Universidad de Cantabria

Facultad de Ciencias

ANILLOS DE PICARD-VESSIOT

PICARD-VESSIOT RINGS

Trabajo de Fin de Grado
para acceder al

GRADO EN MATEMÁTICAS

Autora: Clara Gómez Blanco

Director: Jesús Javier Jiménez Garrido

Junio - 2025

AGRADECIMIENTOS

En primer lugar, quiero dar las gracias a todos los profesores que me han acompañado durante estos años de carrera. En especial, quiero mencionar a Javier, mi tutor de este trabajo de fin de grado. Gracias por tu orientación, por tu paciencia, tu dedicación y por ayudarme a dar forma a esta memoria, he aprendido mucho contigo.

Gracias a mi familia, mi pilar fundamental. Sois quienes primero se preocupan en los momentos complicados y quienes más se alegran cuando consigo mis objetivos. Este trabajo también es vuestro, porque siempre habéis estado ahí.

Quiero dedicárselo a mis abuelos Angelines, José María, Carmen y Emilio. Aunque seguramente a día de hoy no entiendan del todo qué es lo que he estudiado, sus sabias palabras, su cariño y sus ánimos han sido el mejor motor durante este camino. Y, especialmente, dedicárselo a mis padres, Inma y Emilio. Vuestros abrazos y vuestros consejos siempre me hacen sentir que todo es posible. Gracias a vosotros, me he convertido en la persona que soy hoy. Me siento muy afortunada de teneros.

A mis amigos de toda la vida, gracias por seguir a mi lado. Estudiar juntos en la biblioteca en época de exámenes ha sido más llevadero, y nuestros planes han sido la mejor desconexión.

También quiero agradecer a mi grupo de universidad y sobretodo, a mis amigas, sin vosotras esta etapa habría sido mucho más difícil. Habéis sido un apoyo constante, me he sentido comprendida, querida y acompañada. Solo espero que lo que la universidad ha unido no se separe nunca.

Y en especial, a mi novio Marcos, gracias por estar ahí siempre, por animarme cuando he dudado y por celebrar cada logro como si fuera tuyo. Eres lo mejor que me llevo de la universidad.

Gracias a todos.

RESUMEN

El objetivo principal del trabajo es el estudio de los anillos de Picard-Vessiot para introducir la teoría de Galois diferencial. Esta teoría puede considerarse una generalización de la teoría clásica de Galois, donde los cuerpos se sustituyen por cuerpos diferenciales y las ecuaciones polinómicas por ecuaciones diferenciales lineales.

A lo largo de la memoria se desarrolla, de forma progresiva, el marco necesario para construir una extensión del cuerpo base que contenga un sistema fundamental de soluciones de una ecuación diferencial, el anillo de Picard-Vessiot. Se empezará por los conceptos de anillos y cuerpos diferenciales, ecuaciones diferenciales lineales y posteriormente anillos y extensiones de Picard-Vessiot. El trabajo finaliza con el estudio del grupo de automorfismos del anillo de Picard-Vessiot que conmutan con la derivación, conocido como grupo de Galois diferencial, y se enunciará el Teorema Fundamental de la teoría de Galois diferencial.

Palabras clave: cuerpo diferencial, extensión diferencial, ecuación diferencial lineal, módulo diferencial, anillo de Picard-Vessiot, grupo de Galois diferencial, teoría diferencial de Galois.

ABSTRACT

The main objective of this final project is the study of Picard-Vessiot rings as a means to introduce differential Galois theory. This theory can be seen as a generalization of classical Galois theory, where fields are replaced by differential fields, and polynomial equations by linear differential equations.

Throughout the work, the necessary framework is progressively developed to construct an extension of the base field that contains a fundamental system of solutions of a differential equation, the Picard-Vessiot ring. It is started with the concepts of differential rings and fields, followed by linear differential equations, and then Picard-Vessiot rings and extensions. The project concludes with the study of the group of automorphisms of the Picard-Vessiot ring that commute with the derivation, known as the differential Galois group. The Fundamental Theorem of Differential Galois Theory will be stated.

Keywords: differential field, differential extension, linear differential equation, differential module, Picard-Vessiot ring, differential Galois group, differential Galois theory.

ÍNDICE

CAPÍTULO 1

INTRODUCCIÓN

Este trabajo tiene como objetivo introducir la teoría de Galois diferencial a través del estudio de los anillos de Picard-Vessiot. La teoría de Galois clásica trata de determinar cuando podemos expresar las soluciones de una ecuación polinomial en términos de operaciones elementales de los coeficientes. Para ello, se consideran los automorfismos del cuerpo de descomposición del polinomio, es decir, el cuerpo que contiene a todas las raíces que dejan invariantes al cuerpo de los coeficientes. Estos automorfismos forman un grupo que se denomina grupo de Galois de la ecuación polinomial. En el contexto diferencial, las extensiones de Picard-Vessiot cumplen el papel del cuerpo de descomposición en la teoría clásica.

La teoría de Picard-Vessiot se inicia a finales del siglo XIX con los trabajos de E.Picard [5] y su alumno E.Vessiot [9] sobre la existencia de la teoría de Galois aplicada al estudio de ecuaciones diferenciales lineales para el caso concreto del cuerpo de funciones racionales. En esta teoría, los cuerpos de la teoría clásica se sustituyen por cuerpos diferenciales, es decir, cuerpos equipados con una derivación que es una aplicación aditiva que cumple con la regla de Leibniz. La ecuación polinomial se sustituye por una ecuación diferencial lineal sobre un cuerpo diferencial K de tipo

$$y^{(n)} + a_{n-1}y^{(n-1)} + ... + a_1 y' + a_0 y = b,$$

con $b \in K$ y $a_i \in K$ para cada $i \in \{0, ..., n-1\}$. Resulta que el espacio de soluciones de esta ecuación tiene dimensión a lo sumo n sobre el subcuerpo de constantes, del mismo modo que un polinomio de grado n tiene a lo sumo n raíces en el cuerpo de coeficientes. Cuan-

do no hallamos suficientes soluciones en K buscamos ampliar este cuerpo para obtener una base del espacio de soluciones. El propósito de esta memoria es mostrar de manera detallada cómo se puede construir esta extensión de K que contiene a las soluciones de la ecuación, el anillo de Picard-Vessiot.

Para lograrlo, en el segundo capítulo introduciremos la noción de anillo y cuerpo diferencial y estudiaremos cómo extender las derivaciones a cocientes, localizaciones y extensiones algebraicas y trascendentes. Señalamos que salvo que se diga lo contrario siempre trabajaremos con anillos y cuerpos de característica cero, al final del segundo capítulo indicaremos brevemente los inconvenientes de trabajar en característica positiva.

