo probado anteriormente, son algebraicamente dependientes sobre C_K. Así, existen $\beta_0, \beta_1, \ldots, \beta_n \in C_K$ tales que

$$\beta_0 + \beta_1\alpha + \cdots + \beta_n\alpha^n = 0.$$

Luego el polinomio $q(X) = \beta_0 + \beta_1X + \cdots + \beta_nX^n \in C_K[X]$ tiene como raíz a α. Como C_K es algebraicamente cerrado: $\alpha \in C_K$. □

Proposición 3.29. *Sea K un cuerpo diferencial con C_K algebraicamente cerrado y sea $K \subset L$ una extensión de Galois finita, entonces $K \subset L$ es una extensión de Picard-Vessiot.*

Prueba. Sea G el grupo de Galois de la extensión $K \subset L$. Como la extensión $K \subset L$ es de Galois, entonces es separable, luego por la proposición 2.17 podemos extender la derivación de K a L y además todo elemento de G es un K-automorfismo diferencial.

Sea $p(X) \in K[X]$ un polinomio cuyo cuerpo de descomposición es L, sea $X = \{a_1, \ldots, a_n\}$ el conjunto formado por las raíces de p, y V el C_K-espacio vectorial generado por X. Como G permuta el conjunto finito X, entonces V es $G-$estable. También, como $L = K\langle a_1, \ldots, y_n\rangle$ (L es generado sobre K como cuerpo diferencial por X) entonces $L = K\langle V\rangle$. Como $K \subset L$ es una extensión de Galois, $L^G = K$. Por último, por el lema anterior $C_K = C_L$. Así $K \subset L$ es una extensión de Picard-Vessiot. □

En esta proposición podemos incluso saber cuál es el operador $\mathcal{L}$ del cual L es una extensión de Picard Vessiot para K: escogemos una C_K-base $x_1, \ldots, x_n$ de V entonces

$$\mathcal{L}(Y) = W(x_1, \ldots, x_n)^{-1} W(Y, x_1, \ldots, x_n).$$

Si las raíces de $p(X) = 0$ son C_K- linealmente independientes, estas mismas forman una base de V.

Ejemplo 3.30. Sea K un cuerpo diferencial con C_K algebraicamente cerrado y sea $a \in K$. Sea $p(X) = X^n - a \in K[X]$ y sea L el cuerpo de descomposición de $p(X)$. Entonces por la proposición anterior, L es una extensión de Picard-Vessiot. Sea z una raíz de p y sea $\xi \in C_K$ una raíz primitiva $n-$ésima de la unidad. Entonces el conjunto X de raíces de $p(X) = 0$ en L es

$$X = \left\{ \xi^i z : 0 \leq i \leq n-1 \right\}$$

y el C_K-espacio vectorial V generado por X tiene base $\{z\}$, entonces el operador correspondiente es $\mathcal{L}(Y) = W(z)^{-1} W(Y, z) = \dfrac{z'}{z} Y - Y'$.

Capítulo 4

Teorema fundamental de la teoría de Picard-Vessiot

En este capítulo definiremos el grupo de Galois diferencial de una extensión diferencial de cuerpos $K \subset L$, y probaremos que cuando la extensión es de Picard-Vessiot, su grupo de Galois diferencial posee la estructura de un grupo algebraico sobre C_K. Luego, podremos establecer el teorema fundamental de la teoría de Galois diferencial, que nos brinda una correspondencia biyectiva entre los cuerpos diferenciales intermedios de una extensión de Picard-Vessiot y los subgrupos cerrados de su grupo de Galois diferencial.

4.1. Grupo de Galois diferencial

Ahora veremos una proposición que será usada más adelante para obtener una parte del teorema fundamental de la teoria Picard-Vessiot.

Definición 4.1. Si $K \subset L$ es una extensión diferencial de cuerpos, el grupo

$$\begin{aligned} G(L|K) &= \{\sigma : L \to L : \sigma \text{ es } K - \text{automorfismo diferencial}\} \\ &= \left\{\sigma : L \to L : \sigma \text{ es isomorfismo diferencial con } \sigma_{|_K} = id_K\right\} \end{aligned}$$

es llamado grupo de Galois diferencial de la extensión $K \subset L$.

Cuando $K \subset L$ es una extensión de Picard-Vessiot para una ecuación $\mathcal{L}(Y) = 0$, el grupo $G(L|K)$ es también llamado grupo de Galois de $\mathcal{L}(Y) = 0$ sobre K. Usaremos la notación $Gal_K(\mathcal{L})$ o bien $Gal(\mathcal{L})$ si está claro cuál es el cuerpo base.

Ejemplo 4.2. Consideremos $K \subset L$, una extensión algebraica separable. Por la proposición 2.17 todo $K-$automorfismo de L es un $K-$automorfismo diferencial, luego el grupo de Galois y el grupo de Galois diferencial de la extensión coinciden.

Queremos ver que si $K \subset L$ es una extensión de Picard-Vessiot, entonces el subcuerpo de L fijado por la acción de $G(L|K)$ es igual a K. Obtendrenos esto con la ayuda de un corolario de la siguiente proposición.

Proposición 4.3. .

a) Si $K \subset L$ es una extensión de Picard - Vessiot para $\mathcal{L}(Y) = 0$ y $x \in L \backslash K$, entonces existe un $K-$automorfismo diferencial σ de L tal que $\sigma(x) \neq x$.

b) Sean $K \subset L \subset M$ extensiones de cuerpos diferenciales donde $K \subset L$ y $K \subset M$ son extensiones de Picard - Vessiot, entonces cualquier K-automorfismo diferencial de L puede ser extendido a un K-automorfismo diferencial de M.

Prueba.

a) Podemos asumir que L es el cuerpo de fracciones de R/P, donde R es el álgebra universal de soluciones para $\mathcal{L}$ y P es un ideal diferencial maximal de R. Sea $x \in L, x = \dfrac{a}{b}$ con $a, b \in R/P, b \neq 0$. Entonces $x \in A := (R/P)\,[b^{-1}] = \{a/b^n : a \in R/P, n \in \mathbb{N}\}$. Consideremos la K-álgebra diferencial

$$T = A \otimes_K A \subset L \otimes_K L.$$

Denotemos por $z = x \otimes 1 - 1 \otimes x \in T$, con $x = \frac{a}{b}$ elegido anteriormente; asi, como $x \notin K$, tenemos $z \neq 0$ y $z' \neq 0$ (pues si $z' = 0$, $z \in K$) y z no es nilpotente (pues si $z^n = 0$ para algún $n \in \mathbb{N}$, entonces $nz^{n-1}z' = (z^n)' = 0$, lo cual no es posible pues K tiene característica cero). De este modo, no solo podemos localizar T bajo el conjunto multiplicativo de las potencias de z (denotado por $T[z^{-1}]$) sino también podemos pasar al cociente $T[z^{-1}]/Q$, donde Q es un ideal diferencial maximal de $T\,[z^{-1}]$. Como $z \in T[z^{-1}]$ es inversible, entonces su imagen en el cociente $\overline{z} \neq 0$. Consecuentemente, tenemos

$$\begin{aligned} \tau_1 : A &\longrightarrow T[z^{-1}]/Q; & \tau_2 : A &\longrightarrow T[z^{-1}]/Q; \\ w &\longmapsto w \otimes 1 + Q. & w &\longmapsto 1 \otimes w + Q. \end{aligned}$$

Como P es maximal, el cociente R/P es un cuerpo y por eso no tiene ideales propios, y en consecuencia tampoco los tiene su localización $(R/P)[b^{-1}] = A$. Luego τ_1 y τ_2 son inyectivas, es decir cada $\mathrm{Ker}(\tau_i)$ debe ser cero, así ambas se extienden a K-mapeos diferenciales de $L \longrightarrow E = \mathrm{Frac}(T[z^{-1}]/Q)$. Por la proposicion 3.8, obtenemos $C_E = C_K$ y así $\tau_1(L) = \tau_2(L)$. Por otro lado, un calculo directo nos muestra que

$$\begin{aligned}\tau_1(x) - \tau_2(x) &= (x \otimes 1 + Q) - (1 \otimes x + Q);\\ &= (x \otimes 1 - 1 \otimes x) + Q = z + Q \neq 0.\end{aligned}$$

Así $\tau = \tau_1^{-1}\tau_2$ es un $K-$automorfismo diferencial de L con $\tau(x) \neq x$.

b) Como $K \subset L$ es una extensión de Picard Vessiot, podemos asumir la construcción dada en el teorema 3.9; es decir, $L = \mathrm{Frac}(R/P)$, donde $R = K[Y_{ij}][W^{-1}]$ y P es un ideal diferencial maximal de R. Con la extensión de Picard Vessiot $K \subset M$, asumida en la hipótesis, es fácil verificar que $L \subset M$ es también una extensión de Picard Vessiot para el mismo operador diferencial $\mathcal{L}$ que $K \subset M$, que a su vez puede ser visto como un operador definido sobre L. Así, podemos asumir nuevamente la construcción dada en el teorema 3.9, es decir M es el cuerpo de fracciones del cociente de $R_1 = L[Y_{ij}][W^{-1}]$ por un ideal diferencial maximal de dicha $L-$álgebra. Se puede verificar que $P_1 = L \otimes_K P$ es un ideal diferencial maximal de R_1, luego $M = \mathrm{Frac}(R_1/P_1)$. Sea $\sigma : L \to L$ un $K-$automorfismo diferencial, como

$$R_1 = L[Y_{ij}][W^{-1}] = L \otimes_K K[Y_{ij}][W^{-1}] = L \otimes_K R$$

definimos

$$\begin{aligned}\sigma \otimes id_R : L \otimes_K R &\to L \otimes_K R,\\ x \otimes y &\mapsto \sigma(x) \otimes y.\end{aligned}$$

Esta aplicación induce

$$\begin{aligned}\overline{\sigma \otimes id_R} : \frac{L \otimes_K R}{P_1} &\to \frac{L \otimes_K R}{P_1},\\ \overline{x \otimes y} &\mapsto \overline{\sigma(x) \otimes y},\end{aligned}$$

que es inyectiva, entonces podemos extenderla a su cuerpo de fracciones M.

Por lo tanto, se cumple la proposición. □

Dado un cuerpo diferencial L y un grupo G de automorfismos diferenciales de L, es fácil ver que el conjunto $L^G = \{x \in L : \sigma(x) = x \ \forall \sigma \in G\}$ es un subcuerpo diferencial de L.

Corolario 4.4. *Sea $K \subset L$ es una extensión de Picard-Vessiot y sea G el grupo de K-automorfismos diferenciales de L, entonces $L^G = K$.*

Prueba. La inclusión $K \subset L^G$ es clara, y la inclusión $L^G \subset K$ esta dada por la parte (a) en la proposición 4.3 . □

Teorema 4.5. *Sea K un cuerpo diferencial y $\mathcal{L}(Y) = 0$ una ecuación diferencial lineal homogénea de orden n definida sobre K. Entonces, el grupo de Galois diferencial de $\mathcal{L}(Y) = 0$ es isomorfo a un subgrupo del grupo lineal general* $\mathrm{GL}(n, C_K)$*, salvo conjugación.*

Prueba. Si $\{y_1, \ldots, y_n\}$ es un conjunto fundamental de soluciones de $\mathcal{L}(Y) = 0$, cualquier otra solución es una combinación lineal de estos elementos sobre C_K, luego para todo $\sigma \in Gal(\mathcal{L})$ y para cada $j \in \{1, \ldots, n\}$ tendremos que $\sigma(y_j)$ es también una solución de $\mathcal{L}(Y) = 0$, así:

$$\sigma(y_j) = \sum_{i=1}^{n} c_{ij} y_i,$$

donde $c_{ij} \in C_K$. Por lo tanto, a cada $\sigma \in Gal(\mathcal{L})$ le podemos asociar la matriz $(c_{ij}) \in GL(n, C_K)$ (la matriz (c_{ij}) es inversible pues $W(y_1, \ldots, y_n) \neq 0$). Es más, como $L = K\langle y_1, \ldots, y_n \rangle$, un K-automorfismo de L es determinado por las imágenes de los y_j. Entonces obtenemos un morfismo inyectivo

$$\begin{aligned} Gal(\mathcal{L}) &\longrightarrow \mathrm{GL}(n, C_K), \\ \sigma &\longmapsto (c_{ij}). \end{aligned} \tag{4.1.1}$$

Si $\{z_1, \ldots, z_n\}$ es otro conjunto fundamental de soluciones de $\mathcal{L}$,

$$\sigma(z_j) = \sum_{i=1}^{n} a_{ij} z_i, \quad \text{donde} \quad a_{ij} \in C_K.$$

Luego las matrices $C = (c_{ij})$ y $A = (a_{ij})$ satisfacen

$$C = P^{-1} A P$$

donde P es la matriz de cambio de base entre ambos conjuntos fundamentales:

$$\text{si} \quad y_j = \sum_{i=1}^{n} \lambda_{ij} z_i, \quad \text{entonces} \quad P = (\lambda_{ij}).$$

Consecuentemente, podemos identificar el grupo $Gal(\mathcal{L})$ con un subgrupo de $\mathrm{GL}(n, C_K)$, que está unicamente determinado, salvo conjugación. □

Veremos en la proposición 4.12 que $Gal(\mathcal{L})$ es cerrado en $\mathrm{GL}(n, C_K)$ con respecto a la topología de Zariski.

Ahora veremos la continuación de algunos ejemplos previos de extensiones de Picard-Vessiot y calcularemos su grupo de Galois diferencial.

4.1.1. Ejemplos de grupos de Galois diferenciales

Ejemplo 4.6. Recordemos el ejemplo 3.4 sobre adjunción de una integral. Teniamos que $L = K\langle\alpha\rangle$ es una extensión de Picard Vessiot de K para $\mathcal{L}(Y) = Y'' - \frac{a'}{a}Y'$ donde $\alpha' = a \in K$ no es una derivada en K. Calcularemos su grupo de Galois diferencial. Para esto, recordemos que $\{1, \alpha\}$ es un conjunto fundamental de soluciones de $\mathcal{L}$, entonces

$$Gal_K(\mathcal{L}) = \left\{\sigma : K\langle 1, \alpha\rangle \to K\langle 1, \alpha\rangle : \sigma \text{ es isomorfismo diferencial con } \sigma_{|_K} = id_K\right\}$$

Como $\sigma(1)$ y $\sigma(\alpha)$ son soluciones de $\mathcal{L} = 0$, existen c_{ij}, $i, j = 1, 2$ tales que

$$\sigma(1) = c_{11} + c_{21}\alpha.$$
$$\sigma(\alpha) = c_{12} + c_{22}\alpha.$$

Como σ es un automorfismo diferencial:

- $\sigma(1) = 1$ entonces $c_{11} + c_{21}\alpha = 1$ luego tenemos $(c_{11} - 1) + c_{21}\alpha = 0$ y como $\{1, \alpha\}$ es un conjunto C_K-linealmente independiente: $c_{11} = 1$ y $c_{21} = 0$.