En el tercer capítulo, presentamos el concepto de ecuación diferencial y su formulación en términos de sistemas lineales. Además, se introduce el concepto de módulo diferencial para estudiar propiedades de los sistemas sin depender de una base concreta lo que permite un enfoque más general y algebraico en el estudio de las soluciones.

En el cuarto capítulo se recogen los resultados centrales del trabajo. Destacamos que una diferencia clave respecto a la teoría clásica es que, al añadir soluciones de una ecuación diferencial, lo que se obtiene no es necesariamente un cuerpo, sino un anillo diferencial. Para garantizar la minimalidad de este anillo será necesario introducir la noción de anillo diferencial simple y probar las propiedades básicas. Con ello, demostraremos la existencia y unicidad de los anillos de Picard-Vessiot. Estos anillos resultan ser dominios por lo que podremos considerar su cuerpo de fracciones que denominamos extensión de Picard-Vessiot. Concluimos el capítulo y la memoria estudiando el grupo de automorfismos para esta extensión que conmutan con la derivación, el grupo diferencial de Galois. A diferencia de lo que ocurre en la teoría clásica donde el grupo de Galois de una ecuación polinomial es siempre finito, en el estudio de las ecuaciones diferenciales los grupos que aparecen pueden ser grupos infinitos. Finalmente enunciaremos, sin demostrar, la correspondencia de Galois a este contexto.

Para la elaboración del texto se han seguido dos fuentes fundamentales [6] y [8], completando los detalles de los razonamientos y realizando las demostraciones de los resultados auxiliares que se encuentran planteados como ejercicios en estas referencias.

CAPÍTULO 2

ANILLOS Y CUERPOS DIFERENCIALES

En este capítulo se presentarán los conceptos fundamentales relacionados con la teoría de anillos y cuerpos diferenciales. En particular, se abordarán las nociones de anillo de constantes, se estudiará bajo qué condiciones se puede extender la derivación a un anillo cociente o a un anillo localizado de nuestro anillo original. Con esta información analizaremos qué ocurre con la derivación para las extensiones algebraicas y trascendentes de cuerpos en la última sección.

> Todos los anillos y cuerpos considerados en este capítulo se suponen conmutativos, con un elemento unidad y de característica 0, o equivalentemente, que contienen a $\mathbb{Q}$ como subcuerpo.

Al final del capítulo ilustraremos con algunos ejemplos y resultados los problemas que aparecen cuando se quiere trasladar esta teoría a cuerpos de característica positiva.

2.1. Anillos y cuerpos diferenciales

En la sección que sigue, se presentarán la definición de anillo y cuerpo diferencial, junto con una serie de ejemplos ilustrativos.

Definición 2.1. Sea R un anillo y $\partial : R \to R$ una aplicación. Decimos que ∂ es una **derivación** si para todos $a, b \in R$ se cumple que

1. **Homomorfismo entre grupos aditivos**: $\partial(a+b) = \partial(a) + \partial(b)$.

2. **Regla del producto o regla de Leibniz**: $\partial(ab) = \partial(a)b + a\partial(b)$.

Un anillo R equipado con una derivación se llama **anillo diferencial**, y en el caso de que el anillo sea cuerpo diremos que es un **cuerpo diferencial**. Dado un anillo diferencial R, decimos que un anillo diferencial S es una **extensión diferencial** de R si R es subanillo de S y la derivación de S restringida a R coincide con la derivación de R.

Ejemplo 2.2. Los siguientes son anillos diferenciales:

1. Cualquier anillo R con **derivación trivial**, es decir, $\partial = 0$.

2. Dado un anillo diferencial (R, ∂) y $x \in R$, la aplicación $\tilde{\partial}(a) = x \cdot \partial(a)$ para cada $a \in R$ es también una derivación sobre R.

3. Dado un anillo R consideramos la derivación usual sobre el conjunto de series de potencias formales $R[[X]]$ dada por $\partial(\sum_{k=0}^{\infty} a_k X^k) = \sum_{k=1}^{\infty} k a_k X^{k-1}$. Se tiene que $(R[[x]], \partial)$ es un anillo diferencial y en particular el anillo de polinomios $(R[x], \partial)$ también.

4. Dado (R, ∂) un anillo diferencial con derivación $a' := \partial(a)$ para cada $a \in R$. Se define el **anillo de polinomios diferenciales en** $y_1, \ldots, y_n$ **sobre** R, denotado por $R\{\{y_1, \ldots, y_n\}\}$, de la siguiente manera: para cada $i \in \{1, 2, \ldots, n\}$ y cada $j \in \mathbb{N}$, se considera la indeterminada $y_i^{(j)}$ y definimos $R\{\{y_1, \ldots, y_n\}\}$ como el anillo de polinomios

$$R[y_1^{(0)}, y_1^{(1)}, y_1^{(2)}, \ldots, y_2^{(0)}, y_2^{(1)}, y_2^{(2)}, \ldots, y_n^{(0)}, y_n^{(1)}, y_n^{(2)}, \ldots].$$

   Obsérvese que este anillo no es noetheriano.
   Extendemos la derivación de R a una derivación en $R\{\{y_1, \ldots, y_n\}\}$ estableciendo $(y_i^{(j)})' = y_i^{(j+1)}$. Por simplicidad, escribiremos y_i para $y_i^{(0)}$, y_i' para $y_i^{(1)}$ y así sucesivamente. Cuando $n = 1$, dado $P \in R\{\{y\}\}$ decimos que P tiene **orden** n si n es el menor natural tal que $P \in R[y, y', ..., y^{(n)}]$.

5. El anillo $\mathscr{C}^\infty(\mathbb{R})$ de las funciones indefinidamente derivables sobre R con la derivada usual es un anillo diferencial que no es un dominio. Por otro lado, el anillo de las funciones enteras $\mathscr{H}(\mathbb{C})$ es un dominio diferencial por el Principio de los Ceros Aislados.

Presentamos también ejemplos de cuerpos diferenciales que emplearemos a lo largo de la memoria. Los resultados de la Sección 2.3 garantizarán que estos ejemplos son efectivamente cuerpos diferenciales.

Ejemplo 2.3. Sea C un cuerpo, los siguientes son cuerpos diferenciales.

1. Dado un cuerpo C, tenemos que el cuerpo de fracciones racionales $C(z)$ tiene estructura de cuerpo diferencial con la derivación usual $\partial(f) = \frac{\partial f}{\partial z}$.

2. El cuerpo $C((z))$ de series de Laurent formales sobre C se construyen como el cuerpo de fracciones del anillo de series de potencias formales $C[[z]]$ y sus elementos admiten una representación en la forma

$$f(z) = \sum_{n=n_0}^{\infty} a_n z^n,$$

con $n_0 \in \mathbb{Z}$, es decir, con una cantidad finita de términos de exponente negativo y con $a_n \in C$ para cada $n \geq n_0$. Tenemos que $C((z))$ es un cuerpo diferencial con la derivación usual definida sobre cada monomio.