- $\sigma(\alpha)' = \sigma(\alpha')$ entonces

  $$c_{22}a = c_{22}\alpha' = \sigma(\alpha)' = \sigma(\alpha') = \sigma(a) = id_K(a) = a$$

  luego $c_{22} = 1$. Así, todo $\sigma \in Gal_K(\mathcal{L})$ verifica que $\sigma(\alpha) = \alpha + c$, entonces le podemos hacer corresponder la matriz (c_{ij}), luego

$$Gal_K(\mathcal{L}) \simeq \left\{ \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} : c \in C_K \right\} \simeq (C_K, +) \subset GL(2, C_K).$$

Ejemplo 4.7. Recordemos el ejemplo 3.5 sobre adjunción de una exponencial de una integral. Teniamos que $L = K\langle\alpha\rangle$ es una extensión de Picard Vessiot de K para $\mathcal{L}(Y) = Y' - aY$ donde $\dfrac{\alpha'}{\alpha} = a \in K\backslash\{0\}$. Calcularemos su grupo de Galois diferencial. Para esto, recordemos que $\{\alpha\}$ es un conjunto fundamental de soluciones de $\mathcal{L}$, entonces

$$Gal_K(\mathcal{L}) = \left\{\sigma : K\langle\alpha\rangle \to K\langle\alpha\rangle : \sigma \text{ es isomorfismo diferencial con } \sigma_{|_K} = id_K\right\}.$$

Sea $\sigma \in Gal_K(\mathcal{L})$, entonces

$$\sigma(\alpha)' = \sigma(\alpha') = \sigma(a\alpha) = \sigma(a)\sigma(\alpha) = a\sigma(\alpha)$$

luego

$$\left(\frac{\sigma(\alpha)}{\alpha}\right)' = \frac{\alpha\sigma(\alpha)' - \alpha'\sigma(\alpha)}{\alpha^2} = \frac{\alpha a\sigma(\alpha) - a\alpha\sigma(\alpha)}{\alpha^2} = 0$$

así $\sigma(\alpha) = c\alpha$ para algún $c \in C_L = C_K$.
Como vimos en el ejemplo 3.5, la extension L podía ser de dos formas:

- Si α es algebraico, entonces $\alpha^n \in K$ para algún n. Entonces

  $$\sigma(\alpha)^n = \sigma(\alpha^n) = id_K(\alpha^n).$$

  Luego $(c\alpha)^n = \alpha^n$ y $c^n = 1$ entonces c es una raíz enésima de la unidad y $Gal_K(\mathcal{L})$ es un grupo ciclico finito.

- Si α es trascendental sobre K podemos definir un $K-$automorfismo diferencial de L por $\alpha \mapsto c\alpha$, entonces $Gal_K(\mathcal{L}) \simeq (C_K^*, \cdot)$

Ahora veremos ejemplos sobre el cuerpo diferencial $K = \mathbb{C}(z)$ dotado de la derivación usual teniendo en cuenta que en el ejemplo 3.3 ya hemos probado que estas son extensiones de Picard-Vessiot.

Ejemplo 4.8. Consideremos el operador diferencial $\mathcal{L}(Y) = Y'' + Y = 0$. Notamos que $\mathcal{L}(\operatorname{sen} z) = 0$ y $\mathcal{L}(\cos z) = 0$. Sea $L = \mathbb{C}(z)\langle\operatorname{sen} z, \cos z\rangle = \mathbb{C}(z, \operatorname{sen} z, \cos z)$ entonces $C_K = C_L = \mathbb{C}$, así $K \subset L$ es una extensión de Picard Vessiot de $\mathbb{C}(z)$ para $\mathcal{L}$. Hallaremos su grupo de Galois diferencial

$$Gal_K(\mathcal{L}) = \{\sigma : L \to L : \sigma \text{ es } \mathbb{C}(z) - \text{automorfismo diferencial}\}$$

Como $\sigma(\operatorname{sen} z)$ y $\sigma(\cos z)$ son soluciones de $\mathcal{L} = 0$, existen $c_{ij} \in \mathbb{C}$, $i, j = 1, 2$ tales que

$$\sigma(\operatorname{sen} z) = c_{11} \operatorname{sen} z + c_{21} \cos z$$
$$\sigma(\cos z) = c_{12} \operatorname{sen} z + c_{22} \cos z$$

Como σ es un automorfismo diferencial

- $\sigma(\operatorname{sen} z)' = \sigma(\operatorname{sen} z')$ entonces

  $$c_{11} \cos z - c_{21} \operatorname{sen} z = c_{12} \operatorname{sen} z + c_{22} \cos z$$

  y como $\{\operatorname{sen} z, \cos z\}$ es un conjunto $\mathbb{C}-$linealmente independiente: $c_{11} = c_{22}$ y $c_{12} = -c_{21}$.

- $\sigma(\cos z)' = \sigma(\cos z')$ entonces

  $$c_{12} \cos z - c_{22} \operatorname{sen} z = -c_{11} \operatorname{sen} z - c_{21} \cos z$$

  luego: $c_{11} = c_{22}$ y $c_{12} = -c_{21}$.

Por otro lado, como $\operatorname{sen} z^2 + \cos z^2 = 1$, entonces $\sigma(\operatorname{sen} z)^2 + \sigma(\cos z)^2 = 1$. Resolviendo, $c_{11}^2 + c_{12}^2 = 1$, así

$$Gal_K(\mathcal{L}) \simeq \left\{ \begin{pmatrix} c_{11} & c_{12} \\ -c_{12} & c_{11} \end{pmatrix} : c_{11}, c_{12} \in \mathbb{C}, c_{11}^2 + c_{12}^2 = 0 \right\}$$

Ejemplo 4.9. Consideremos el operador diferencial $\mathcal{L}(Y) = Y^{(3)} - Y' = 0$. Notamos que $\mathcal{L}(1) = 0$, $\mathcal{L}(e^z) = 0$ y $\mathcal{L}(e^{-z}) = 0$ Sea $L = \mathbb{C}(z)\langle 1, e^z, e^{-z}\rangle = \mathbb{C}(z, e^z)$ entonces $C_K = C_L = \mathbb{C}$, así $K \subset L$ es una extensión de Picard Vessiot de $\mathbb{C}(z)$ para $\mathcal{L}$. Hallaremos su grupo de Galois diferencial. Como $\sigma(1)$, $\sigma(e^z)$ y $\sigma(e^{-z})$ son soluciones de $\mathcal{L} = 0$, existen $c_{ij} \in \mathbb{C}$, $i, j = 1, 2, 3$ tales que

$$\sigma(1) = c_{11} + c_{21}e^z + c_{31}e^{-z}$$
$$\sigma(e^z) = c_{12} + c_{22}e^z + c_{32}e^{-z}$$
$$\sigma(e^{-z}) = c_{12} + c_{22}e^z + c_{33}e^{-z}$$

Como σ es un automorfismo diferencial

- $\sigma(1) = 1$ entonces $c_{11} + c_{21}e^z + c_{31}e^{-z} = 1$ y como $\{1, e^z, e^{-z}\}$ es un conjunto $\mathbb{C}-$linealmente independiente: $c_{11} = 1$ y $c_{21} = c_{31} = 0$.

- $\sigma(e^z)' = \sigma(e^{z\prime})$ entonces

$$c_{23}e^z - c_{33}e^{-z} = -c_{13} - c_{23}e^z - c_{33}e^{-z}$$

luego: $c_{13} = c_{23} = 0$ y $c_{12} = -c_{21}$.

Por otro lado, como $e^z.e^{-z} = 1$, entonces $\sigma(e^z).\sigma(e^{-z}) = 1$. Resolviendo, $c_{22}c_{33} = 1$, así

$$Gal_K(\mathcal{L}) \simeq \left\{ \begin{pmatrix} 1 & 0 & 0 \\ 0 & c_{22} & 0 \\ 0 & 0 & \frac{1}{c_{22}} \end{pmatrix} : c_{22} \in \mathbb{C}^* \right\} \simeq (\mathbb{C}^*, \cdot)$$

Ejemplo 4.10. Consideremos el operador diferencial $\mathcal{L}(Y) = Y' - \dfrac{1}{nz}Y = 0$ cuyos coeficientes son analíticos en un conjunto abierto simplemente conexo $U \subset \mathbb{C}\setminus\{0\}$, por ejemplo podemos considerar la región $U = \{z \in \mathbb{C} : |z+1| < 1\}$. Notamos que $\mathcal{L}(\sqrt[n]{z}) = 0$. Sean $K = \mathbb{C}(z)$ y $L = \mathbb{C}(z)\langle \sqrt[n]{z} \rangle = \mathbb{C}(\sqrt[n]{z})$ entonces $C_K = C_L = \mathbb{C}$, así $K \subset L$ es una extensión de Picard Vessiot de $\mathbb{C}(z)$ para $\mathcal{L}$. Hallaremos su grupo de Galois diferencial. Como $\sigma(\sqrt[n]{z})$ es una solución de $\mathcal{L} = 0$, existe $c \in \mathbb{C}$ tal que $\sigma(\sqrt[n]{z}) = c\sqrt[n]{z}$. Como σ es un automorfismo diferencial

- $\sigma(\sqrt[n]{z})' = \sigma((\sqrt[n]{z})')$ entonces

$$\frac{c}{nz}\sqrt[n]{z} = \sigma(\sqrt[n]{z})' = \sigma((\sqrt[n]{z})') = \sigma\left(\frac{1}{nz}\sqrt[n]{z}\right) = \frac{c}{nz}\sqrt[n]{z}$$

por lo tanto c es libre, es decir, todos los valores de c son admisibles para que σ sea un $\mathbb{C}(z)-$automorfismo diferencial.

Por otro lado, como $(\sqrt[n]{z})^n - z = 0$, entonces $\sigma(\sqrt[n]{z})^n - \sigma(z) = 0$. Resolviendo, $(c\sqrt[n]{z})^n - z = 0$,luego $c^n = 1$ es decir c es una raíz enésima de la unidad $c = e^{2\pi i\frac{m}{n}}$ donde $m = 0, \ldots, n-1$. Así $Gal_K(\mathcal{L})$ es un grupo ciclico finito de orden n

$$Gal_K(\mathcal{L}) \simeq \left\{1, e^{2\pi i\frac{1}{n}}, e^{2\pi i\frac{2}{n}}, \ldots, e^{2\pi i\frac{n-1}{n}} : c_{11}, c_{12} \in \mathbb{C}, c_{11}^2 + c_{12}^2 = 0\right\}$$

Ejemplo 4.11. Consideremos el operador diferencial $\mathcal{L}(Y) = Y'' - (1+z^2)Y = 0$. Notamos que $\mathcal{L}(e^{\frac{1}{2}z^2}) = 0$ y $\mathcal{L}(f(z)e^{\frac{1}{2}z^2}) = 0$ donde $f(z) = \int_0^z e^{-w^2}dw$ está definida sobre $\mathbb{C}$. Sea $L = \mathbb{C}(z)\left\langle e^{\frac{1}{2}z^2}, f(z)e^{\frac{1}{2}z^2}\right\rangle = \mathbb{C}(e^{\frac{1}{2}z^2}, f(z)e^{\frac{1}{2}z^2})$ entonces $C_K = C_L = \mathbb{C}$, así $K \subset L$ es una extensión de Picard Vessiot de $\mathbb{C}(z)$ para $\mathcal{L}$. Hallaremos su grupo de Galois diferencial. Como $\sigma(e^{\frac{1}{2}z^2})$ y $\sigma(f(z)e^{\frac{1}{2}z^2})$ son soluciones de $\mathcal{L} = 0$, existen $c_{ij} \in \mathbb{C}$, $i, j = 1, 2$ tales que

$$\sigma(e^{\frac{1}{2}z^2}) = c_{11}e^{\frac{1}{2}z^2} + c_{21}f(z)e^{\frac{1}{2}z^2}$$
$$\sigma(f(z)e^{\frac{1}{2}z^2}) = c_{12}e^{\frac{1}{2}z^2} + c_{22}f(z)e^{\frac{1}{2}z^2}$$

Como σ es un automorfismo diferencial

- $\sigma(e^{\frac{1}{2}z^2})' = \sigma(e^{\frac{1}{2}z^2\prime})$ entonces

$$c_{11}ze^{\frac{1}{2}z^2} + c_{21}zf(z)e^{\frac{1}{2}z^2} + c_{21}e^{\frac{1}{2}z^2}e^{-z^2} = c_{11}ze^{\frac{1}{2}z^2} + c_{21}zf(z)e^{\frac{1}{2}z^2}$$

  y como $\left\{e^{\frac{1}{2}z^2}, f(z)e^{\frac{1}{2}z^2}\right\}$ es un conjunto $\mathbb{C}-$linealmente independiente: $c_{21} = 0$ y $c_{11} \in \mathbb{C}^*$.

- $\sigma(f(z)e^{\frac{1}{2}z^2})' = \sigma((f(z)e^{\frac{1}{2}z^2})')$ entonces

$$c_{12}ze^{\frac{1}{2}z^2} + c_{22}zf(z)e^{\frac{1}{2}z^2} + c_{22}e^{\frac{1}{2}z^2}e^{-z^2} = c_{12}ze^{\frac{1}{2}z^2} + c_{22}zf(z)e^{\frac{1}{2}z^2} + \frac{1}{c_{11}}\frac{1}{e^{\frac{1}{2}z^2}}$$

  luego: $c_{22} = \frac{1}{c_{11}}$.

Entonces

$$Gal_K(\mathcal{L}) \simeq \left\{ \begin{pmatrix} c_{11} & c_{12} \\ 0 & \frac{1}{c_{11}} \end{pmatrix} : c_{11} \in \mathbb{C}^*, c_{12} \in \mathbb{C} \right\}.$$

4.2. El grupo de Galois diferencial como grupo algebraico lineal

Sea $K \subset L$ una extensión de Picard-Vessiot. Vimos luego del ejemplo 4.2, que el grupo de Galois diferencial $G(L|K)$ es isomorfo al subgrupo de $\mathrm{GL}(n, C_K)$ dado por la imagen del morfismo dado en (4.1.1). En el siguiente teorema, veremos que este subgrupo es un cerrado en la topología de Zariski.

Proposición 4.12. *Sea K un cuerpo diferencial y $L = K\langle y_1, ..., y_n\rangle$ una extensión de Picard-Vessiot de K. Entonces existe un conjunto S de polinomios $F(X_{ij}), 1 \leq i, j \leq n$ con coeficientes en C_K tal que:*

1. *Si $\sigma \in G(L|K)$ y $\sigma(y_j) = \sum_{i=1}^{n} c_{ij}y_i$, entonces $F(c_{ij}) = 0$ para todo $F \in S$.*
2. *Dada una matriz (c_{ij}) con $F(c_{ij}) = 0$ para todo $F \in S$, existe $\sigma \in G(L|K)$ tal que $\sigma(y_j) = \sum_{i=1}^{n} c_{ij}y_i$.*

Prueba. Sea $K\{Z_1, ..., Z_n\}$ el anillo de polinomios diferenciales en n indeterminados sobre K. Definimos el K-morfismo diferencial

$$\begin{aligned} \phi : K\{Z_1, ..., Z_n\} &\longrightarrow L, \\ Z_i &\longmapsto y_i. \end{aligned}$$

Como ϕ es sobreyectiva, por el primer teorema de isomorfismo

$$\frac{K\{Z_1, ..., Z_n\}}{\mathrm{Ker}(\phi)} \simeq L,$$

entonces $\mathrm{Ker}(\phi)$ es un ideal primo.

Sea $L[X_{ij}], 1 \leq i, j \leq n$ el anillo de polinomios en las indeterminadas X_{ij} con derivación definida por $X'_{ij} = 0$. Definimos un K- morfismo diferencial:

$$\begin{aligned} \varphi : K\{Z_1, ..., Z_n\} &\longrightarrow L[X_{ij}], \\ Z_j &\longmapsto \sum_{i=1}^{n} X_{ij} Y_i. \end{aligned}$$

Sea $\Delta = \varphi(\mathrm{Ker}(\phi))$ y sea $\{w_k\}$ una base del C_K - espacio vectorial L podemos escribir cada polinomio de Δ como combinación lineal de los w_K con coeficientes polinomiales en $C_K[X_{ij}]$. En efecto:

Dado $p(X_{ij}) \in \Delta$ entonces $p(X_{ij}) = \varphi(f(Z_1, ..., Z_n))$ donde $f(Z_1, ..., Z_n) \in \mathrm{Ker}(\varphi)$

Sea $f(Z_1, ..., Z_n) = \sum_{i_1,...,i_n=1}^{m} a_{i_1}, ..., a_{i_n} Z_1^{i_1} ... Z_n^{i_n}$ entonces

$$0 = \varphi(f) = \sum_{i_1,...,i_n=1}^{m} a_{i_1,...,i_n} \varphi(Z_i^{i_1}) ... \varphi(Z_n^{i_n}) \tag{4.2.1}$$

Observamos que: $\varphi(Z_i) = \sum_{j=1}^{n} X_{ij} Y_j$, entonces

$$\varphi(Z'_i) = [\varphi(Z_i)]' = \sum_{j=1}^{n} (X_{ij} Y_j)' = \sum_{j=1}^{n} (X_{ij} Y_j)' = \sum_{j=1}^{n} (X_{ij} Y'_j + X'_{ij} Y_j) = \sum_{j=1}^{n} X_{ij} Y'_j$$

cumpliendose lo analogo para las derivadas de mayor orden.

Continuando 4.2.7:

$$\begin{aligned} 0 = \varphi(f) &= \sum_{i_1,...,i_n=1}^{m} a_{i_1,...,i_n} \varphi(Z_1)^{(i_1)} \dots \varphi(Z_n)^{(i_n)} \\ &= \sum_{i_1,...,i_n=1}^{m} a_{i_1,...,i_n} \left(\sum_{j_1=1}^{n} X_{1j_1} Y_{j_1}^{(i_1)} \right) \dots \left(\sum_{j_1=1}^{n} X_{nj_n} Y_{j_n}^{(i_n)} \right) \\ &= \sum_{i_1,...,i_n=1}^{m} \left(\sum_{j_1,...,j_n=1}^{n} X_{1j_1} X_{2j_2} \dots X_{nj_n} a y_{j_1}^{(i_1)} \dots y_{j_n}^{(i_n)} \right) \end{aligned} \tag{4.2.2}$$

Como $\{w_k\}$ es base de L sobre C_K: $ay_{j_1}^{(1_i)}...ay_{j_n}^{(1_n)} = \sum_{k=1}^{r} \lambda_k w_k$ donde $\lambda_k \in C_K$

Continuando 4.2.2:

$$\begin{aligned}\varphi(f) &= \sum_{i_1,\ldots,i_n=1}^{m} \left(\sum_{j_1,\ldots,j_n=1}^{n} X_{1_{j_1}}...X_{n_{j_n}} \left(\sum_{k=1}^{r} \lambda_K w_K \right) \right) \\ &= \sum_{i_1,\ldots,i_n=1}^{m} \left(\sum_{j_1,\ldots,j_n=1 k=1}^{n,r} \lambda_K X_{1_{j_1}}...X_{n_{j_n}} \right) w_k\end{aligned}$$

Asi $P(X_{ij}) = \varphi(f) = \sum_{k=1}^{r} P_k(X_{ij}) w_k$ donde $P_k(X_{ij}) \in C_K[X_{ij}]$ para todo $p \in \Delta$

Definimos el conjunto:

$$S = \{P_k(X_{ij}) \in C_K[X_{ij}] : \varphi(f) = \sum_{k=1}^{r} P_k(X_{ij}) w_k, f \in \mathrm{Ker}(\phi)\}.$$

Probaremos ahora las dos partes de la proposición.

1. Sea $\sigma \in G(L\backslash K)$ tal que $\sigma(y_j) = \sum_{i=1}^{n} c_{ij} y_i$. Consideramos el diagrama:

$$\begin{array}{ccc} K\{Z_1 \ldots Z_n\} & \xrightarrow{\phi} & L \\ \varphi \downarrow & & \downarrow \sigma \\ L[X_{ij}] & \xrightarrow[\psi_{c_{ij}}]{} & L \end{array}$$

El diagrama es conmutativo:

$$(\sigma \circ \phi)(Z_i) = \sigma(y_i) = \sum_{j=1}^{n} c_{ij} y_j = \psi_{c_{ij}} \left(\sum_{j=1}^{n} X_{ij} y_j \right) = \psi_{c_{ij}}(\varphi(Z_i)) = \left(\psi_{c_{ij}} \circ \varphi\right)(Z_i)$$

Dado $f \in \mathrm{Ker}(\psi)$,

$$\left(\psi_{c_{ij}} \circ \varphi\right)(f) = (\sigma \circ \phi)(f) = \sigma(0) = 0.$$

Así

$$0 = \psi_{c_{ij}}(\varphi(f)) = \psi_{c_{ij}} \left(\sum_{k=1}^{r} P_k(X_{ij}) w_k \right) = \sum_{k=1}^{r} P_k(c_{ij}) w_k$$

donde $P_k(X_{ij}) \in C_K[X_{ij}]$. Luego $P_k(c_{ij}) \in C_K$, y como $\{w_k\}$ es base y por tanto un conjunto linealmente independiente: $P_k(c_{ij}) = 0 \, \forall k = 1, \ldots r$. Así todos los polinomios de S se anulan en c_{ij}.

2. Sea $(c_{ij}) \in GL(n, C_K)$ tal que $F(c_{ij}) = 0$ para todo $F \in S$. Definimos el morfismo diferencial:

$$\begin{aligned}\tau = \psi_{c_{ij}} \circ \varphi : K\{Z_1, \ldots, Z_n\} &\to K\{y_1, \ldots, y_n\} \\ Z_j &\mapsto \sum_{i=1}^{n} c_{ij} y_i\end{aligned}$$

Afirmación: $\mathrm{Ker}(\phi) \subset \mathrm{Ker}(\tau)$.
Sea $P(Z_1, \ldots, Z_n) \in \mathrm{Ker}(\psi)$ entonces $\varphi(P) = \sum_{k=1}^{r} \alpha_k(X_{ij}) w_k$ con $\alpha_k(X_{ij}) \in S$.
Ahora

$$\tau(P) = \left(\psi_{c_{ij}} \circ \varphi\right)(P) = \psi_{c_{ij}} \left(\sum_{k=1}^{r} \alpha_k(X_{ij}) w_k \right) = \sum_{k=1}^{r} \alpha_k(c_{ij}) w_k$$

Pero $\alpha_k(c_{ij}) = 0$ por hipótesis, así $\tau(P) = 0$,

Definimos

$$\begin{aligned} \sigma : K\{y_1, \ldots, y_n\} &\to K\{y_1, \ldots, y_n\} \\ y_j &\mapsto \sum_{i=1}^{n} c_{ij} y_i \end{aligned}$$

Veamos que σ está bien definida: Si $y_i = y_j$ entonces $\phi(Z_i - Z_j) = \phi(Z_i) - \phi(Z_j) = 0$ y $Z_i - Z_j \in \mathrm{Ker}(\phi)$. Por la afirmacion antes probada, $Z_i - Z_j \in \mathrm{Ker}(\tau)$, luego

$$\sigma(y_i) = \sum_{h=1}^{n} c_{hi} y_h = \sigma(y_j)\tau(Z_i) = \tau(Z_j) = \sum_{h=1}^{n} c_{hj} y_h \tag{4.2.3}$$

Luego σ es un morfismo bien definido. Basta probar que σ es biyectivo.
Supongamos que existe algún $u \in \mathrm{Ker}(\sigma), u \neq 0$.
Afirmación: $u \notin \overline{K}$. En efecto, supongamos $u \in \overline{K}$.
Sea $p(X) = \mathrm{Irr}(u, K)(X) = a_0 + a_1 X + a_2 X^2 + \cdots + X^n$ entonces

$$\begin{aligned} 0 &= p(u) = a_0 + a_1 u + u^n \\ 0 &= \sigma\left(p(u)\right) = \sigma(a_0) + \sigma(a_1)\sigma(u) + \cdots + (\sigma(u))^n = \sigma(a_0) \\ 0 &= \sigma(a_0) \end{aligned}$$

así: $a_0 \in \mathrm{Ker}(\sigma)$. Como p es irreducible: $a_0 \neq 0$, luego $Ker(\sigma) = K\{y_1, \ldots, y_n\}$ entonces $\sigma \equiv 0$ y σ no seria un morfismo.
Así la afirmación está probada, es decir u es trascendente, entonces:

$$\mathrm{trdeg}\left[K\{y_1, \ldots, y_n\} : K\right] > \mathrm{trdeg}\left[K\{\sigma(y_1), \ldots, \sigma(y_n)\} : K\right]$$

Por otro lado:

$$\mathrm{trdeg}\left[K\{y_j, \sigma(y_j)\} : K\right] = \mathrm{trdeg}\left[K\{y_j, c_{ij}\} : K\right] = \mathrm{trdeg}\left[K\{y_j\} : K\right]$$

y analogamente obtenemos que

$$\operatorname{trdeg}\left[K\left\{y_j, \sigma(y_j)\right\} : K\right] = \operatorname{trdeg}\left[K\left\{\sigma(y_j)\right\} : K\right]$$

Como la matriz (c_{ij}) es invertible, la imagen contiene a $y_1, \ldots y_n$ entonces σ es sobreyectivo. Así, tenemos que σ es biyectivo y puede ser extendido a un automorfismo

$$\sigma : K\left\langle y_1, \ldots, y_n\right\rangle \to K\left\langle y_1, \ldots, y_n\right\rangle$$

Así la proposición queda probada. □

En conclusión tenemos que $G(L|K)$ es isomorfo un subgrupo de $\mathrm{GL}(n, C_K)$ que es cerrado en la topologia de Zariski, es decir, $G(L|K)$ es isomorfo a un grupo algebraico lineal.

Observación 4.13. Los subgrupos cerrados propios de $GL(1, C_K) \simeq C_K^*$ son finitos y por tanto son grupos cíclicos, entonces para una ecuación diferencial lineal homogénea de grado 1, los únicos grupos de Galois diferencial son C_K^* ó un grupo cíclico finito.

Ahora veremos de otra forma que el grupo de Galois diferencial de una extensión de Picard-Vessiot es un grupo algebraico.

Observación 4.14. *Primero veremos que* $\mathrm{GL}(n, C_K)$ *actúa sobre* R*, donde esta última es la* $K-$*álgebra construida en la definición 2.31. Consideremos el isomorfismo*

$$\varphi : K\left[Y_{ij}\right]\left[W^{-1}\right] \longrightarrow K \otimes_{C_K} C_K\left[\mathrm{GL}(n, C_K)\right]$$
$$aY_{ij} \longmapsto a \otimes X_{i+1,j}$$

donde $a \in K$*,* $0 \leq i \leq n-1$*,* $1 \leq j \leq n$ *y* $C_K\left[\mathrm{GL}(n, C_K)\right] = C_K\left[X_{11}, \ldots, X_{nn}, 1/det\right]$ *denota el anillo de coordenadas del grupo algebraico* $\mathrm{GL}(n, C_K)$*. Consideremos también la acción de* $\mathrm{GL}(n, C_K)$ *en si mismo por traslaciones a derecha:*

$$\mathrm{GL}(n, C_K) \times \mathrm{GL}(n, C_K) \longrightarrow \mathrm{GL}(n, C_K)$$
$$(g, h) \longmapsto hg^{-1}$$

y la acción correspondiente de $\mathrm{GL}(n, C_K)$ *sobre* $C_K\left[\mathrm{GL}(n, C_K)\right]$*:*

$$\mathrm{GL}(n, C_K) \times C_K\left[\mathrm{GL}(n, C_K)\right] \longrightarrow C_K\left[\mathrm{GL}(n, C_K)\right]$$
$$(g, f) \longmapsto \rho_g(f)$$

donde

$$\begin{aligned}\rho_g(f) : \mathrm{GL}(n, C_K) &\longrightarrow C_K \\ h &\longmapsto f(hg)\end{aligned}$$

Entonces tenemos:

$$(g, aY_{ij}) \longmapsto a\rho_g(Y_{ij})$$

$$\begin{array}{ccc} \mathrm{GL}(n, C_K) \times K[Y_{ij}][W^{-1}] & \longrightarrow & K[Y_{ij}][W^{-1}] \\ \downarrow{\scriptstyle id\times\varphi} & & \uparrow{\scriptstyle \varphi^{-1}} \\ \mathrm{GL}(n, C_K) \times K \otimes_{C_K} C_K\,[\mathrm{GL}(n, C_K)] & \longrightarrow & K \otimes_{C_K} C_K\,[\mathrm{GL}(n, C_K)] \end{array}$$

$$(g, a \otimes X_{i+1j}) \longmapsto a \otimes \rho_g(X_{i+1j})$$

Así podemos hacer actuar a $\mathrm{GL}(n, C_K)$ *sobre* R*, actuando sobre el segundo factor:*

$$\begin{aligned}\mathrm{GL}(n, C_K) \times R &\longrightarrow R \\ (g, aY_{ij}) &\longmapsto a\rho_g(Y_{ij})\end{aligned}$$

Ahora caracterizaremos los elementos de $G(L|K)$ *con ayuda de esta acción.*

En la obervación 2.32 vimos que $\{Y_{01}, \ldots, Y_{0n}\}$ *es un conjunto fundamental de soluciones de* $\mathcal{L} = 0$ *en* $K[Y_{ij}][W^{-1}]$ *donde* $\mathcal{L}$ *es el operador diferencial de la definición 2.31. Entonces, dado* $\sigma \in G(L|K)$ *le podemos asociar una matriz en* $\mathrm{GL}(n, C_K)$ *como vimos antes del ejemplo 4.6. En efecto, sea*

$$\sigma(Y_{0j}) = \sum_{k=1}^{n} c_{kj} Y_{0k}$$

derivando, y por la regla de derivación en R *tenemos*

$$\sigma(Y_{ij}) = \sum_{k=1}^{n} c_{kj} Y_{ik} \tag{4.2.4}$$

Así dado $\sigma \in G(L|K)$ *le asociamos la matriz* $g = (c_{ij}) \in \mathrm{GL}(n, C_K)$*. Luego* $G(L|K)$ *actúa sobre* R*, haciendo actuar a* $\mathrm{GL}(n, C_K)$ *sobre* R*:*

$$\begin{aligned}G(L|K) \times R &\longrightarrow R \\ (\sigma, aY_{ij}) &\longmapsto a\rho_g(Y_{ij})\end{aligned}$$

Dado $g \in \mathrm{GL}(n, C_K)$ *entonces podemos calcular la acción de* g *sobre la funcion* Y_{ij} *que lleva a una matriz de* $\mathrm{GL}(n, C_K)$ *a su entrada* $ij-$*ésima:*

$$\rho_g(Y_{ij})(h) = Y_{ij}(hg) = (hg)_{ij} = \sum_{k=1}^{n} h_{ik}c_{kj} = (\sum_{k=1}^{n} c_{kj}Y_{ik})(h)$$

Si P *es el ideal diferencial maximal de* R *considerado en el teorema 3.9, entonces los ideales* $\langle Y_{ij}\rangle$ *estan contenidos en* R*, luego todos los* Y_{ij} *pertenecen a* P*.*

Como P *es un ideal, entonces* $\sigma(Y_{ij}) = \rho_g(Y_{ij}) \in P$*. Luego como los elementos de* P *son generados por los* Y_{ij}*, tenemos que dado* $\sigma \in G(L|K)$ *se tiene que* $\sigma(P) = P$*, por tanto* $c(P) = P$ *donde* c *es la matriz asociada a* σ *mediante* (4.2.4)*.*

Reciprocamente, sea $c = (c_{ij}) \in \mathrm{GL}(n, C_K)$ *tal que* $c(P) = P$*. La acción de* $\mathrm{GL}(n, C_K)$ *sobre* R *induce una acción de* $\mathrm{GL}(n, C_K)$ *sobre* R/P*. En efecto, sean* y_{ij} *las imágenes de los elementos* Y_{ij} *en el cociente* R/P *entonces podemos calcular la acción de* c *sobre cualquier elemento de* R/P

$$c(ay_{ij}) = a\rho_c(y_{ij}) = a\sum_{k=1}^{n} c_{kj}y_{ik}, \;\; a \in K$$

Luego podemos definir $\sigma : R/P \to R/P$ *como*

$$\sigma(ay_{ij}) = a\sum_{k=1}^{n} c_{kj}y_{ik}$$

y como $c(P) = P$ *entonces* $\sigma(P) = P$ *luego podemos extender* σ *al cuerpo de fracciones* $\mathrm{Fracc}(R/P) = L$*. Por* (4.14) *tenemos que* $\sigma_{|_K} = id_K$*, así* $\sigma \in G(L|K)$ *donde* c *es su matriz asociada.*

Luego tenemos la caracterización:

$$G(L|K) = \{c \in \mathrm{GL}(n, C_K) : c(P) = P\}.$$

Sea $\{\psi_1, \ldots, \psi_m\}$ *un conjunto de generadores de* P*. Podemos asumir que los* $\psi_i \in K[Y_{ij}]$*. Sea* W_N *el* C_K-*espacio vectorial de polinomios de* $K[Y_{ij}]$ *de grado menor o igual a* N*. Dados* $\psi \in W_N$ *y* $c \in \mathrm{GL}(n, C_K)$ *es fácil verificar que* $\deg(c(\psi)) = \deg(\psi)$*, luego* W_N *es* $\mathrm{GL}(n, C_K)-$*estable. Si* N *es el máximo de los grados de los* ψ_i *entonces* $V_N = W_N \cap P$ *genera* P*.*