3. Si $C = \mathbb{C}$, dentro del cuerpo de series de Laurent formales $\mathbb{C}((z))$ podemos considerar el subcuerpo de las series de Laurent convergentes $\mathbb{C}(\{z\})$ en un entorno punteado del origen que es también un cuerpo diferencial para la restricción de la derivación.

4. El cuerpo de todas las funciones meromorfas en cualquier subconjunto abierto conexo del plano complejo extendido $\mathbb{C} \cup \{\infty\}$ es un cuerpo diferencial con la derivación usual. Este cuerpo incluye todas las funciones definidas que son holomorfas en dicho abierto excepto en un número finito de puntos donde tiene polos.

Definición 2.4. Sean (R_1, ∂_1) y (R_2, ∂_2) dos anillos diferenciales y $\phi : R_1 \rightarrowtail R_2$ un homomorfismo de anillos. Decimos que ϕ **es diferencial** si para todo elemento $v \in R_1$ se tiene que $\phi(\partial_1(v)) = \partial_2(\phi(v))$.

Continuando con el Ejemplo 2.2, podemos generalizar la noción de evaluar polinomios al anillo de polinomios diferenciales.

Definición 2.5. Sean (R, ∂) un anillo diferencial, S una extensión diferencial de R y los elementos $u_1, u_2, ..., u_n \in S$. Definimos el **homomorfismo de evaluación de polinomios diferenciales en** $u_1, ..., u_n$ como el homomorfismo $\phi : R\{\{y_1, \ldots, y_n\}\} \rightarrow S$ diferencial R-lineal que para cada $i \in \{1, 2, \ldots, n\}$ y cada $j \in \mathbb{N}$, cumple que $\phi(y_i^{(j)}) = u_i^{(j)}$. Denotamos a la imagen de P por ϕ como $P(u_1, u_2, ..., u_n)$.

Ejemplo 2.6. En relación con la Definición 2.5, tomando $R = S = C(z)$ y $\phi : C(z)\{\{y\}\} \rightarrow C(z)$ dado por $\phi(y) = z^2$, luego $\phi(y') = 2z$, $\phi(y'') = 2$ y $\phi(y^{(n)}) = 0$ para $n \in \mathbb{N}$ con $n \geq 3$, tenemos que el polinomio diferencial $P(y) = y - \frac{1}{2} z y'$ cumple que $P(z^2) = 0$.

2.2. Anillo de constantes

En esta sección vamos a introducir el concepto de conjunto de constantes de un anillo diferencial.

Definición 2.7. Sea (R,∂) un anillo diferencial y $c \in R$. Decimos que c es una **constante** si $\partial(c) = 0$. Se define el conjunto de constantes por $C = \{c \in R | \partial(c) = 0\}$.

Observación 2.8. En el Ejemplo 2.2, se observa que el conjunto de constantes es todo R en el primer caso. En el segundo caso, el conjunto de constantes podría contener nuevas constantes si x es un divisor de cero. En el tercero y el cuarto, es simplemente el conjunto de constantes del cuerpo base R. En el último, se corresponde con las funciones constantes.

Por otro lado, en los dos primeros casos del Ejemplo 2.3, el conjunto de constantes es simplemente el cuerpo base C, mientras que en los dos últimos se corresponde con las funciones constantes.

En todos los casos observamos que el conjunto de constantes de un anillo es un anillo y el de un cuerpo es un cuerpo. Este es un hecho general como veremos a continuación.

Proposición 2.9. *Sea (R,∂) un anillo diferencial. Entonces el conjunto de constantes C es un subanillo de R.*

Demostración. Dados $c_1, c_2 \in C$ como ∂ es un homomorfismo de grupos tenemos que $\partial(c_1 - c_2) = \partial(c_1) + \partial(-c_2) = \partial(c_1) - \partial(c_2) = 0 - 0 = 0$. Por lo tanto, se tiene que $c_1 - c_2 \in C$. Por otro lado, empleando la regla de Leibniz se cumple que

$$\partial(c_1 \cdot c_2) = \partial(c_1) \cdot c_2 + c_1 \cdot \partial(c_2) = 0 + 0 = 0,$$

luego $c_1 \cdot c_2 \in C$. Finalmente, también tenemos que $\partial(1) = \partial(1 \cdot 1) = 2\partial(1)$, por la regla de Leibniz, luego se tiene que $\partial(1) = 0$ porque $car(R) \neq 2$ y deducimos que $1 \in C$. ■

Para probar que el anillo de constantes de un cuerpo diferencial es también un cuerpo necesitamos usar la siguiente fórmula para calcular la derivada de un cociente.

Proposición 2.10. *Sea (R,∂) un anillo diferencial $t, s \in R$ tales que s es una unidad, es decir, $s \in R^*$. Entonces se cumple que*

$$\partial\left(\frac{t}{s}\right) = \frac{\partial(t)s - t\partial(s)}{s^2}. \tag{2.1}$$

Demostración. En primer lugar, empleando la regla de Leibniz, por la Proposición 2.9, se tiene que 1 es una constante y observamos que

$$0 = \partial(1) = \partial\left(\frac{1}{s}\cdot s\right) = \partial\left(\frac{1}{s}\right)\cdot s + \frac{1}{s}\cdot\partial(s),$$

luego $\partial(1/s) = -\partial(s)/s^2$. Aplicando de nuevo la regla de Leibniz tenemos que

$$\partial\left(\frac{t}{s}\right) = \partial(t)\cdot\frac{1}{s} + t\cdot\partial\left(\frac{1}{s}\right) = \partial(t)\cdot\frac{1}{s}\cdot\left(-\frac{\partial(s)}{s^2}\right)\cdot t = \frac{\partial(t)s - t\partial(s)}{s^2}.$$

■

Corolario 2.11. *Sea (R,∂) un cuerpo diferencial entonces el conjunto de constantes C es un cuerpo.*

Demostración. Por la Proposición 2.9, sabemos que C es un subanillo de R, dado $c \in C$, $c \neq 0$, veamos que $c^{-1} \in C$ para concluir que es un subcuerpo. Empleando la fórmula (2.1) tenemos que $\partial(c^{-1}) = -\partial(c)/c^2 = 0$ y concluimos que $c^{-1} \in C$. ■

En particular, se tiene que $car(C) = car(R) = 0$ luego $\mathbb{Q}$ es un subcuerpo de C.

2.3. Cociente y localización de un anillo diferencial

En esta sección vamos a estudiar bajo qué condiciones la derivación de un anillo diferencial induce una derivación sobre los anillos cocientes o los anillos localizados. Comenzamos caracterizando los ideales que producen anillos cociente diferenciales.

Teorema 2.12. *Sean (R,∂) un anillo diferencial e $I \subset R$ un ideal, entonces la correspondencia*

$$\begin{aligned}\tilde{\partial} : R/I &\to R/I\\ a + I &\to \partial(a) + I,\end{aligned}$$

define una derivación sobre R/I si y solo si $\partial(I) \subset I$.

Demostración. En primer lugar, supongamos que $\tilde{\partial}$ es una derivación. Tomamos $x \in I$, tenemos que $\partial(x) + I = \tilde{\partial}(x + I) = \tilde{\partial}(0 + I) = \partial(0) + I = 0 + I$, luego $\partial(x) \in I$, es decir, $\partial(I) \subset I$. Recíprocamente, si suponemos que $\partial(I) \subset I$, para cada $x \in I$ tenemos que

$$\pi_I(\partial(x)) = \partial(x) + I = 0_{R/I},$$

donde $\pi_I : R \to R/I$ es la aplicación de paso al cociente. Por tanto, se tiene que $I \subset \ker(\pi_I \circ \partial)$ y podemos aplicar la Propiedad Universal del grupo cociente para deducir que existe un único homomorfismo de grupos $\tilde{\partial} : R/I \to R/I$ tal que $\tilde{\partial}(a+I) = \pi_I(\partial(a)) = \partial(a) + I$. Para concluir solo debemos comprobar que $\tilde{\partial}$ cumple la regla de Leibniz. Dados $a, b \in R$, se tiene que

$$\begin{aligned}\tilde{\partial}((a+I)(b+I)) = \tilde{\partial}(ab+I) = \partial(ab) + I = (\partial(a)b + a\partial(b)) + I = \partial(a)b + a\partial(b) + I \\ = (\partial(a)+I)(b+I) + (a+I)(\partial(b)+I) = \tilde{\partial}(a+I)(b+I) + (a+I)\tilde{\partial}(b+I).\end{aligned}$$

■

Observamos que para verificar la condición $\partial(I) \subset I$ basta comprobar que se cumple para los generadores de I.

Proposición 2.13. *Sean (R, ∂) un anillo diferencial e $I \subset R$ un ideal generado por $\{a_j\}_{j\in J}$. Si $\partial(a_j) \in I$ para cada $j \in J$, entonces $\partial(I) \subset I$.*

Demostración. Tomamos $a \in I$, como I está generado por $\{a_j\}_{j\in J}$ tenemos que a se puede escribir como $a = \sum_{k=1}^{m} r_k a_{j_k}$, para algunos $r_k \in R$ y a_{j_k} generadores de I. Aplicamos ∂ a a utilizando la regla de Leibniz

$$\partial(a) = \partial\left(\sum_{k=1}^{m} r_k a_{j_k}\right) = \sum_{k=1}^{m} (\partial(r_k) a_{j_k} + r_k \partial(a_{j_k})).$$

Como por hipótesis $\partial(a_{j_k}) \in I$, tenemos que $r_k\partial(a_{j_k}) \in I$ y como $a_{j_k} \in I$, $\partial(r_k)a_{j_k} \in I$. Por tanto, cada uno de los sumandos de la expresión anterior pertenece a I, luego $\partial(a) \in I$ y concluimos que $\partial(I) \subset I$. ■

Recordamos que decimos que un subconjunto S de R es **multiplicativamente cerrado** si $1_R \in S$ y si para todos $s_1, s_2 \in S$ se tiene que $s_1 \cdot s_2 \in S$. El **anillo localizado de R respecto a S** se construye considerando el conjunto de clases de equivalencia definido sobre $R \times S$ por la relación $(r_1, s_1) \sim (r_2, s_2)$ si y solo si existe un $s_3 \in S$ tal que $s_3(r_1 s_2 - r_2 s_1) = 0$. El símbolo r/s denota la clase de equivalencia del par (r, s) y el conjunto de clases se denota por $S^{-1}R$. A continuación, veamos cuando podemos extender una derivación de R a $S^{-1}R$. Un ejemplo de este tipo de construcción es el cuerpo de fracciones de un dominio D tomando $R = D$ y $S = D^*$.

Teorema 2.14. *Sean (R,∂) un anillo diferencial y $S \subset R$ un conjunto multiplicativamente cerrado. Entonces la correspondencia*

$$\begin{aligned} \tilde{\partial} : S^{-1}R &\to S^{-1}R \\ \frac{r}{s} &\mapsto \frac{\partial(r)s - r\partial(s)}{s^2}, \end{aligned}$$

define una derivación sobre $S^{-1}R$ y es la única que cumple que $\tilde{\partial}(r) = \partial(r)$ para cada $r \in R$.

Demostración. En primer lugar, demostraremos que $\tilde{\partial}$ está bien definida. Supongamos que $r_1/s_1 = r_2/s_2$. Por definición de la relación de equivalencia, existe un elemento $s_3 \in S$ tal que $s_3(r_1s_2 - r_2s_1) = 0$. Aplicamos la derivación ∂ a ambos lados de esta igualdad y usamos la regla de Leibniz en el anillo R

$$0 = \partial[s_3(r_1s_2 - r_2s_1)] = \partial(s_3)(r_1s_2 - r_2s_1) + s_3[\partial(r_1)s_2 + r_1\partial(s_2) - \partial(r_2)s_1 - r_2\partial(s_1)].$$

Para simplificar notación, llamamos $B = \partial(r_1)s_2 + r_1\partial(s_2) - \partial(r_2)s_1 - r_2\partial(s_1)$.
Multiplicamos la igualdad anterior por $s_3s_1s_2$, lo que anula el primer término, debido a que $s_3(r_1s_2 - r_2s_1) = 0$, y obtenemos $s_3^2Bs_1s_2 = 0$.
Queremos ver que las imágenes por la derivada $\tilde{\partial}$ de r_1/s_1 y r_2/s_2 son iguales. Aplicamos entonces la fórmula de $\tilde{\partial}$ a cada fracción y restamos

$$\tilde{\partial}\left(\frac{r_1}{s_1}\right) - \tilde{\partial}\left(\frac{r_2}{s_2}\right) = \frac{\partial(r_1)s_1 - r_1\partial(s_1)}{s_1^2} - \frac{\partial(r_2)s_2 - r_2\partial(s_2)}{s_2^2}.$$

Operando el numerador de la fracción, vemos que

$$[\partial(r_1)s_1 - r_1\partial(s_1)]s_2^2 - [\partial(r_2)s_2 - r_2\partial(s_2)]s_1^2 = B\,s_1\,s_2 + (r_2s_1 - r_1s_2)\,(s_1\partial(s_2) + s_2\partial(s_1)).$$