Podemos identificar $G(L|K)$ *con el grupo de automorfismos* $c \in \mathrm{GL}(n, C_K)$ *tales que* $c(V_N) \subset V_N$*. En efecto, si* $c \in G(L|K)$ *entonces*

$$c(V_N) = c(W_N \cap M) \subset c(W_N) \cap c(M) \subset W_N \cap M = V_N$$

Reciprocamente, si $c(V_N) \subset V_N$ *entonces*

$$c(M) = c(\langle V_N \rangle) = \langle c(V_N) \rangle \subset \langle V_N \rangle = M$$

Así

$$G(L|K) = \{c \in \mathrm{GL}(n, C_K) : c(V_N) \subset V_N\}. \tag{4.2.5}$$

Sea $\{f_1, \ldots, f_p\}$ *una base de* V_N *cobre* C_K*. Podemos extenderla a una base* $\{f_1, \ldots, f_p, \ldots f_q\}$ *de* W_N *sobre* C_K*. Como los* $f_i \in K[Y_{ij}]$ *y* W_N *es* $\mathrm{GL}(n, C_K)-$*estable entonces dado* $c \in \mathrm{GL}(n, C_K)$ *tenemos*

$$c(f_s(Y_{ij})) = f_s(c(Y_{ij})) = f_s\left(\sum_{k=1}^{n} Y_{ik}c_{kj}\right) = \sum_{r=1}^{q} \lambda_{rs}(c_{ij}) f_r(Y_{ij})$$

para todo $s = 1, \ldots, q$*, donde* $\lambda_{rs} \in C_K[\mathrm{GL}(n, C_K)]$*.*

Luego, por la caracterización dada en (4.2.5)*,* $c \in G(L|K)$ *sí y sólo si*

$$c(f_s(Y_{ij})) = \sum_{r=1}^{p} \lambda_{rs}(c_{ij}) f_r(Y_{ij})$$

para todo $s = 1, \ldots, p$*, esto es* $\lambda_{rs}(c_{ij}) = 0$ *para todo* $r = p+1, \ldots, q$ *y* $s = 1, \ldots, n$*. Entonces* $G(L|K)$ *es un subgrupo cerrado del gurpo algebraico* $\mathrm{GL}(n, C_K)$*.*

Probaremos la proposición 4.17, que será de utilidad en la demostración del teorema fundamental de la teoría de Picard-Vessiot. Usaremos dos lemas.

Para cualquier cuerpo F denotaremos por

$$F\left[Y_{ij}, 1/\det\right]$$

al anillo de polinomios en las indeterminadas Y_{ij}, $i, j = 1, \ldots, n$, localizado con respecto al determinante de la matriz (Y_{ij}). Además, si $\beta = \{v_s\}_{s \in S}$ una base de L sobre C_L tal que $1 \in \beta$, para cada ideal I en $B := C_L\left[Y_{ij}, 1/det\right]$,

$$IA = \left\{\sum_{s \in S} \lambda_s v_s : \lambda_s \in I\right\},$$

donde $A := L\left[Y_{ij}, 1/det\right]$.

Lema 4.15. *Sea* L *un cuerpo diferencial, consideremos* $A := L\left[Y_{ij}, 1/det\right]$ *y extendemos la derivación de* L *hacia* A *definiendo* $Y'_{ij} = 0$*. Consideramos* $B := C_L\left[Y_{ij}, 1/det\right]$ *como subanillo de* $L\left[Y_{ij}, 1/det\right]$*. Entonces la aplicación:*

$$\varphi : \{\textit{Ideales de } B\} \longrightarrow \{\textit{Ideales diferenciales de } A\}$$
$$I \longmapsto IA$$

es una biyección, y su inversa está dada por $\varphi^{-1}(J) = J \cap B$*.*

Prueba. Es claro, por la definición, que φ es inyectiva.

Para probar la sobreyectividad consideraremos a J como un ideal diferencial en A y veremos que

$$\varphi(I) = J, \quad \text{donde} \quad I = J \cap B, \tag{4.2.6}$$

con lo cual también se obtiene que su inversa está dada por $\varphi^{-1}(J) = J \cap B$.

Para demostar (4.2.6), consideramos inicialmente a $\beta = \{v_r\}_{r\in S_1}$ como una base de L sobre C_L tal que $1 \in \beta$, y así obtenemos que β es también una base libre de A como B-módulo. De este modo, cuando $b \in J$, tenemos que $b \in A$, luego b se puede escribir de forma única como

$$b = \sum_{r\in S_1} \alpha_r v_r$$

donde $\alpha_r \in B$ para todo $r \in S_1$. Por otro lado, cada $\alpha_r \in B$ se puede escribir de forma única como

$$\alpha_r = \sum_{s\in S_2} \lambda_{rs} u_s$$

donde $\lambda_{rs} \in C_K, \forall s \in S_2$ y $\{u_r\}_{r\in S_2}$ es una base de B sobre C_L. Entonces:

$$\begin{aligned} b &= \sum_{r\in S_1} \left(\sum_{s\in S_2} \lambda_{rs} u_s \right) v_r = \sum_{s\in S_2} \left(\sum_{r\in S_1} \lambda_{rs} v_r \right) u_s \\ &= \sum_{s\in S_2} \mu_s u_s \end{aligned} \tag{4.2.7}$$

donde $\mu_s \in L$. Por lo tanto, cualquier elemento de J puede ser esrito de forma única como en (4.2.7).

Afirmación. Cada elemento $b = \sum_{s\in S_2} \mu_s u_s \in J$ satisface $b \in IA$.

En efecto, sea $l(b)$ el número de subíndices $s \in S_2$ tales que $\mu_s \neq 0$. Procederemos por inducción sobre $l(b)$.

- Si $l(b) = 0$ entonces $b = 0 \in IA$.
- Si $l(b) = 1$ entonces $b = \mu_1 u_1$ donde $\mu_1 \in L$ y $u_1 \in B$.
  Como J es un ideal: $u_1 = \mu_1^{-1} b \in J$, luego $u_1 \in I$ y entonces $b \in IA$.
- Hipótesis Inductiva: si $1 < l(q) < l(b)$ entonces $q \in IA$. Sea $b = \sum_{s\in S_2} \mu_s u_s$ donde $\mu_s \in L$. Como L es un cuerpo podemos suponer que $\mu_{s_1} = 1$ para algún $s_1 \in S_2$. Si $\mu_s \in C_L$ para todo $s \in S_2$, entonces $\mu_s \in B$ luego $b \in B \cap J = I$.

Supongamos entonces que existe algun $s_2 \in S_2$ tal que $\mu_{s_2} \in L \backslash C_L$. Tenemos que: $b' = \sum_s (\mu'_s u_s + \mu_s u'_s)$. Notemos que como $u_s \in B = C_L\,[Y_{ij}, 1/det]$

$$u_s = \sum_{m,n} c_s Y_{ij}^{(n)} \left(\frac{1}{det}\right)^m, \;\; c_s \in C_L$$
$$u'_s = \sum \beta_s \left[c_s Y'_{ij} + c'_s Y_{ij}\right] = 0, \;\; \beta_s \in B$$

Luego $b' = \sum_s \mu'_s u_s$. Como $\mu_{s_1} = 1$ entonces $\mu'_{s_1} = 0$, luego $l(b') < l(b)$ y $b' \in IA$.

Por otra parte:

$$\begin{aligned}(\mu_{s_2}^{-1} b)' &= \sum_s \left[(\mu_{s_2}^{-1}\mu_s)' u_s + (\mu_{s_2}^{-1}\mu_s) u'_s\right] \\ &= \sum_{s \neq s_2} (\mu_{s_2}^{-1}\mu_s)' u_s\end{aligned}$$

Así $l((\mu_{s_2}^{-1} b)') < l(b)$ y $(\mu_{s_2}^{-1} b)' \in IA$.

Como $(\mu_{s_2}^{-1} b)' = (\mu_{s_2}^{-1})' b + \mu_{s_2}^{-1} b'$, entonces $(\mu_{s_2}^{-1})' b = (\mu_{s_2}^{-1} b)' - \mu_{s_2}^{-1} b' \in IA$.

Como $\mu_{s_2} \in L \backslash C_L$ entonces $\mu'_{s_2} \neq 0$, luego $(\mu_{s_2}^{-1})' = -\mu'_{s_2}(\mu_{s_2}^{-1})^2 \neq 0$ y así $b \in IA$.

Por lo tanto, se cumple la afirmación en la página 91 y se concluye la prueba. □

Lema 4.16. *Sea K un cuerpo diferencial con cuerpo de constantes C_K. Sea $K \subset L$ una extensión de Picard-Vessiot con grupo de Galois diferencial $G(L|K)$. Consideremos $A = L\,[Y_{ij}, 1/\mathrm{det}]$, $B = K\,[Y_{ij}, 1/\mathrm{det}]$. Entonces la aplicación*

$$\begin{aligned}\varphi : \{\textit{Ideales de } B\} &\longrightarrow \{\textit{Ideales } G(L|K)- \textit{ estables de } A\} \\ I &\longmapsto IA\end{aligned}$$

es una biyección y su inversa estáa dada por $\psi^{-1}(J) = J \cap B$.

Prueba. La prueba es silimar al lema anterior. Para la sobreyectividad, probaremos que cualquier ideal $G(L|K)-$ estable J de A esta generado por $J \cap B = I$.

Sea $\{u_s\}_{s \in S}$ una base de B sobre K.

Sea $b \in J$, entonces

$$b = \sum_{\text{finita}} \alpha_s Y_{ij}^{(k)} \left(\frac{1}{\det}\right)^{(n)}$$

donde $\alpha_s \in L$. Como $K \subset L$ es una extensión de Picard-Vessiot, entonces $L = K\langle y_1, \ldots, y_n \rangle$ donde $y_1, \ldots, y_n$ es un conjunto fundamental de soluciones de $\mathcal{L}(Y) = 0$ en L. Luego para cada α_s

$$\alpha_s = \sum_{\text{finita}} \gamma_i y_i^{(r)}$$

donde $\gamma_i \in K$. Así

$$b = \sum \left(\sum \gamma_i y_i^{(r)} \right) Y_{ij}^{(k)} \left(\frac{1}{\det} \right)^{(n)} = \sum \left(\sum \gamma_i Y_{ij}^{(k)} \left(\frac{1}{\det} \right)^{(n)} \right) y_i^{(r)}$$

Como $\{u_s\}_{s \in S}$ es base de B sobre K:

$$\sum \gamma_i Y_{ij}^{(k)} \left(\frac{1}{\det} \right)^{(n)} = \sum_{s \in S} \theta_s u_s$$

donde $\theta_s \in K$. Luego:

$$b = \sum \sum \theta_s u_s y_i^{(r)} = \sum \left(\theta_s y_i^{(r)} \right) u_s$$

Así, cualquier $b \in J$ puede ser escrito de forma única como

$$b = \sum_{s \in S} \mu_s u_s$$

donde $\mu_s \in L$.

Afirmación. Cada elemento $b = \sum_{s \in S} \mu_s u_s \in J$ satisface $b \in IA$.

En efecto, sea $l(b)$ el número de subíndices $s \in S$ tales que $\mu_s \neq 0$. Procederemos por inducción sobre $l(b)$.

- Si $l(b) = 0$ entonces $b = 0 \in IA$.
- Si $l(b) = 1$ entonces $b = \mu_1 u_1$ donde $\mu_1 \in L$ y $u_1 \in B$.
  Como J es un ideal: $u_1 = \mu_1^{-1} b \in J$, luego $u_1 \in I$ y entonces $b \in AI$.
- Hipótesis Inductiva: si $1 < l(q) < l(b)$ entonces $q \in IA$. Sea $b = \sum_{s \in S} \mu_s u_s$ donde $\mu_s \in L$. Como L es un cuerpo podemos suponer que $\mu_{s_1} = 1$ para algún $s_1 \in S$. Si $\mu_s \in K$ para todo $s \in S$, entonces $b \in B$ luego $b \in B \cap J = I$. Supongamos entonces que existe algun $s_2 \in S$ tal que $\mu_{s_2} \in L \backslash K$:

Sea $\sigma \in G = G(L|K)$:

$$\begin{aligned}\sigma(b) - b &= \sum_{s\in S} \sigma(\mu_s)\sigma(u_s) - \sum_{s\in S} \mu_s u_s \\ &= \sum_{s\neq s_1} \sigma(\mu_s)u_s + \sigma(\mu_{s_1})\mu_{s_1} - \sum_{s\neq s_1} \mu_s u_s - \mu_{s_1}u_{s_1} \\ &= \sum_{s\neq s_1} \left[\sigma(\mu_s) - \mu_s\right] u_s\end{aligned}$$

Entonces $l\left(\sigma(b) - b\right) < l(b)$, luego por la hipótesis inductiva: $\sigma(b) - b \in IA$. Por la proposición 4.3, como $\mu_{s_2} \in L\backslash K$, existe $\sigma_0 \in G$ tal que $\sigma_0(\mu_{s_2}) \neq \mu_{s_2}$, luego

$$\begin{aligned}\sigma_0(\mu_{s_2}^{-1}b) - \mu_{s_2}^{-1}b &= \sum_{s\in S} \left[\sigma_0(\mu_{s_2}^{-1}\mu_s) - \mu_{s_2}^{-1}\mu_s\right] u_s \\ &= \sum_{s\neq s_2} \left[\sigma_0(\mu_{s_2}^{-1}\mu_s) - \mu_{s_2}^{-1}\mu_s\right] + \left[\sigma_0(1) - 1\right] u_{s_2}\end{aligned}$$

así $l(\sigma_0(\mu_{s_2}^{-1}b) - \mu_{s_2}^{-1}b) < l(b)$, entonces $\sigma_0(\mu_{s_2}^{-1}b) - \mu_{s_2}^{-1}b \in IA$. Por otro lado:

$$\begin{aligned}(\sigma_0(\mu_{s_2}^{-1}) - \mu_{s_2}^{-1})b &= \sigma_0(\mu_{s_2}^{-1})b - \mu_{s_2}^{-1}b + \sigma_0(\mu_{s_2}^{-1}b) - \sigma_0(\mu_{s_2}^{-1}b) \\ &= \sigma_0(\mu_{s_2}^{-1}b) - \mu_{s_2}^{-1}b - \sigma_0(\mu_{s_2}^{-1})\left(\sigma_0(b) - b\right)\end{aligned}$$

Como $\sigma_0(\mu_{s_2}) \neq \mu_{s_2}$ entonces $\sigma_0(\mu_{s_2}^{-1}) - \mu_{s_2}^{-1} \neq 0$, luego

$$b = (\sigma_0(\mu_{s_2}^{-1}) - \mu_{s_2}^{-1})^{-1}(\sigma_0(\mu_{s_2}^{-1}) - \mu_{s_2}^{-1})b \in IA$$

Se cumple el lema. □

Proposición 4.17. *Sea K un cuerpo diferencial, $K \subset L$ una extensión de Picard Vessiot con grupo de Galois diferencial $G(L|K) = G$. Sea $T = R/P$ entonces tenemos el isomorfismo de $\overline{K}[G]-$módulos :*

$$\overline{K} \otimes_K T \simeq \overline{K} \otimes_{C_K} C_K\left[G\right]$$

Prueba. Consideramos la $K-$álgebra $R = K\left[Y_{ij}, 1/\det\right]$ con derivación

$$\begin{aligned}Y'_{ij} &= Y_{i+1,j}, 0 \leq i \leq n-2 \\ Y'_{n-1,j} &= -a_0Y_{0j} - a_1Y_{1j} - \cdots - a_{n-1}Y_{n-1,j}\end{aligned}$$

Consideramos el $L-$álgebra $L\left[Y_{ij}, 1/\det\right]$ con la derivación definida por la derivación en L y la anterior formula. Consideramos la C_K-álgebra $C_K\left[X_{st}, 1/\det\right]$

donde X_{st}, $1 \leq s,t \leq n$ son indeterminadas, det es el determinante de (X_{st}) y recordemos que $C_K[X_{st}, 1/\det]$ es el álgebra coordenada $C_K[\mathrm{GL}(n, C_K)]$ del grupo algebraico $\mathrm{GL}(n, C_K)$.