Multiplicamos esta expresión por $s_3^2 \in S$, obteniendo que el segundo término se anula, ya que contiene el factor $r_2s_1 - r_1s_2$, y por hipótesis eso es 0. Por ello, la expresión se reduce a

$$s_3^2\left([\partial(r_1)s_1 - r_1\partial(s_1)]s_2^2 - [\partial(r_2)s_2 - r_2\partial(s_2)]s_1^2\right) = s_3^2B\,s_1\,s_2.$$

Comprobamos entonces que el resultado anterior es 0 debido a que $s_3^2B\,s_1\,s_2$ lo era. Así, se concluye que

$$s_3^2\left(\tilde{\partial}\left(\frac{r_1}{s_1}\right) - \tilde{\partial}\left(\frac{r_2}{s_2}\right)\right) = 0.$$

Por tanto, tomando $s_4 = s_3^2 \in S$, se cumple la condición de igualdad en el anillo localizado porque las imágenes de r_1/s_1 y r_2/s_2 bajo $\tilde{\partial}$ coinciden en $S^{-1}R$, lo que prueba que $\tilde{\partial}$ está

bien definida.
Veamos que cumple las propiedades de una derivación

$$\tilde{\partial}\left(\frac{r_1}{s_1}+\frac{r_2}{s_2}\right)=\tilde{\partial}\left(\frac{r_1s_2+r_2s_1}{s_1s_2}\right)=\frac{\partial(r_1s_2+r_2s_1)s_1s_2-(r_1s_2+r_2s_1)\partial(s_1s_2)}{s_1^2s_2^2}.$$

Aplicando las propiedades de ∂ por ser derivación se obtiene

$$\tilde{\partial}\left(\frac{r_1}{s_1}+\frac{r_2}{s_2}\right)=\frac{[\partial(r_1)s_2+\partial(s_2)r_1+s_1\partial(r_2)+r_2\partial(s_1)]s_1s_2-(r_1s_2+r_2s_1)[\partial(s_1)s_2+s_1\partial(s_2)]}{s_1^2s_2^2},$$

y operando,

$$\tilde{\partial}\left(\frac{r_1}{s_1}+\frac{r_2}{s_2}\right)=\frac{\partial(r_1)s_1s_2^2-r_1\partial(s_1)s_2^2}{s_1^2s_2^2}+\frac{\partial(r_2)s_2s_1^2-r_2\partial(s_2)s_1^2}{s_1^2s_2^2}=\tilde{\partial}\left(\frac{r_1}{s_1}\right)+\tilde{\partial}\left(\frac{r_2}{s_2}\right).$$

Veamos que satisface la regla de Leibniz

$$\tilde{\partial}\left(\frac{r_1}{s_1}\frac{r_2}{s_2}\right)=\frac{[\partial(r_1)r_2+r_1\partial(r_2)]s_1s_2-(r_1r_2)[\partial(s_1)s_2+s_1\partial(s_2)]}{s_1^2s_2^2}.$$

Reagrupando se tiene que

$$\tilde{\partial}\left(\frac{r_1}{s_1}\frac{r_2}{s_2}\right)=\frac{[\partial(r_1)s_1-r_1\partial(s_1)]r_2}{s_1^2s_2}+\frac{r_1[r_2\partial(s_2)-s_2\partial(r_2)]}{s_1s_2^2}=\tilde{\partial}\left(\frac{r_1}{s_1}\right)\frac{r_2}{s_2}+\tilde{\partial}\left(\frac{r_2}{s_2}\right)\frac{r_1}{s_1}.$$

Por último, la unicidad de $\tilde{\partial}$ está garantizada por (2.1). ■

Observación 2.15. Sea (R,∂) un anillo diferencial, $r\in R$ y $n\in\mathbb{N}$ con $n\geq 1$. Por inducción, probamos

$$\partial(r^n)=nr^{n-1}\partial(r). \tag{2.2}$$

Veamos que podemos generalizar el resultado del teorema anterior y extender la derivación al localizado sobre un anillo de polinomios, asignando adicionalmente cualquier valor prefijado para las derivadas de las indeterminadas.

Teorema 2.16. *Sean (R,∂) un anillo diferencial y $a_1,a_2,...,a_n\in R[X_1,X_2,...,X_n]$. Entonces tenemos que existe una única derivación $\tilde{\partial}$ sobre $R[X_1,X_2,...,X_n]$ tal que $\tilde{\partial}(r)=\partial(r)$ para cada $r\in R$ y tal que para cada $i\in\{1,2,...,n\}$, $\tilde{\partial}(X_i)=a_i$.*

Demostración. Comenzamos probando la unicidad y obteniendo una fórmula para la derivación que emplearemos para probar la existencia. Tomamos un polinomio cualquiera

$f(X_1,\dots,X_n)=\sum_\alpha c_\alpha X^\alpha \in R[X_1,...,X_n]$ donde empleamos la notación usual de multíndices, es decir, $\alpha=(\alpha_1,\alpha_2,\dots,\alpha_n)\in\mathbb{N}^n$ y $X^\alpha = X_1^{\alpha_1}X_2^{\alpha_2}\cdots X_n^{\alpha_n}$. La derivación $\tilde{\partial}$ que queremos definir debe extender a ∂. Además, $\tilde{\partial}$ es lineal lo que nos permite escribir

$$\tilde{\partial}(f)=\sum_\alpha \tilde{\partial}(c_\alpha X^\alpha)=\sum_\alpha \left(\tilde{\partial}(c_\alpha)X^\alpha + c_\alpha\tilde{\partial}(X^\alpha)\right).$$

Como queremos que $\tilde{\partial}(c_\alpha)=\partial(c_\alpha)$, la primera parte de la suma debería ser igual a $\sum_\alpha \partial(c_\alpha)X^\alpha$. Para calcular $\tilde{\partial}(X^\alpha)$, usamos la regla de Leibniz reiteradamente como en (2.2) obteniendo que

$$\tilde{\partial}(X^\alpha)=\sum_{i=1}^n \alpha_i X_1^{\alpha_1}\cdots X_i^{\alpha_i-1}\cdots X_n^{\alpha_n}\tilde{\partial}(X_i).$$

Como debemos imponer que $\tilde{\partial}(X_i)=a_i$ tenemos que $\tilde{\partial}(X^\alpha)=\sum_{i=1}^n a_i\alpha_i X^{\alpha-e_i}$, donde $X^{\alpha-e_i}$ representa el monomio $X_1^{\alpha_1}\cdots X_i^{\alpha_i-1}\cdots X_n^{\alpha_n}$. Por lo tanto, se debe cumplir que

$$\tilde{\partial}(f)=\sum_\alpha\left(\partial(c_\alpha)X^\alpha + c_\alpha\sum_{i=1}^n a_i\alpha_i X^{\alpha-e_i}\right). \tag{2.3}$$

La ecuación (2.3) garantiza la unicidad de $\tilde{\partial}$ y para probar la existencia debemos verificar que $\tilde{\partial}$ define una derivación. Esto se hace comprobando primero la propiedad sobre monomios y luego extendiendo por linealidad e inducción al número de términos, asegurando que cumple la regla de Leibniz. ■

Para concluir esta sección veamos que podemos extender la derivación directamente a un localizado del anillo de polinomios.