Consideramos la acción del grupo G sobre $\mathrm{GL}(n, C_K)$ por traslación a izquierda:

$$G \times \mathrm{GL}(n, C_K) \to \mathrm{GL}(n, C_K)$$
$$(g, h) \longmapsto gh$$

que induce la acción de G sobre $C_K[\mathrm{GL}(n, C_K)]$

$$G \times C_K[\mathrm{GL}(n, C_K)] \to C_K[\mathrm{GL}(n, C_K)]$$
$$(g, f) \longmapsto \lambda_g(f)$$

donde $\lambda_g(f)(h) = f(g^{-1}h)$. Definimos la relación entre las indeterminadas Y_{ij} y X_{st} por:

$$(Y_{ij}) = (r_{ab})(X_{st}),$$

donde $r_{ab} = \overline{Y_{ab}}$.

De la definición de derivación para los Y_{ij} y la relación entre (Y_{ij}) y (X_{st}) tenemos que $X'_{st} = 0$ para todo $s, t = 1, \ldots, n$. Tenemos entonces los siguientes anillos:

$$K[Y_{ij}, 1/\det] \subset L[Y_{ij}, 1/\det] = L[X_{st}, 1/\det] \subset C_K[X_{st}, 1/\det]$$

cada uno dotado de una derivación y una $G-$acción.

Por el lema 4.16 tenemos una biyección entre el conjunto de ideales diferenciales de $K[Y_{ij}, 1/\det]$ y el conjunto de ideales diferenciales $G-$estables de $L[Y_{ij}, 1/\det]$, y por el lema 4.15 tenemos una biyección entre el conjunto de ideales diferenciales $G-$estables de $L[Y_{ij}, 1/\det]$ y el conjunto de ideales $G-$estables de $C_K[X_{st}, 1/\det]$. Componiendo ambas, obtenemos una biyección entre el conjunto de ideales diferenciales de $K[Y_{ij}, 1/\det]$ y el conjunto de ideales $G-$estables de $C_K[X_{st}, 1/\det]$.

Luego para el ideal diferencial maximal P de $K[Y_{ij}, 1/det]$, tenemos que

$$Q = PL[Y_{ij}, 1/\det] \cap C_K[X_{st}, 1/\det]$$

es un ideal maximal $G-$estable de $C_K[X_{st}, 1/det]$ y por tanto un ideal radical, luego define una variedad W de $\mathrm{GL}(n, C_K)$:

$$W = \{g \in GL(n, C_K) : f(g) = 0, f \in Q\}$$

Sean $g_0 \in W$ un elemento fijo arbitrario, $f \in Q$ y $\sigma \in G$, tenemos que $\lambda_{\sigma^{-1}}(f) \in Q$ pues Q es $G-$estable, luego $f(\sigma g_0) = \lambda_{\sigma^{-1}}(f)(g_0) = 0$. Así $\sigma g_0 \in W$ para todo $\sigma \in G$, luego $W = g_0 G$ es una clase de equivalencia en $\mathrm{GL}(n, C_K)$ para el grupo G visto como subgrupo de $\mathrm{GL}(n, C_K)$. Entonces tenemos que $W \simeq G$, luego $W_{\overline{K}} \simeq G_{\overline{K}}$ y por tanto sus anillos de coordenadas tambien son isomorfos:

$$\overline{K} \otimes_{C_K} C_K[W] = \overline{K}[W_{\overline{K}}] \simeq \overline{K}[G_{\overline{K}}] = \overline{K} \otimes_{C_K} C_K[G]$$

Consideremos

$$\begin{aligned} \pi : L[Y_{ij}, 1/det] &\longrightarrow \frac{L[Y_{ij}, 1/det]}{P} \\ Y_{ij} &\longmapsto \overline{Y_{ij}} \end{aligned}$$

Como P es un ideal de $K[Y_{ij}, 1/det]$ entonces $\mathrm{Ker}(\pi) = PL[Y_{ij}, 1/det]$, luego por el primer teorema de isomorfismos para anillos,

$$\frac{L[Y_{ij}, 1/det]}{PL[Y_{ij}, 1/det]} \simeq \frac{L[Y_{ij}, 1/det]}{P},$$

así tenemos:

$$\begin{aligned} L \otimes_K T = L \otimes_K (R/P) = L \otimes_K \frac{K[Y_{ij}, 1/det]}{P} \simeq L \otimes_K K[\overline{Y_{ij}}, \overline{1/det}] \\ \simeq L[\overline{Y_{ij}}, \overline{1/det}] = \frac{L[Y_{ij}, 1/det]}{P} \simeq \frac{L[Y_{ij}, 1/det]}{PL[Y_{ij}, 1/det]} \end{aligned}$$

Consideremos ahora

$$\begin{aligned} \pi' : L[Y_{ij}, 1/det] &\longrightarrow \frac{L[Y_{ij}, 1/det]}{Q} \\ Y_{ij} &\longmapsto \overline{Y_{ij}} \end{aligned}$$

Como Q es un ideal de $C_K[X_{st}, 1/det]$, entonces $\mathrm{Ker}(\pi') = QL[Y_{ij}, 1/det] = PL[Y_{ij}, 1/det]$. Luego por el primer teorema de isomorfismos para anillos:

$$\frac{L[Y_{ij}, 1/det]}{PL[Y_{ij}, 1/det]} \simeq \frac{L[Y_{ij}, 1/det]}{Q},$$

Y observamos también que

$$\frac{L[Y_{ij}, 1/det]}{Q} \simeq L[\overline{Y_{ij}}, \overline{1/det}] \simeq L \otimes_{C_K} C_K[\overline{Y_{ij}}, \overline{1/det}] = L \otimes_{C_K} \frac{C_K[Y_{ij}, 1/det]}{Q}.$$

Por lo tanto:

$$L \otimes_K T \simeq \frac{L[Y_{ij}, 1/det]}{PL[Y_{ij}, 1/det]} \simeq L \otimes_{C_K} \frac{C_K[Y_{ij}, 1/det]}{Q} = L \otimes_{C_K} C_K[W].$$

Entonces

$$\overline{L} \otimes_K T \simeq \overline{L} \otimes_{C_K} C_K [W] .$$

Sea V la subvariedad afin de $\mathrm{GL}(n, C_K)$ que corresponde al ideal P de $K[Y_{ij}, 1/\det]$: $V = \{x \in \mathrm{GL}(n, C_K) : f(x) = 0, \forall f \in P\}$, entonces $T = K[V]$, así:

$$V_{\overline{L}} \simeq W_{\overline{L}}.$$

Como V y W son ambas variedades sobre K^{n^2}, por la proposición 1.5 tenemos que $V_{\overline{K}} \simeq W_{\overline{K}}$, luego sus anillos de coordenadas tambien son isomorfos:

$$\overline{K} \otimes_K K[V] = \overline{K}[V_{\overline{K}}] \simeq \overline{K}[W_{\overline{K}}] = \overline{K} \otimes_{C_K} C_K [W] .$$

Finalmente:

$$\overline{K} \otimes_K T \simeq \overline{K} \otimes_{C_K} C_K [W] \simeq \overline{K} \otimes_{C_K} C_K [G] .$$

□

Observamos que en el isomorfismo de la proposición 4.17, el lado izquierdo $\overline{K} \otimes_K T$ no requiere el grupo G para su definición, mientras que el lado derecho $\overline{K} \otimes_{C_K} C_K [G]$ determina G, por lo tanto este isomorfismo será uno de los primeros pasos para recuperar G a partir de $K = L^G$.

Corolario 4.18. *Sea $K \subset L$ una extensión de Picard Vessiot con $G = G(L|K)$ entonces* $\dim G(L|K) = \mathrm{trdeg}\,[L : K]$

Prueba. La dimensión de la variedad algebraica G es igual a la dimensión de Krull de su anillo de coordenadas $C_K[G]$. Se puede probar que la dimensión de Krull de una C_K-álgebra no cambia cuando es multiplicada tensorialmente por una extensión de cuerpo de C_K. Por la proposición anterior, la dimensión de Krull[1] de $C_K[G]$ es igual a la dimensión de Krull del álgebra T, que por el lema de normalización de Noether es igual al grado de trascendencia de L sobre K. □

[1]En álgebra conmutativa, se llama dimensión de Krull de un anillo R al supremo de las longitudes de las cadenas de ideales primos ordenados por inclusión estricta.

4.3. El Teorema fundamental

El objetivo de este capítulo es establecer el teorema fundamental de la teoria de Picard-Vessiot, que es análogo al teorema fundamental en teoria de Galois clásica.

Si $K \subset L$ es una extensión de Picard-Vessiot y F es un cuerpo diferencial intermedio, entonces $F \subset L$ es una extensión de Picard-Vessiot para el mismo operador diferencial lineal homogéneo que $K \subset L$. Luego $L \subset F$ es una extensión de Picard Vessiot con grupo de Galois diferencial

$$G(L|F) = \left\{\sigma \in G(L|K) : \sigma_{|_F} = id_F\right\}.$$

Si H es un subgrupo de $G(L|K)$ denotamos por L^H al subcuerpo de L fijado por la acción de H

$$L^H = \{x \in L : \sigma(x) = x, \forall \sigma \in H\}.$$

Notamos que L^H es estable bajo la derivación de L.

Proposición 4.19. *Sea $K \subset L$ una extensión de Picard Vessiot y $G(L|K)$ su grupo de Galois diferencial. Las correspondencias*

$$H \mapsto L^H, \quad F \mapsto G(L|F)$$

definen aplicaciones biyectivas mutuamente inversas que invierten la inclusión entre el conjunto de subgrupos Zariski cerrados H de $G(L|K)$ y el conjunto de cuerpos diferenciales F con $K \subset F \subset L$.

Prueba. Sean H_1, H_2 subgrupos de $G(L|K)$ con $H_1 \subset H_2$ entonces $L^{H_2} \subset L^{H_1}$. Analogamente, si F_1, F_2 son cuerpos diferenciales intermedios de la extensión $K \subset L$ con $F_1 \subset F_2$ entonces $G(L|F_2) \subset G(L|F_1)$.

Veamos ahora que $L^{G(L|F)} = F$ para todo F cuerpo diferencial intermedio de $K \subset L$.

En efecto, como $K \subset L$ es una extensión de Picard Vessiot y $K \subset F \subset L$ entonces $F \subset L$ es una extensión de Picard Vessiot, luego por el corolario 4.4 se tiene que $L^{G(L|F)} = F$.

Veamos ahora que si H es un subgrupo de $G(L \mid K)$, no necesariamente cerrado, entonces $G(L|L^H)$ es la clausura de Zarski de H en G.

Dado $\sigma \in H$, entonces por definición de L^H tenemos que $\sigma(x) = x$ para todo $x \in L^H$, así $\sigma_{|_{L^H}} = id_{L^H}$ y por tanto $\sigma \in G(L|L^H)$. Así tenemos la inclusión

$H \subset G(L|L^H)$. Entonces $\overline{H}^G \subset G(L|L^H)$. Supongamos que $\overline{H}^G \neq G(L|L^H)$, entonces existe $g \in G(L|L^H)$ tal que $g \notin \overline{H}^G$.

Como

$$\overline{H}^G = \mathcal{V}(\mathcal{I}(H)) = \mathcal{V}(\{f \in C_K[\mathrm{GL}(n, C_K)] : f(h) = 0, h \in H\})$$

existe $f \in C_K[\mathrm{GL}(n, C_K)]$ tal que $f_{|_H} = 0$ con $f(g) \neq 0$.

Sea $L = \langle y_1, \ldots, y_n \rangle$, consideremos las matrices $A = (y_j^{(i)})$, $0 \leq i \leq n-1$, $1 \leq j \leq n$ y $B = (y_j^{(i)})$, $0 \leq i \leq n-1$, $1 \leq j \leq n$, donde $u_1, \ldots, u_n$ son indeterminadas diferenciales.

Hacemos actuar al grupo de Galois por la derecha, es decir, definimos la matriz M_σ de $\sigma \in G(L|K)$ tal que $(\sigma(y_1), \ldots, \sigma(y_n)) = (y_1, \ldots, y_n)M_\sigma$, es decir $M_\sigma = (c_{ij}) \in \mathrm{GL}(n, C_K)$ donde $\sigma(y_i) = \sum_{j=1}^{n} y_j c_{ji}$.

Como $W(y_1, \ldots, y_n) \neq 0$, entonces A es inversible y podemos definir el polinomio

$$F(u_1, \ldots, u_n) = f(A^{-1}B) \in L\{u_1, \ldots, u_n\}$$

Luego, si $\sigma \in H$, como $f_{|_H} = 0$, tenemos que $f(M_\sigma) = 0$, entonces:

$$F(\sigma(y_1), \ldots, \sigma(y_n)) = f(A^{-1}C)$$

donde $(\sigma(y_j^i))$, $0 \leq i \leq n-1, 1 \leq j \leq n$.

Luego $F(\sigma(y_1), \ldots, \sigma(y_n)) = f(AA^{-1}M_\sigma) = f(M_\sigma) = 0$, y para $g \in G(L|L^H)$ tenemos $F(g(y_1), \ldots, g(y_n)) = f(M_g) \neq 0$. Esto quiere decir que el polinomio F tiene la propiedad de que $F(\sigma(y_1), \ldots, \sigma(y_n)) = 0$ para todo $\sigma \in H$ pero no para todo $\sigma \in G(L|L^H)$.

Supongamos que escogemos F de entre todos los polinomios con esta propiedad, y que tiene el menor número de monomios distitntos de cero. Sea entonces

$$F(u_1, \ldots, u_n) = \sum_{i_1, \ldots, i_n = 1}^{m} \lambda_{i_1, \ldots, i_n} u_1^{(i_1)} \ldots u_n^{(i_n)}$$

con m minimal, tal que $\lambda_{i_1, \ldots, i_n} \neq 0$. Denotaremos $i_1, \ldots, i_n := i$. Como los coeficientes de F pertenecen al cuerpo L y son distintos de cero, podemos asumir que alguno de estos es la ideantidad, sea entonces $\lambda_s = 1$.

Sea $\tau \in H$, podemos definir el polinomio:

$$(\tau F)(u_1, \ldots, u_n)) = \sum_{i=1}^{m} \tau(\lambda_i) u_1^{(i_1)} \ldots u_n^{(i_n)}$$

Entonces, dado $\sigma \in H$:

$$\begin{aligned}
(\tau F)\left(\sigma(y_1),\ldots,\sigma(y_n)\right) &= \sum_{i=1}^{m} \tau\left(\lambda_i\right) \sigma(y_1)^{(i_1)} \ldots \sigma(y_n)^{(i_n)} \\
&= \sum_{i=1}^{m} \tau\left(\lambda_i\right) \tau(\tau^{-1}\sigma(y_1))^{(i_1)} \ldots \tau(\tau^{-1}\sigma(y_n))^{(i_n)} \\
&= \tau\left(\sum_{i=1}^{m} \lambda_i (\tau^{-1}\sigma(y_1))^{(i_1)} \ldots (\tau^{-1}\sigma(y_n))^{(i_n)}\right) \\
&= \tau\left(F\left(\tau^{-1}\sigma(y_1),\ldots,\tau^{-1}\sigma(y_n)\right)\right) \\
&= 0, \quad \text{pues} \quad \tau^{-1}\sigma \in H
\end{aligned}$$

Por otro lado, observamos que:

$$\begin{aligned}
(F-\tau F)\left(u_1,\ldots,u_n\right) &= \sum_{i=1}^{m} \lambda_i u_1^{(i_1)} \ldots u_n^{(i_n)} - \sum_{i=1}^{m} \tau\left(\lambda_i\right) u_1^{(i_1)} \ldots u_n^{(i_n)} \\
&= \sum_{i\neq s}^{m} \left[\lambda_i - \tau\left(\lambda_i\right)\right] u_1^{(i_1)} \ldots u_n^{(i_n)}
\end{aligned}$$

tiene al menos un término menos que F.

Como F es el polinomio con menos terminos (monomios distintos de cero) que se anula en $(\sigma(y_1),\ldots,\sigma(y_n))$ para todo $\sigma \in H$ pero no para todo $\sigma \in G(L|L^H)$, entonces $F-\tau F$ debe anularse en $(\sigma(y_1),\ldots,\sigma(y_n))$ para todo $\sigma \in G(L|L^H)$. Ahora,

- Si $F-\tau F \neq 0$ para alg"un $\tau \in H$, entonces al menos alguno de sus coeficientes es distinto de cero, es decir existe algún $\lambda_j \neq 1$ tal que $\lambda_j - \tau(\lambda_j) \neq 0$. Sea $a = \dfrac{\tau(\lambda_j)-\lambda_j}{\lambda_j}$, entonces

$$\begin{aligned}
(F - a(F-\tau F)) &= \sum_{i=1}^{m} \lambda_i u_1^{(i_1)} \ldots u_n^{(i_n)} - \sum_{i\neq s}^{m} a\left[\lambda_{i_1,\ldots,i_n} - \tau(\lambda_i)\right] u_1^{(i_1)} \ldots u_n^{(i_n)} \\
&= \sum_{i\neq s}^{m} \left[\lambda_{i_1,\ldots,i_n} - a\lambda_i + \tau(\lambda_i)\right] u_1^{(i_1)} \ldots u_n^{(i_n)} + u_1^{(s_1)} \ldots u_n^{(s_n)} \\
&= \sum_{i\neq s,j}^{m} \left[\lambda_i - a\lambda_i + \tau(\lambda_i)\right] u_1^{(i_1)} \ldots u_n^{(i_n)} + u_1^{(s_1)} \ldots u_n^{(s_n)} \\
&= \sum_{i\neq j} \left[\lambda_i - a\lambda_i + \tau(\lambda_i)\right] u_1^{(i_1)} \ldots u_n^{(i_n)}
\end{aligned}$$

  tiene al menos un término menos que F. Como F y τF se anulan en $(\sigma(y_1),\ldots,\sigma(y_n))$ para todo $\sigma \in H$, lo mismo sucede con $F - a\left(F-\tau F\right)$.

Por otro lado, teniamos que $F - \tau F$ se anula en $(g(y_1), \ldots, g(y_n))$ pero $F(g(y_1), \ldots, g(y_n)) \neq 0$, luego $F - a(F - \tau F)(g(y_1), \ldots, g(y_n)) \neq 0$. Por lo tanto $F - a(F - \tau F)$ verifica la misma propiedad que F, lo cual contradice la minimalidad de términos de F.

- Si $F - \tau F = 0$ para todo $\tau \in H$, entonces todos sus coeficientes son ceros, luego $\lambda_i = \tau(\lambda_i)$ para todo $\tau \in H$, $i \neq 1$, así todos los coeficientes de F son $H-$invariantes, es decir $\lambda_i \in L^H$. Como $K \subset L$ es una extensión de Picard Vessiot y L^H es un cuerpo intermedio de dicha extensión, por una observación anterior tenemos que $L^H \subset L$ es una extensión de Picard Vessiot. Por el corolario 4.4 $L^H = L^{G(L|L^H)}$, entonces $\lambda_i \in L^{G(L|L^H)}$.

  Así, dado $\sigma \in G(L|L^H)$, se tiene que $\lambda_i = \sigma(\lambda_i)$ para todo $i = 1, \ldots, m$, entonces $F = \sigma F$, luego

  $$F(\sigma(y_1), \ldots, \sigma(y_n)) = (\sigma F)(\sigma(y_1), \ldots, \sigma(y_n)) = \sigma(F(y_1, \ldots y_n)) = \sigma(f(Id_L))$$

  Como H es un subgrupo se tiene que $id_L \in H$ y como $f_{|_H} = 0$ tenemos que $\sigma(f(id_L)) = 0$. Por lo tanto tenemos que $F(\sigma(y_1), \ldots, \sigma(y_n)) = 0$ para todo $\sigma \in G(L|L^H)$, lo cual no es cierto pues no se cumple para el elemento $g \in G(L|L^H)$.

Finalmente $G(L|L^H) = \overline{H}^G$. □

Proposición 4.20. *Sea $K \subset L$ una extensión de cuerpos diferenciales, con grupo de Galois diferencial $G = G(L|K)$*

a) Si H es un subgrupo normal de G, entonces L^H es $G-$estable.

b) Si F es un cuerpo diferencial intermedio de la extensión, que es $G-$estable, entonces $G(L|F)$ es un subgrupo normal de G. Es más, el morfismo

$$G(L|K) \longrightarrow G(F|K)$$
$$\sigma \longmapsto \sigma_{|_F}$$

induce un isomorfismo del cociente $G/G(L|F)$ en el grupo de todos los $K-$automorfismos diferenciales de F que pueden ser extendidos a L.

Prueba.

a) Sean $a \in L^H$ y $\sigma \in G$, queremos probar que $\sigma(a) \in L^H$. Sea $\tau \in H$, como H es un subgrupo normal de G, entonces $\sigma^{-1}\tau\sigma \in H$. Luego $(\sigma^{-1}\tau\sigma)(a) = a$ entonces $\tau(\sigma(a)) = \sigma(a)$.

b) Sea F un cuerpo diferencial $G-$estable con $K \subset F \subset L$, queremos probar que $G(L|F)$ es un subgrupo normal de G. Sea $\sigma \in G$ y $\tau \in G(L|F)$, mostraremos que $\sigma^{-1}\tau\sigma \in G(L|F)$. Sea $a \in F$, como F es $G-$estable entonces $\sigma(a) \in F$ y como $\tau \in G(L|F)$ tenemos que $\tau_{|_F} = id_F$, luego $\tau(\sigma(a)) = \sigma(a)$, así $\sigma^{-1}\tau\sigma(a) = a$.

Por otro lado, como F es $G-$estable entonces $\sigma(x) \in F$ para todo $\sigma \in G$ y $x \in F$, luego $\sigma_{|_F} \subset F$ es decir $\sigma_{|_F} \in G(F \mid K)$. Por lo tanto podemos definir:

$$\varphi : G(L|K) \longrightarrow G(F|K)$$
$$\sigma \longmapsto \sigma_{|_F}.$$

Si $\sigma \in \mathrm{Ker}(\varphi)$ entonces $\sigma_{|_F} = id_F$ y por definición $\sigma \in G(L \mid F)$. Por otro lado

$$\mathrm{Im}(\varphi) = \left\{\sigma_{|_F} \in G(F|K) : \sigma \in G(L|K)\right\}$$

que es el conjunto de todos los $K-$automorfismos diferenciales de F que pueden ser extendidos a L. Luego se obtiene el isomorfismo inducido, mediante el primer teorema de isomorfismos para grupos.

□

Definición 4.21. Sea $K \subset L$ una extensión de cuerpos diferenciales, diremos que es una extensión **normal** si para cada $x \in L \setminus K$, existe un elemento $\sigma \in G(L|K)$ tal que $\sigma(x) \neq x$.

Proposición 4.22. *Sea $K \subset L$ una extensión de Picard Vessiot y $G := G(L|K)$.*

a) Sea H un subgrupo cerrado de G. Si H es normal en G, entonces la extensión diferencial de cuerpos $K \subset L^H$ es normal.

b) Sea F un cuerpo diferencial con $K \subset F \subset L$. Si $K \subset F$ es una extensión de Picard Vessiot entonces el subgrupo $G(L|F)$ es normal en $G(L|K)$. En este caso, el morfismo:

$$G(L|K) \longrightarrow G(F|K)$$
$$\sigma \longmapsto \sigma_{|_F}$$

induce un isomorfismo: $G(L|K)/G(L|F) \simeq G(F|K)$

Prueba.

a) Sea $x \in L^H \setminus K$, entonces $x \in L \setminus K$ y como $K \subset L$ es una extensión de Picard Vessiot, por el corolario 4.3 tenemos que existe $\sigma \in G(L \mid K)$ tal que $\sigma(x) \neq x$. Por la proposición anterior tenemos que L^H es $G-$estable, luego $\sigma_{|_{L^H}}(L^H) = L^H$ entonces $\sigma_{|_{L^H}} \in G(L^H|K)$.

b) Por el corolario 3.11, cualquier $K-$automorfismo de L envía F en si mismo, es decir $\sigma(F) \subset F$ para todo $\sigma \in G(L|K)$, esto es, F es $G-$ estable. Luego por la proposición anterior $G(L|F)$ es un subgrupo normal de G.
También, como F es $G-$estable, se tiene que $\sigma_{|_F} \in G(F|K)$ para todo $\sigma \in G$,así podemos definir el morfismo:

$$\varphi : G(L|K) \longrightarrow G(F|K)$$
$$\sigma \longmapsto \sigma_{|_F}.$$

Observamos que $Ker(\varphi) = \left\{\sigma \in G : \sigma_{|_F} = id_F\right\} = G(L|F)$. Por otro lado, como F es un cuerpo intermedio de la extension de Picard Vessiot $K \subset L$ y $K \subset F$ es una extensión de Picard Vessiot, por la proposición 4.3, dado $\tau \in G(F|K)$ entonces τ puede ser extendido a un automorfismo diferencial de L. Observamos que $Im(\varphi) = \left\{\sigma_{|_F} : \sigma \in G(L|K)\right\}$ es el conjunto de $K-$automorfismos diferenciales de F que pueden ser extendidos a L. Así $G(F|K) = Im(\varphi)$ y luego por el primer teorema de isomorfismos para grupos:

$$G(L|K)/G(L|F) \simeq G(F|K)$$

Se demuestra la proposición. □

Ahora veremos el rol que tienen los subgrupos normales H de $G(L|K)$ en el teorema de correspondencia. La siguiente proposición establece la parte más dificil del Teorema Fundamental, que establece que el cuerpo intermedio F que corresponde a un subgrupo normal de G es una extensión de Picard-Vessiot de K.

Para la prueba de una parte de esta proposición necesitaremos los siguientes lemas:

Lema 4.23. *Sea K un cuerpo, $\overline{K}$ una clausura algebraica de K y A una $K-$álgebra. Si $\overline{K} \otimes_K A$ es una $\overline{K}-$álgebra finitamente generada, entonces existe una extensión finita $\widetilde{K}$ de K tal que $\widetilde{K} \otimes_K A$ es una $\widetilde{K}-$álgebra finitamente generada.*

Prueba. Sea $\{v_s\}_{s\in S}$ una base de $\overline{K}$ como K espacio vectorial, y sea $\overline{K}\otimes_K A = \overline{K}[\lambda_1\otimes a_1,\ldots,\lambda_n\otimes a_n]$. Como todos los $\lambda_i\in\overline{K}$, $i=1,\ldots,n$ entonces existe un subconjunto finito $S_i=\left\{s_{i1,\ldots,s_{im_i}}\right\}\subset S$ tal que

$$\lambda_i=\sum_{j=1}^{m_i}\alpha_{ij}v_{s_{ij}}$$

donde $\alpha_{ij}\in K$. Sea $S'=\bigcup_{i=1}^n S_i$. Definimos

$$\widetilde{K}=K(\{v_s\}_{s\in S'})=K(v_{s_{11}},\ldots,v_{s_{1m_1}},\ldots,v_{s_{n1}},\ldots,v_{s_{nm_n}}),$$

entonces

$$\widetilde{K}\otimes_K A=\widetilde{K}[v_{s_{11}}\otimes a_1,\ldots,v_{s_{nm_n}}\otimes a_1,\ldots,v_{s_{11}}\otimes a_n,\ldots,v_{s_{nm_n}}\otimes a_n]$$

es decir $\{v_s\otimes a_i\}_{s\in S',i=1,\ldots,n}$ genera a $\widetilde{K}\otimes_K A$ como $\widetilde{K}-$álgebra. □

Lema 4.24. *Sea K un cuerpo, A una K álgebra finitamente generada y sea U un grupo finito de automorfismos de A. Entonces la subalgebra A^U de A fijada por la acción de U, es decir $A^U=\{a\in A:\sigma(a)=a,\ \forall\sigma\in U\}$ es una K álgebra finitamente generada.*

Prueba. Sea $U=\{\sigma_1,\ldots,\sigma_N\}$. Definimos para todo $a\in A$:

$$S(a)=\frac{1}{N}\sum_{i=1}^N\sigma_i(a)$$

y consideremos el polinomio

$$P_a(T)=\prod_{i=1}^N(T-\sigma_i(a))=T^N+\sum_{i=1}^N(-1)^i a_i T^{N-i}$$

donde $a_i=e_i(\sigma_1(a),\ldots,\sigma_N(a))$ y e_i son los polinomios simétricos elementales.

Observemos que

$$S(a^j)=\frac{1}{N}\sum_{i=1}^N\sigma_i(a^j)=\frac{1}{N}\sum_{i=1}^N(\sigma_i(a))^j=\frac{1}{N}p_j(\sigma_1(a),\ldots,\sigma_N(a))$$

donde los p_j son los polinomios simétricos de sumas de potencias.

Por la fórmula de Newton:

$$e_i=(-1)^i\sum_{m_1+2m_2+\ldots+im_i=i}\prod_{j=1}^i\frac{(-p_j)^{m_j}}{m_j\,!j^{m_j}}$$

podemos expresar los a_i en términos de $S(a^j)$, $j = 1, \ldots, N$. Es fácil ver que $S(a^j) \in A^U$ para todo $j = 1, \ldots, n$.

Sea $A = K[u_1, \ldots u_m]$ y consideremos la subalgebra B de A^U: $B = K[S(u_i^j)]_{\substack{i=1,\ldots,m \\ j=1,\ldots,N}}$. Como U es un grupo, entonces algún $\sigma_{i_0} = id_A$, luego $\sigma_{i_0}(u_i) = u_i$ para todo $i = 1, \ldots, m$, así

$$0 = P_{u_i}(u_i) = \prod_{j=1}^{N}(u_i - \sigma_j(u_i)) = u_i^N + \sum_{j=1}^{N}(-1)^j u_{ij} u_i^{N-j}$$

donde $u_{ij} = S_j(\sigma_1(u_i), \ldots, \sigma_N(u_i))$ y como vimos antes, los u_{ij} pueden ser expresados en términos de $S(u_i^j)$, $i = 1, \ldots, m$, $j = 1, \ldots, N$. Entonces

$$u_i N = \sum_{j=1}^{N}(-1)^{j+1} u_{ij} u_i^{N-j}$$

es decir, $u_i N$ puede ser escrito como combinación lilneal de $u_i^{N-1}, \ldots, u_i, 1$ con coeficientes en B.

Luego dados $r_i \in \mathbb{N}$ podemos escribir $u_i^{r_i}$ en términos de $u_i^{a_i}$ con coeficientes en B donde $a_i < N$, entonces podemos escribir un monomio $u_1^{r_1} \ldots u_m^{r_m}$ en términos de $u_1^{a_1} \ldots u_m^{a_m}$ con coeficientes en B donde $a_i < N$. Por lo tanto, todo elemento de A puede ser escrito de la forma

$$a = \sum_{a_i < N} \lambda_{a_1 \ldots a_n} u_1^{a_1} \ldots u_m^{a_m}$$

donde $\lambda_{a_1 \ldots a_n} \in B$. Ahora si $a \in A^U$ entonces

$$a = S(a) = \sum_{a_i < N} S(\lambda_{a_1 \ldots a_n}) S(u_1^{a_1} \ldots u_m^{a_m}) = \sum_{a_i < N} \lambda_{a_1 \ldots a_n} S(u_1^{a_1} \ldots u_m^{a_m})$$

Así A^U puede ser generado sobre K por el conjunto finito

$$\{S(u_1^{a_1} \ldots u_m^{a_m})\}_{a_i < N} \cup \left\{S(u_i^N)\right\}_{i=1,\ldots,m}$$

□

Lema 4.25. *Sea $K \subset L$ una extensión de Picard-Vessiot, $G(L|K)$ su grupo de Galois diferencial y H un subgrupo cerrado normal de $G(L|K)$. Si se tiene una $K-$subalgebra finitamente generada T de L que satisface las siguientes condiciones:*

a) T es $G-$estable y su cuerpo de fracciones de L.

b) Para todo $t \in T$, el C_K-espacio vectorial generado por $\{\sigma(t) : \sigma \in G\}$ es finito dimensional.

c) La subalgebra $T^H = \{t \in T : \sigma(t) = t, \forall \sigma \in H\}$ es una $K-$álgebra finitamente generada.

d) L^H es el cuerpo de fracciones de T^H.