Teorema 2.17. *Sea (R,∂) un anillo diferencial y $S\subset R[X_1,X_2,...,X_n]$ un conjunto multiplicativamente cerrado. Dados $a_1,a_2,...,a_n\in S^{-1}(R[X_1,X_2,...,X_n])$ tenemos que existe una única derivación $\tilde{\partial}$ sobre $S^{-1}(R[X_1,X_2,...,X_n])$ tal que $\tilde{\partial}(r)=\partial(r)$ para cada $r\in R$ y tal que para cada $i\in\{1,2,...,n\}$, $\tilde{\partial}(X_i)=a_i$.*

Demostración. Escribimos $a_i=P_i/Q_i$ con $P_i\in R[X_1,...,X_n]$ y $Q_i\in S$ y consideramos en el anillo $A=R[X_1,...,X_n,T_1,...,T_n]$ el ideal $I=(1-T_1Q_1,...,1-T_nQ_n)$. Usando el Teorema 2.16 extendemos ∂ a una derivación única ∂_A en A tal que $\partial_A(X_i)=P_iT_i$ y $\partial_A(T_i)=-T_i^2\partial_A(Q_i)$ para cada $i\in\{1,...n\}$. Por el Teorema 2.12, ∂_A induce de forma única una derivación $\partial_{A/I}$ en A/I puesto que para cada $i\in\{1,...,n\}$ se tiene que

$$\partial_A(1-T_iQ_i)=-Q_i(-T_i^2\partial_A(Q_i))-T_i\partial_A(Q_i)=\partial_A(Q_i)T_i(1-Q_iT_i)\in I.$$

Denotamos por $\tilde{S}$ a la imagen de S en A/I. Por el Teorema 2.14, extendemos la derivación de forma única a una derivación $\tilde{\partial}$ en $\tilde{S}^{-1}A/I$. Empleando la propiedad universal de la localización de anillos se tiene que $S^{-1}R[X_1,...,X_n]$ es isomorfo a $\tilde{S}^{-1}A/I$ y vemos que

$$\tilde{\partial}(X_i+I) = \partial_{A/I}(X_i+I) = \partial_A(X_i)+I = P_iT_i+I.$$

Observando que la imagen de a_i por el isomorfismo es P_iT_i+I concluimos que tenemos una derivación en $S^{-1}R[X_1,...,X_n]$ que cumple con lo requerido. ■

2.4. Extensiones de cuerpos y derivaciones

En esta sección vamos a ver cómo se comporta la derivación para extensiones de cuerpos. En primer lugar, veamos que para extensiones trascendentes podemos extender la derivación libremente asignando el valor que deseemos a la derivada de un elemento trascendente, empleando los resultados de la sección anterior.

Corolario 2.18. *Sean (F,∂) un cuerpo diferencial, $F(X)$ una extensión trascendental de F y un elemento $a \in F(X)$. Entonces existe una única derivación $\tilde{\partial}$ sobre $F(X)$, que extiende a ∂, tal que $\tilde{\partial}(X) = a$.*

Demostración. Basta aplicar el Teorema 2.17 para $R = F$, $n = 1$, $S = F[X]\setminus\{0\}$ y $a_1 = a$ puesto que $F(X) = S^{-1}(R[X])$. ■

Para obtener propiedades sobre las extensiones algebraicas es fundamental que la característica de F sea 0.

Proposición 2.19. *Sean (F,∂) un cuerpo diferencial, (K,∂) un cuerpo extensión diferencial de F y $a \in K$ tal que a es algebraico sobre F. Entonces a es algebraico sobre el cuerpo de constantes si y solo si $\partial(a) = 0$.*

Demostración. Supongamos que a es algebraico sobre C, el cuerpo de constantes, y consideramos $P(X) = X^n + c_{n-1}X^{n-1} + \cdots + c_0$, su polinomio mínimo en $C[X]$. Evaluando en a, $P(a) = 0$ y derivando vemos que

$$0 = \partial(P(a)) = \partial(a^n + c_{n-1}a^{n-1} + \cdots + c_1a + c_0).$$

Como para cada $i \in \{1,2,...,n\}$, c_i es constante empleando (2.2) se tiene que

$$\partial(c_ia^i) = a^i\partial(c_i) + c_i\partial(a^i) = c_i\,i\,a^{i-1}\partial(a).$$

Por lo tanto, sacando factor común se cumple que

$$0 = \partial(a)(c_n n a^{n-1} + (n-1)c_{n-1}a^{n-2} + \cdots + c_1).$$

Como K es un cuerpo, alguno de los dos factores debe ser nulo. Dado que $P(X)$ es el polinomio mínimo de a, si el factor de la derecha fuera nulo tendríamos que

$$Q(X) = c_n n X^{n-1} + (n-1)c_{n-1}X^{n-2} + \cdots + c_1,$$

sería un polinomio de $C[X]$ no nulo, porque la característica de F y de C es 0, de grado menor que n, lo que es imposible. En consecuencia, se tiene que $\partial(a) = 0$.

Recíprocamente, suponemos que $\partial(a) = 0$. Como a es algebraico sobre F consideramos $P(X) = X^n + f_{n-1}X^{n-1} + ... + f_1 X + f_0$ el polinomio mínimo y mónico en $F[X]$. Evaluando en a y derivando vemos que

$$0 = \partial(P(a)) = \partial(a^n + f_{n-1}a^{n-1} + ... + f_1 a + f_0).$$

Empleando (2.2), como $\partial(a) = 0$ tenemos que $\partial(a^k) = 0$ para todo $k \in \{1, 2, ..., n\}$. Por tanto, sustituyendo, vemos que

$$0 = \partial(f_{n-1})a^{n-1} + ... + \partial(f_1)a + \partial(f_0).$$

Si alguno de los coeficientes f_i no es una constante, tendríamos un polinomio de $F[X]$ de grado menor que n que anularía a a contradiciendo que $P(X)$ es el polinomio mínimo. Por tanto, para cada $i \in \{0, 1, 2, ..., n-1\}$ se tiene que $\partial(f_i) = 0$, luego $P(X) \in C[X]$, es decir, a es algebraico sobre C. ■

Recordamos que el Teorema del Elemento Primitivo que podemos encontrar en [3], establece que dado F un cuerpo de característica 0, y dados a y b elementos algebraicos sobre F. Entonces, existe un elemento $c \in F(a, b)$ tal que $F(a, b) = F(c)$. Empleando este resultado, probamos que la derivación se extiende de forma única a una extensión finita.