Entonces la extensión $K \subset L^H$ es de Picard-Vessiot.

Prueba. Probaremos que en estas condiciones, la extensión $K \subset L^H$ es de Picard-Vessiot. Veremos que T^H es generado sobre K por el espacio de soluciones de una ecuación diferencial lineal homogénea con coeficientes en K.

Primero observemos que como $H \trianglelefteq G$, T^H es $G-$estable. En efecto, dados $t \in T^H$, $\tau \in G$ mostraremos que $\tau(t) \in T^H$. Sea $\sigma \in H$, por la normalidad de H se tiene que $\tau^{-1}\sigma\tau \in H$, luego $(\tau^{-1}\sigma\tau)(t) = t$ es decir $\sigma(\tau(t)) = \tau(t)$. Así T^H es una subalgebra $G-$estable de T y la restricción de la acción de G a T^H induce una acción del grupo cociente G/H sobre T^H.

Por las condiciones *b*) y *c*) podemos encontrar un subespacio finito dimensional $V \subset T^H$ sobre C_K que genera a T^H como $K-$álgebra y que es $G-$estable.

Sea $y_1, \ldots, y_n$ una base de V sobre C_K, entonces el conjunto $\{y_1, \ldots, y_n\}$ es C_K linealmente independiente. Como la extensión $K \subset L$ es de Picard-Vessiot entonces $C_K = C_L$, luego los $y_i \in L$ son C_L linealmente independientes. Por la proposición 2.25: $W(y_1, \ldots, y_n) \neq 0$, luego podemos definir:

$$\mathcal{L}(Y) = \frac{W(Y, y_1, \ldots, y_n)}{W(y_1, \ldots, y_n)}.$$

Para cualquier $y \in V$ el conjunto $\{y, y_1, \ldots, y_n\}$ es C_L linealmente dependiente, entonces $W(y, y_1, \ldots, y_n) = 0$ y luego $\mathcal{L}(y) = 0$.

Es conveniente considerar la forma explícita de $\mathcal{L}$ obtenida por expansión de cofactores a lo largo de la primera columna del numerador. Por el ejemplo 2.23

$$W(Y, y_1, \ldots, y_n) = \sum_{i=o}^{n} a_i Y^{(i)}$$

donde $a_i = (-1)^i \det(\ldots, \underline{y}^{(i-1)}, \underline{y}^{(i+1)}, \ldots)$ y $\underline{y} = (y_1, \ldots, y_n)$. En particular, notamos que $a_n = W(y_1, \ldots, y_n)$. Luego

$$\mathcal{L}(Y) = \sum_{i=0}^{n} b_i Y^{(i)} \text{ donde } b_i = \frac{a_i}{a_n}$$

Como V es $G-$estable, para cualquier $\sigma \in G$ tenemos que $\sigma(y_i) \in V$, $i = 1, \ldots, n$, entonces

$$\sigma(y_i) = \sum_{j=1}^{n} c_{ij} Y_j, c_{ij} \in C_K$$

Luego

$$\sigma(a_i) = a_i \det(\sigma_{|_V})$$

Luego $\sigma(b_i) = \sigma(a_n)^{-1}\sigma(a_i) = \left[\det(\sigma_{|_V})a_n\right]\left[\det(\sigma_{|_V})a_i\right] = a_n^{-1}a_i = b_i$, entonces $b_i \in L^G$. Como $K \subset L$ es una extensión de Picard-Vessiot, $L^G = K$ luego los coeficientes $b_i \in K$ y $\mathcal{L} \in K\{Y\}$. Por lo tanto $T^H = K\langle y_1, \ldots, y_n\rangle$ luego L^H es una extensión Picard-Vessiot de K. □

Proposición 4.26. *Sea $K \subset L$ una extensión de Picard-Vessiot, $G(L|K)$ su grupo de Galois diferencial y H un subgrupo cerrado normal de $G(L|K)$. Entonces existe una $K-$álgebra diferencial T que verifica las condiciones (a), (b), (c) y (d) del lema 4.25.*

Prueba: Sea T la $K-$álgebra R/P considerada en la construcción de la extensión de Picard-Vessiot. Probaremos que T satisface las condiciones establecidas antes.

a) Por construcción, G actúa sobre T y el cuerpo de fracciones de T es igual a L.

b) Tomando en cuenta la observación 4.14, podemos aplicar la parte (a) del lema 1.18 y obtener que la orbita de un elemento $t \in T$ por la acción de G genera un C_K espacio vectorial finito dimensional.

c) Consideramos el isomorfismo de $G-$modulos dado por la proposición 4.17 y restringimos la acción al subgrupo H. Como el grupo H actúa sobre sobre el segundo factor de ambos $\overline{K} \otimes_K T$ y $\overline{K} \otimes_{C_K} C_K[G]$, tenemos que

$$\overline{K} \otimes_K T^H = (\overline{K} \otimes_K T)^H \simeq (\overline{K} \otimes_{C_K} C_K[G])^H = \overline{K} \otimes_{C_K} C_K[G]^H .$$

Por la proposición 1.31, $C_K[G]^H \simeq C_K[G/H]$, como C_K-álgebras. Ahora $C_K[G/H]$ es una C_K-álgebra finitamente generada y asi $\overline{K} \otimes_K T^H$ es una $\overline{K}-$álgebra finitamente generada.
Como $\overline{K} \otimes_K T^H$ es una $\overline{K}-$álgebra finitamente generada, por lema 4.23 existe una extensión finita $\widetilde{K}$ de K tal que $\widetilde{K} \otimes_K T^H$ es una $\widetilde{K}-$álgebra finitamente generada, y por tanto es también una $K-$álgebra finitamente generada. Podemos suponer que la extensión $K \subset \widetilde{K}$ es normal, y consideremos

su grupo de Galois $U = Gal(\widetilde{K}|K)$ actuando sobre $\widetilde{K} \otimes_K T^H$ sobre el primer factor. Luego por el lema 4.24 tenemos que $(\widetilde{K} \otimes_K T^H)^U$ es una $K-$álgebra finitamente generada, así

$$T^H \simeq K \otimes_K T^H = \widetilde{K}^U \otimes_K T^H \simeq (\widetilde{K} \otimes_K T^H)^U.$$

d) Probaremos ahora que el cuerpo de fracciones de T^H es L^H, para lo cual veremos que cualquier elemento $a \in L^H \setminus \{0\}$ se puede escribir como cociente de elementos en L^H.

Consideremos el ideal $J = \{t \in T : ta \in T\}$ formado por denominadores de a. Veamos que J es $H-$estable: sean $\sigma \in H$ y $t \in J$. Como T es $G-$estable tenemos

$$\sigma(ta) = \sigma(t)\sigma(a) = \sigma(t)a \in T,$$

luego $\sigma(t) \in J$. Así J es $H-$estable, es decir H actúa sobre J.

Sea $s \in J \setminus \{0\}$, teniendo en cuenta la observación 4.14 podemos aplicar el lema 1.18, así el espacio vectorial E generado por los $\tau(s)$, $\tau \in H$ sobre C_K es de dimensión finita y $H-$estable. Sea $s_1, \ldots, s_p$ una C_K-base de E y sea $w = W(s_1, \ldots, s_p)$. Expandimos el determinante respecto a la primera fila:

$$W(s_1, \ldots, s_p) = \begin{vmatrix} s_1 & s_2 & \ldots & s_p \\ s_1' & s_2' & \ldots & s_n' \\ \vdots & & \vdots & \\ s_1^{(p-1)} & s_2^{(p-1)} & \ldots & s_p^{(p-1)} \end{vmatrix} = \sum_{i=o}^{p} s_i a_i$$

donde $a_i = (-1)^{i+1} det(\ldots, \underline{s}^{(i-1)}, \underline{s}^{(i+1)}, \ldots)$ y $\underline{s_i} = \left(s_i', s_i'', \ldots, s_i^{(p-1)}\right)$. Luego $w = W(s_1, \ldots, s_p) \in J$.

Como E es $H-$estable, $\tau(s_i) = \sum_{j=1}^{p} c_{ij} s_j$, $c_{ij} \in C_K$ para todo $\tau \in H$. Luego por la proposición 2.24 tendremos $\tau(w) = \det(\tau_{|_E})w$ para todo $\tau \in H$.

Notamos que esto define un caracter χ de H por:

$$\chi : H \to \mathbb{G}_m(C_K)$$
$$\tau \to \det(\tau_{|_E})$$

donde $\mathbb{G}_m$ denota al grupo multiplicativo. Como $\tau(w) = \chi(\tau)w$, decimos que w es un semi-invariante de peso χ.

Sea $t = wa$. Como $w \in J$ entonces $t \in T$. Por otro lado

$$\tau(wa) = \tau(w)\tau(a) = \chi(\tau)wa,$$

es decir $\tau(t) = \det(\tau_{|_E})t$. Entonces t es un semi-invariante de peso χ. Podemos escribir a como t/w, luego si encontramos un semi-invariante μ con peso $1/\chi$ tendremos que $a = t\mu/w\mu$ es el cociente de dos invariantes, como es deseado.

Consideremos la subalgebra de T que consiste de todos los semi-invariantes de peso $1/\chi$:

$$T_{1/\chi} = \{t \in T : \tau(t) = (1/\chi)(\tau)t, \forall \tau \in H\}.$$

Probaremos que $T_{1/\chi} \neq 0$. Consideraremos la acción de H sobre el anillo de coordenadas $C_K[G]$ y probaremos que $C_K[G]_\eta \neq 0$ para todo $\eta \in X(H)$.
Sea H_0 la intersección de los núcleos de todos los caracteres de H:

$$H_0 = \bigcap_{\eta \in X(H)} Ker(\eta).$$

Como cada núcleo $\mathrm{Ker}(\eta) = \eta^{-1}(1)$ es un subgrupo normal y cerrado, su intersección H_0 es un subgrupo normal y cerrado de H. Luego por el corolario 1.27 tenemos que H/H_0 tiene estructura de grupo algebraico.

Es más, dados $\eta \in X(H)$, $g, h \in H$ se tiene

$$\eta(ghg^{-1}h^{-1}) = \eta(g)\eta(h)\eta(g^{-1})\eta(h^{-1}) = \eta(g)\eta(g)^{-1}\eta(h)\eta(h)^{-1} = 1.$$

Luego para todo $\eta \in X(H)$, el subgrupo conmutador $[H, H] \subset \mathrm{Ker}(\eta)$. Entonces $[H, H] \subset H_0$ y así H/H_0 es conmutativo.

Por el teorema 1.47 se tiene que H/H_0 es isomorfo al producto directo de sus subgrupos cerrados:

$$H/H_0 \simeq (H/H_0)_s \times (H/H_0)_u.$$

Denotemos $(H/H_0)_s = H'$ y $(H/H_0)_u = H''$. Por el teorema 1.20 tenemos que H'' es isomorfo a un subgrupo $\widetilde{H''}$ del grupo general lineal $\mathrm{GL}(n, C_K)$. Como $\widetilde{H''}$ es conmutativo, por el lema 1.46 existe $x \in \mathrm{GL}(n, C_K)$ tal que

$$x\widetilde{H''}x^{-1} \subset \mathcal{T}(n, C_K)$$

y como $\widetilde{H''}$ es unipotente, su único autovalor es 1. Así

$$x\widetilde{H''}x^{-1} \subset U(n, C_K)$$

es decir, $\widetilde{H''}$ es conjugado al subgrupo $x\widetilde{H''}x^{-1}$ del grupo unipotente triangular superior $U(n, C_K)$. Por el ejemplo 1.44 se tiene que $H'' \simeq \widetilde{H''}$ no tiene caracteres no triviales.

Dado $\eta \in X(H)$ se tiene que $H_0 \subset \mathrm{Ker}(\eta)$, y como $H_0 \trianglelefteq H$, por la propiedad universal del cociente, existe un único homomorfismo $\overline{\eta} : H/H_0 \to \mathbb{G}_m$ tal que $\overline{\eta} \circ \pi = \eta$, donde π es la proyección canónica de H en H/H_0. Esto define un isomorfismo

$$X(H) \to X(H/H_0)$$
$$\eta \mapsto \overline{\eta}$$

cuya inversa está dada por $\overline{\eta} \mapsto \overline{\eta} \circ \pi$. Así tenemos que

$$X(H) \simeq X(H/H_0) \simeq X(H')$$

Sea $\eta \in X(H')$. Entonces $\eta \in C_K[H']$, luego para cada $x, y \in H'$ tenemos

$$(x\eta)(y) = \eta(xy) = \eta(x)\eta(y),$$

entonces $x\eta = \eta(x)\eta$, es decir $\eta \in C_K[H']_\eta$ y así $C_K[H']_\eta \neq 0$.

La inclusión $H' \hookrightarrow G/H_0$ induce un epimorfismo entre los anillos coordenados $\pi : C_K[G/H_0] \to C_K[H']$. Probaremos que

$$\pi_{|_{C_K[G/H_0]_\eta}} : C_K[G/H_0]_\eta \to C_K[H']_\eta$$

también es un epimorfismo.

Sea $a \neq 0$, $a \in C_K[H']_\eta$ y sea $\alpha \in C_K[G/H_0]$ tal que $\pi(\alpha) = a$. Por el lema 1.18 existe un subespacio $H'-$estable de dimensión finita E_1 de $C_K[G/H_0]$ que contiene a α.

De manera análoga a lo que sucedía con H'', tenemos que H' es isomorfo a un subgrupo $\widetilde{H'}$ del grupo general lineal $\mathrm{GL}(n, C_K)$. Como $\widetilde{H'}$ es conmutativo y semisimple, por el lema 1.46 tenemos que $\widetilde{H'}$ es conjugado en el grupo general lineal a un subgrupo $\widehat{H'}$ del grupo de matrices diagonales $\mathcal{D}(n, C_K)$.

Luego a cada elemento h' de H' le podemos asociar un único elemento $\rho(h')$ en $\widehat{H'}$. Como E_1 es $H'-$estable entonces E_1 es también $\widehat{H'}-$estable. Esto define una representación de H' en E_1:

$$H' \longrightarrow \mathrm{GL}(E_1)$$
$$h' \longmapsto \rho(h').$$

Como $\rho(h')$ es diagonalizable para todo $h' \in H'$, entonces existe una base $\{\alpha_1, \ldots, \alpha_p\}$ de E_1 sobre C_K tal que todos los $\rho(h')$ se diagonalizan en dicha base, es decir

$$\rho(h')(\alpha_i) = c(\alpha_i, h')\alpha_i$$

donde $c(\alpha_i, h') \in C_K$. Denotemos $c(\alpha_i, h') = \eta_i(h')$ y $\rho(h') = \tau$, entonces tenemos el diagrama conmutativo:

$$\begin{array}{ccc} E & \xrightarrow{\tau} & E \subset C_K[G/H_0] \\ {\scriptstyle\pi}\downarrow & & \downarrow{\scriptstyle\pi} \\ C_K\left[H'\right] & \xrightarrow[\tau_{|_{C_K[H']}}]{} & C_K\left[H'\right] \end{array} .$$

Podemos escoger la base de E_1 tal que $\{\alpha_1, \ldots, \alpha_l\}$ con $l < p$ sea una base de $E_1 \cap \mathrm{Ker}(\pi)$.Sea

$$\alpha = \sum_{j=1}^{p} c_j \alpha_j, \quad c_j \in C_K$$

entonces

$$\tau(\alpha) = \sum_{j=1}^{p} c_j \tau(\alpha_j) = \sum_{j=1}^{p} c_j \eta_j(\tau)\alpha_j$$

luego

$$\pi\left(\tau(\alpha)\right) = \sum_{j=1}^{p} c_j \eta_j(\tau)\pi(\alpha_j) = \sum_{j=l+1}^{p} c_j \eta_j(\tau)\pi(\alpha_j).$$

Por otro lado

$$\pi\left(\tau(\alpha)\right) = \tau\left(\pi(\alpha)\right) = \tau(a) = \eta(\tau)a = \eta(\tau)\sum_{j=1}^{p} c_j \pi(\alpha_j) = \eta(\tau)\sum_{j=l+1}^{p} c_j \pi(\alpha_j).$$

Así tenemos

$$\sum_{j=l+1}^{p} c_j[\eta(\tau) - \eta_j(\tau)]\pi(\alpha_j) = 0.$$

Como $a \neq 0$ entonces existe algún $j > l$ tal que $c_j \neq 0$, entonces $\eta_j(\tau) = \eta(\tau)$, es decir α_j es un semi-invariante de peso η. Entonces tenemos $0 \neq C_K\left[G/H_0\right]_\eta \subset C_K\left[G\right]_\eta$. Hemos probado así, que $C_K\left[G\right]_\eta \neq 0$ para todo $\eta \in X(H)$ entonces $C_K\left[G\right]_{1/\chi} \neq 0$.