Teorema 2.20. *Sean (F, ∂) un cuerpo diferencial y $\tilde{F}$ una extensión finita de F. Entonces ∂ tiene una única extensión a $\tilde{F}$.*

Demostración. Por el Teorema del Elemento Primitivo, existe $a \in F$ tal que $\tilde{F} = F(a)$ porque la característica de F es cero. Denotamos por $P(X) = X^n + f_{n-1}X^{n-1} + ... + f_1 X + f_0$ al polinomio mínimo de a sobre F. La prueba se divide en dos partes: en primer lugar, queremos extender ∂ a una derivación $\bar{\partial}$ sobre $F[X]$ aplicando el Teorema 2.16 y dicha derivación debe cumplir que $\bar{\partial}(P(X)) \in (P(X))$ para poder garantizar que, en segundo lugar, podamos

aplicar el Teorema 2.12 para obtener una derivación sobre $F[X]/(P(X)) \simeq F(a)$.
Comenzamos extendiendo la derivación a $F[X]$, para ello aplicamos el Teorema 2.16 para $R = F, n = 1$ y $\bar{\partial}(X) = Q(X)$, donde debemos elegir adecuadamente $Q(X)$ para que se cumpla que $\bar{\partial}(P(X)) \in (P(X))$. Comenzamos calculando $\bar{\partial}(P(X))$ en función de la derivada $\bar{\partial}(X) = Q(X)$. Aplicando la linealidad de la derivación y la regla de Leibniz, escribiendo $f_n = 1$ se tiene que

$$\bar{\partial}(P(X)) = \bar{\partial}(X^n + f_{n-1}X^{n-1} + \cdots + f_0) = \sum_{k=0}^{n} \bar{\partial}(f_k X^k) = \sum_{k=0}^{n} \bar{\partial}(f_k)X^k + \sum_{k=0}^{n} f_k \bar{\partial}(X^k).$$

Usando que $\bar{\partial}(f_i) = \partial(f_i)$ para cada $i \in \{0, 1, 2, ..., n\}$ y la ecuación (2.2) tenemos que

$$\bar{\partial}(P(X)) = \sum_{k=0}^{n} X^k \partial(f_k) + \sum_{k=0}^{n} f_k k X^{k-1} Q(X).$$

Si denotamos por d/dX la derivación usual en $F[X]$, tenemos que:

$$\bar{\partial}(P(X)) = \sum_{k=0}^{n} \partial(f_k)X^k + Q(X)\frac{d}{dX}(P).$$

Para hallar $Q(X)$ observamos que, como $P(X)$ es el polinomio mínimo de a, entonces para un $R(x) \in F[x]$ se tiene que $R(X) \in (P(X))$ si y solo si $R(a) = 0$. Por tanto, debe cumplirse que

$$\sum_{k=0}^{n} \partial(f_k)a^k + Q(a) \cdot \frac{d}{dX}(P(a)) = 0.$$

Como $P(X)$ es el polinomio mínimo de a, y la característica de F es cero $\frac{dP}{dX}(a) \neq 0$ y podemos despejar. En consecuencia, $\bar{\partial}(P(X)) \in (P(X))$ si y solo si

$$Q(a) = \frac{-\sum_{k=0}^{n} \partial(f_k)a^k}{\frac{dP}{dX}(a)}. \tag{2.4}$$

Como este valor al que llamaremos b está en $F(a)$, existen $q_0, q_1, \ldots, q_{n-1} \in F$ tal que escribimos $b = q_0 + q_1 a + \cdots + q_{n-1}a^{n-1}$, luego basta tomar $Q(X) = q_0 + q_1 X + \cdots + q_{n-1}X^{n-1}$.

En resumen, aplicando el Teorema 2.16, por esta elección de $Q(X)$ tenemos una derivación $\bar{\partial}$ sobre $F[X]$ que extiende a ∂, y que cumple que $\bar{\partial}(P(X)) \in (P(X))$. Finalmente, aplicando el Teorema 2.12, obtenemos una derivación $\tilde{\partial}$ sobre $F(a) = F[X]/(P(X))$ inducida por $\bar{\partial}$ que extiende a ∂.
Como $\bar{\partial}$ induce una única derivación $\tilde{\partial}$ sobre $F(a)$, para comprobar que $\tilde{\partial}$ es única basta comprobar que el valor de $\tilde{\partial}(a)$ es independiente del polinomio $Q(X)$ que hayamos elegido para construir $\bar{\partial}$. Como $P(a) = 0$, operando como antes, observamos que

$$0 = \tilde{\partial}(P(a)) = \tilde{\partial}\left(\sum_{k=0}^{n} f_k a^k\right) = \sum_{k=0}^{n} \tilde{\partial}(f_k)a^k + \tilde{\partial}(a)\frac{dP}{dX}(a).$$

Como $\tilde{\partial}$ extiende a ∂ se tiene que $\tilde{\partial}(a) = b = Q(a)$, luego $\tilde{\partial}$ no depende de la elección del polinomio Q, solo depende del valor de b, y por lo tanto, $\tilde{\partial}$ es única. ■

Como consecuencia del teorema anterior vemos que la derivación se extiende de forma única a cualquier extensión algebraica y en particular, a la clausura algebraica.

Corolario 2.21. *Sea (F,∂) un cuerpo diferencial y $\tilde{F}$ una extensión algebraica de F. Entonces ∂ tiene una única extensión a $\tilde{F}$.*

Demostración. La unicidad está garantizada porque por el teorema anterior el valor de la extensión de la derivación en $a \in \tilde{F}$ está determinado por la ecuación (2.4).
Para probar la existencia consideramos el conjunto

$$\sum := \left\{(K,\partial_K) \mid F \subset K \subset \tilde{F},\ (K,\partial_K) \text{ es una extensión diferencial de } (F,\partial)\right\}.$$

Observamos que $\sum \neq \emptyset$ porque $(F,\partial) \in \sum$. Dada una cadena de $\sum$, $\{(K_i,\partial_i)\}_{i\in I}$, consideramos (K,D) dada por $K = \cup_{i\in I} K_i$ y derivada $D(a) = \partial_i(a)$ para cada $a \in K_i$. Comprobamos que (K,D) es una extensión diferencial de (F,∂) y que es una cota superior de la cadena $\{(K_i,\partial_i)\}_{i\in I}$. Por tanto, por el lema de Zorn, se tiene que existe (K_{max},∂_{max}) un elemento maximal de $\sum$.
Si existiera un elemento $a \in \tilde{F} \setminus K_{max}$ aplicando el teorema anterior podríamos extender ∂_{max} a $K_{max}(a)$, contradiciendo la maximalidad. Por tanto, $K_{max} = \tilde{F}$ y tenemos que la derivación se extiende a $\tilde{F}$. ■

Observamos que los resultados del Teorema 2.20 y el Corolario 2.21 son falsos en general si F tiene característica $p > 0$.