Como el grupo H actúa sobre el segundo factor de $\overline{K} \otimes_{C_K} C_K\left[G\right]$ tenemos que

$$\left(\overline{K} \otimes_{C_K} C_K\left[G\right]\right)_{1/\chi} = \overline{K} \otimes_{C_K} C_K\left[G\right]_{1/\chi} \neq 0.$$

Considerando el isomorfismo de $G-$módulos dado por la proposición 4.17 con acción restringida al subgrupo H. Como el grupo H actúa sobre ambos $\overline{K} \otimes_K T$ y $\overline{K} \otimes_{C_K} C_K[G]$ actuando sobre el segundo factor, se concluye que $\left(\overline{K} \otimes_K T\right)_{1/\chi} \neq 0$.

Ahora, si $t \in \overline{K} \otimes_K T$ entonces tenemos $t \in \widetilde{K} \otimes_K T$ para alguna extensión finita $\widetilde{K}$ de K. Podemos suponer que $K \subset \widetilde{K}$ es una extensión normal y tomamos $U = G(\widetilde{K}|K)$. Sea $t = \sum_{i=1}^{m} \widetilde{k_i} \otimes_K s_i \in (\widetilde{K} \otimes_K T)_{1/\chi}$, entonces

$$\tau(t) = (1/\chi)(\tau)t$$
$$\sum_{i=1}^{m} \widetilde{k_i} \otimes_K \tau(s_i) = \frac{1}{\chi(\tau)} \sum_{i=1}^{m} \widetilde{k_i} \otimes_K s_i. \tag{4.3.1}$$

Como H actúa sobre $\widetilde{K} \otimes_K T$ actuando en el factor de la derecha, U actúa sobre $\widetilde{K} \otimes_K T$ actuando en el factor de la izquierda, y ambas acciones conmutan, dado $\tau \in H$ tenemos:

$$\begin{aligned}
\tau(\sum_{\sigma \in U} \sigma(t)) &= \tau(\sum_{\sigma \in U} (\sum_{i=1}^{m} \sigma(\widetilde{k_i}) \otimes_K s_i)) \\
&= \sum_{\sigma \in U} (\sum_{i=1}^{m} \sigma(\widetilde{k_i}) \otimes_K \tau(s_i)) \\
&= \sum_{\sigma \in U} \sigma(\sum_{i=1}^{m} \widetilde{k_i} \otimes_K \tau(s_i)) \\
&= \sum_{\sigma \in U} \sigma(\frac{1}{\chi(\tau)} \sum_{i=1}^{m} \widetilde{k_i} \otimes_K s_i) \quad \text{por (4.3.1)} \\
&= \frac{1}{\chi(\tau)} \sum_{\sigma \in U} \sigma(\sum_{i=1}^{m} \widetilde{k_i} \otimes_K s_i) \\
&= \frac{1}{\chi(\tau)} \sum_{\sigma \in U} \sigma(t)
\end{aligned}$$

Entonces el elemento $\sum_{\sigma \in U} \sigma(t)$ es un semi-invariante con peso $1/\chi$. Observemos también que

$$\sum_{\sigma \in U} \sigma(t) = \sum_{\sigma \in U} (\sum_{i=1}^{m} \sigma(\widetilde{k_i}) \otimes_K s_i) = \sum_{i=1}^{m} (\sum_{\sigma \in U} \sigma(\widetilde{k_i})) \otimes_K s_i$$

y que $\sum_{\sigma \in U} \sigma(\widetilde{k_i}) \in \widetilde{K}^U = K$, entonces $\sum_{\sigma \in U} \sigma(t) \in K \otimes_K T \simeq T$. Así $T_{1/\chi} \neq 0$. $\square$

Proposición 4.27. *Sea $K \subset L$ una extensión de Picard-Vessiot y $G(L|K)$ su grupo de Galois diferencial. Si H es un subgrupo cerrado normal de $G(L|K)$ entonces la extensión $K \subset L^H$ es de Picard-Vessiot.*

Prueba. La prueba se sigue de la proposición 4.26 y el lema 4.25. □

Teorema 4.28 (Teorema Fundamental)**.** *Sea $K \subset L$ una extensión de Picard Vessiot y $G(L|K)$ su grupo de Galois diferencial.*

- *Las correspondencias*

$$H \mapsto L^H,\ F \mapsto G(L|F)$$

definen mapeos biyectivos mutuamente inversos que invierten la inclusión entre el conjunto de subgrupos Zariski cerrados H de $G(L|K)$ y el conjunto de cuerpos diferenciales F con $K \subset F \subset L$.

- *El cuerpo intermedio F es una extensión de Picard-Vessiot de K si y sólo si el subgrupo $H = G(L|F)$ es normal en $G(L|K)$.En este caso, el morfismo:*

$$G(L|K) \longrightarrow G(F|K)$$
$$\sigma \longmapsto \sigma_{|_F}$$

induce un isomorfismo: $G(L|K)/G(L|F) \simeq G(F|K)$

Prueba. Ahora las proposiciones 4.19, 4.22 y 4.27 establecen el teorema fundamental de la Teoria de Picard-Vessiot. □

Ejemplo 4.29. Para presentar este ejemplo, consideramos el cuerpo diferencial $\mathbb{C}(z)$ con la derivación usual $\dfrac{d}{dz}$. Probaremos que no existe un elemento $b \in \mathbb{C}(z)\setminus\{0\}$ ni un número $n \in \mathbb{Z}\setminus\{0\}$ tales que

$$b' = nzb$$

En efecto, si existiese $b = \dfrac{p(z)}{q(z)}$ que verifica $b' = nzb$ entonces

$$\frac{p(z)'q(z) - p(z)q(z)'}{q(z)^2} = \left(\frac{p(z)}{q(z)}\right)' = nz\frac{p(z)}{q(z)}$$

Sean $n = gr(p)$ y $m = gr(q)$ entonces

$$p(z)'q(z) - p(z)q(z)' = nzp(z)q(z)$$

donde el término de la izquierda tiene grado $r < mn$ y el término de la derecha tiene grado $nm + 1$, lo cual es una contradicción.

Consideremos el operador diferencial

$$\mathcal{L}(Y) = Y' - zY,$$

que no tiene solución en $\mathbb{C}(z)$.

Sabemos por este ejemplo 3.5 que $\mathbb{C}(z) \subset \mathbb{C}(e^{\frac{1}{2}z^2})$ es una extensión de Picard-Vessiot de $\mathbb{C}(z)$ para $\mathcal{L}$, cuyo grupo de Galois diferencial es el grupo multiplicativo

$$Gal_K(\mathcal{L}) =\simeq (\mathbb{C}^*, \cdot)$$

asi que hallaremos los subgrupos cerrados no triviales G de $\mathbb{C}^*$. Estos están dados por las raíces de una familia finita de polinomios

$$G = \left\{a \in \mathbb{C}^* : f_i(a) = 0, f_i(z) = z^{n_i} + a_{n_i-1}z^{n_i-1} + \cdots + a_0, i \in I \text{ finito}\right\}$$

Sabemos que cada polinomio $f_i(z)$ tiene n_i raíces en $\mathbb{C}$ (contando multiplicidad), así $|G| \leq min\{n_i : i \in I\}$, es decir G es un subgrupo finito de $\mathbb{C}^*$. Sea $|G| = n$, entonces por el teorema de Lagrange, todo $g \in G$ debe cumplir $g^n = 1$, luego cada subgrupo G debe ser de la forma

$$G = H_n = \left\{e^{2\pi i\frac{m}{n}} : m = 0, \ldots, n-1\right\}$$

Luego tenemos la relación entre los subgrupos cerrados de $\mathbb{C}^*$ y los cuerpos diferenciales intermedios de la extensión

$$\begin{array}{ccc}
\{1\} & \longrightarrow & L = \mathbb{C}(e^{\frac{1}{2}z^2}) \\
\big| & & \big| \\
H_n & \longrightarrow & L^{H_n} = \mathbb{C}(e^{\frac{n}{2}z^2}) \\
\big| & & \big| \\
Gal_K(\mathcal{L}) & \longrightarrow & K = \mathbb{C}(z)
\end{array}$$

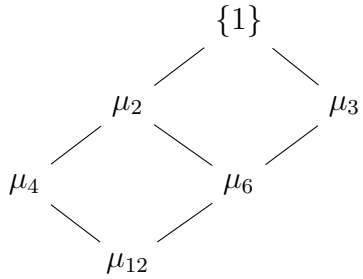
Ejemplo 4.30. Recordemos el ejemplo 4.10, donde $\mathbb{C}(z) \subset \mathbb{C}(z)\langle \sqrt[n]{z} \rangle$ es una extensión de Picard Vessiot, con grupo de Galois diferencial

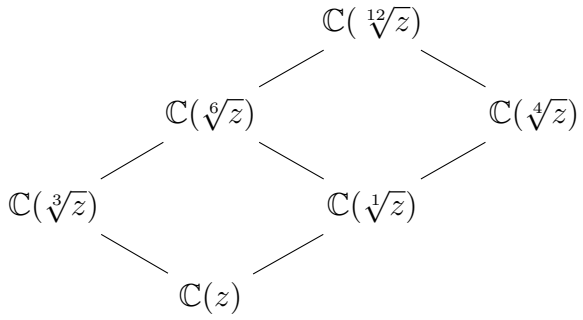
$$Gal_K(\mathcal{L}) \simeq \left\{ 1, e^{2\pi i \frac{1}{n}}, e^{2\pi i \frac{2}{n}}, \ldots, e^{2\pi i \frac{n-1}{n}} : c_{11}, c_{12} \in \mathbb{C}, c_{11}^2 + c_{12}^2 = 0 \right\}.$$

Luego tenemos la correspondencia

$$\begin{array}{ccc} \{1\} & \text{———} & L = \mathbb{C}(\sqrt[n]{z}) \\ | & & | \\ H_m & \text{———} & L^{H_n} = \mathbb{C}(\sqrt[n/m]{z}) \\ | & & | \\ Gal_K(\mathcal{L}) = H_n & \text{———} & K\mathbb{C}(z) \end{array}$$

Por ejemplo, si $n = 12$ tendremos





Conclusiones

1. Dado un cuerpo diferencial K, y una ecuación diferencial lineal homogénea,

$$\mathcal{L}(Y) = a_0 Y + a_1 Y' + \cdots + a_{n-1} Y^{(n-1)} + Y^{(n)} \tag{4.3.2}$$

   con coeficientes $a_i \in K$, siempre es posible asociarle la llamada extensión de Picard-Vessiot, que es la extensión $L = K\langle y_1, \ldots, y_n \rangle$ que satisface las condiciones de la definición 3.2. La extensión de Picard-Vessiot $K \subset L$ asociada a (4.3.2) es la análoga a la extensión de Galois de un polinomio en teoria de Galois clásica.

2. El teorema sobre la existencia de cuerpos de descomposición en teoria de Galois clásica tiene también su análogo en la versión diferencial. Para esto se debe satisfacer la condición de que el cuerpo de constantes de K debe ser algebraicamente cerrado (asumimos también que $\mathrm{char}(K) = 0$). Bajo esta hipótesis, siempre existe una extensión de Picard-Vessiot L de K y es única salvo automorfismos diferenciales.

3. En teoria de Galois clásica el grupo de Galois es un grupo de permutaciones entre las raices de un polinomio. En este trabajo, definimos el grupo de Galois diferencial de la ecuación (4.3.2) como el grupo de transformaciones de L que deja invariantes todas las relaciones entre los y_i y sus derivadas de todos los ordenes, por tanto se puede considerar como un grupo de simetrías internas de la ecuación (4.3.2), pero se tiene además que posee estructura de grupo algebraico lineal.

4. Finalmente, al igual que en la teoria clásica, se tiene una correspondencia entre los cuerpos diferenciales intermedios de una extensión de Picard-Vessiot $K \subset L$ y los subgrupos Zariski cerrados de su grupo de Galois diferencial $G(L|K)$.

Bibliografía

[1] Crespo, T. and Hajto, Z. (2007). Introduction to differential Galois Theory. Recuperado el 12 de Julio del 2018. `http://www2.im.uj.edu.pl/badania/preprinty/imuj2007/pr0711.pdf`

[2] Crespo, T. and Hajto, Z. (2011). *Algebraic Groups and Differential Galois Theory*. Graduate Studies in Mathematics, **122** American Mathematical Society. Providence, RI, xiv+225 pp.

[3] Humphreys, J. (2002). *Linear Algebraic Groups*. Revised third edition. Graduate Texts in Mathematics, **211**. Springer-Verlag, New York, 2002. xvi+914 pp. ISBN: 0-387-95385-X

[4] Kovacic, J. (2006). Existence of a Picard Vessiot extension. Recuperado el 25 de Enero del 2020. `http://ksda.ccny.cuny.edu/PostedPapers/existence.pdf`

[5] Lang, S. (2002). *Algebra*. Revised third edition. Graduate Texts in Mathematics, **211**. Springer-Verlag, New York, 2002. xvi+914 pp. ISBN: 0-387-95385-X

[6] Magid, A.R. (1994). *Lectures on Differential Galois Theory*. University Lecture Series, **7.** American Mathematical Society, Providence, RI, 1994. xiv+105 pp. ISBN: 0-8218-7004-1

[7] Morales Ruiz, J. (2011). *Hamilton y la Teoria de Galois.* Recuperado el 12 de Julio del 2018 de `https://www.researchgate.net/publication/39380078`

[8] Morales-Ruiz, J. y Ramis, J. (2001) Galoisian Obstructions to Integrability of Hamiltonian Systems. I Methods and Applications of Analysis,**8**, no 1, 33-96.

[9] Morales-Ruiz, J. , Ramis, J. y Simó, C. (2007) *Integrability of Hamiltonian Systems and Differential Galois Groups of Higher Variational Equations* Annales scientifiques de l.É.N.S., Série **4**, Tome 40, 1, 845-884.

[10] Picard, É. (1887) Sur les équations différentielles linéaires et les groupes algébriques de transformations Annales de la faculté des sciences de Tolouse 1.re série, tome 1, n.o 1, A1-A15.

[11] Seidenberg, A. (1956). *Contribution to the Picard-Vessiot theory of homogeneous linear differential equations.* Amer. J. Math. 78 (1956), 808-818. MR0081897 (18:463c)

[12] van der Put, M. y Singer, M.F. (1997). *Galois Theory of Difference Equations.* Lecture Notes in Mathematics, **1666.** Springer-Verlag, Berlin, 1997. viii+180 pp. ISBN: 3-540-63243-3

[13] Vessiot, E. (1892) Sur l'intégration des équations différentielles linéaires. Annales scientifiques de l.É.N.S.,3.e série, tome **9**, 197-280.

[14] Vessiot, E. (1946). Sur une théorie générale de la réductibilité des équations et systèmes d'équations finies ou différentielles. Annales scientifiques de l.É.N.S., 3.e série, tome **63**, 1-22.

[15] Vessiot, E. (1947). Sur la réductibilité des équations aux dérivées partielles du 1er ordre, à une inconnue, qui ne la contiennent pas et sont linéaires et homogénes par rapport à ses dérivées. Bulletin de la Société Mathématique de France, tome **75**, 9-26.