Ejemplo 2.22. Consideramos X un elemento trascendente sobre $\mathbb{F}_p$, el cuerpo con p elementos, y la extensión algebraica de cuerpos $\mathbb{F}_p(X^p) \subset \mathbb{F}_p(X) \simeq \mathbb{F}_p(X^p)[T]/(T^p - X^p)$. Consideramos ∂ la derivación trivial sobre $\mathbb{F}_p(X^p)$. Para extender ∂ a una derivación $\tilde{\partial}$ en $\mathbb{F}_p(X)$ se requiere que $\tilde{\partial}$ coincida con ∂ en $\mathbb{F}_p(X^p)$. Para ello debe cumplir que $\tilde{\partial}(X^p) = 0$. Pero por la ecuación (2.2) $\tilde{\partial}(X^p) = pX^{p-1}\tilde{\partial}(X)$, luego la ecuación $\tilde{\partial}(X^p) = 0$ se satisface automáticamente, sin importar el valor que se asigne a $\tilde{\partial}(X)$. Por lo tanto, se puede elegir $\tilde{\partial}(X)$ arbitrariamente en $\mathbb{F}_p(X)$ perdiendo así la unicidad.

Concluimos el capítulo observando que algunas cuestiones son más simples en característica positiva dado que los cuerpos perfectos solo admiten la derivación trivial.

Teorema 2.23. *Sea F un cuerpo perfecto de característica $p > 0$, es decir, $F = F^p$. Entonces, toda derivación sobre F es la derivación trivial.*

Demostración. Supongamos que ∂ es una derivación sobre F. Consideremos un elemento $b \in F$, por ser F cuerpo perfecto existe $a \in F$ tal que $b = a^p$. Usamos (2.2) para calcular $\partial(a^p)$ y obtenemos que $\partial(b) = \partial(a)(pa^{p-1})$. Se cumple que $\partial(b) = 0$ porque $\text{car}(F) = p$. Esto significa que la derivación ∂ es la derivación nula sobre F. ■

Más generalmente, se obtiene el siguiente resultado.

Teorema 2.24. *Sea F un cuerpo de característica $p > 0$ tal que $[F : F^p] = p$. Entonces toda derivación $\partial : F \to F$ es de la forma $\partial = g \cdot \frac{d}{dz}$ para un único $g \in F$, donde $\frac{d}{dz}$ se define mediante la fórmula:*

$$\frac{d}{dz}\left(\sum_{i=0}^{p-1} a_i z^i\right) := \sum_{i=1}^{p-1} i\, a_i z^{i-1}, \quad \text{con } a_i \in F^p.$$

Demostración. Como $[F : F^p] = p$, el cuerpo F tiene dimensión finita p sobre su subcuerpo de potencias p-ésimas F^p. Dado que la extensión es de grado p, existe un elemento $z \in F \setminus F^p$ tal que $\{1, z, z^2, \ldots, z^{p-1}\}$ es una base de F como F^p-espacio vectorial. Dada una derivación sobre $\partial : F \to F$ y dado $b \in F^p$ se tiene que existe un $a \in F$ tal que $b = a^p$ luego $\partial(b) = \partial(a^p) = 0$. Por tanto, ∂ es F^p-lineal y queda determinada por la imagen de la base $\{1, z, z^2, \ldots, z^{p-1}\}$. Por (2.2) deducimos que ∂ está determinada por $\partial(z)$ y se tiene que

$$\partial\left(\sum_{i=0}^{p-1} a_i z^i\right) = \sum_{i=0}^{p-1} a_i\, \partial(z^i) = \partial(z) \sum_{i=1}^{p-1} a_i \cdot i z^{i-1}.$$

Para concluir se comprueba que para todo $g \in F$ tomando $\partial(z) = g$ la fórmula anterior define una derivación.

■

CAPÍTULO 3

ECUACIONES DIFERENCIALES LINEALES

En este capítulo vamos a introducir tres formas equivalentes de estudiar las ecuaciones diferenciales lineales, veremos como pasar de una formulación a otra y describiremos sus propiedades fundamentales. En particular, probaremos que el conjunto de soluciones forma un espacio vectorial sobre el cuerpo de constantes cuya dimensión está acotada por el orden de la ecuación. El estudio de las soluciones de las ecuaciones diferenciales lineales se corresponde con el estudio de las raíces de los polinomios diferenciales de grado 1 de $K\{\{y\}\}$, ver Ejemplo 2.2. Concluimos el capítulo probando las propiedades fundamentales del Wronskiano que nos permitirán demostrar el Teorema de Ritt que garantiza que todo polinomio no nulo define una función polinomial no nula.

A lo largo de este capítulo, K denotará un cuerpo diferencial con $car(K) = 0$, cuerpo de constantes C y la derivada de un elemento $a \in K$ se denotará por a'.

3.1. Ecuaciones diferenciales lineales

Definición 3.1. Una **ecuación diferencial lineal (escalar y ordinaria)** de orden $n \in \mathbb{N}$ sobre K es una ecuación de la forma

$$y^{(n)} + a_{n-1}y^{(n-1)} + \cdots + a_1 y' + a_0 y = b,$$

con $b \in K$ y $a_i \in K$ para cada $i \in \{0, 1, ..., n-1\}$. Una ecuación de este tipo se dice **homogénea** si $b = 0$ y en caso contrario, se dice **no homogénea**.

Por simplicidad, escribimos

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

Una solución de una ecuación $L(y) = b$ en una extensión diferencial $R \supset K$ es un elemento $f \in R$ tal que

$$f^{(n)} + a_{n-1}f^{(n-1)} + \cdots + a_1 f' + a_0 f = b.$$

Observamos que también se puede entender como una raíz en R del polinomio diferencial $L(y) - b \in K\{\{y\}\}$. Veamos que la búsqueda de soluciones de ecuaciones no homogéneas de orden n se puede reducir al estudio de las soluciones de ecuaciones homogéneas de orden $n+1$.

Proposición 3.2. *Dada una ecuación diferencial no homogénea de orden n sobre K, $L(y) = b$ con $b \neq 0$, consideramos*

$$L_h(y) = b\left(\frac{1}{b}L(y)\right)'.$$

Entonces cualquier solución de $L(y) = b$ es una solución de $L_h(y) = 0$. Recíprocamente, para cualquier solución v de $L_h(y) = 0$ existe una constante c de K tal que v es una solución de $L(y) = cb$.

Demostración. Suponemos que f es una solución de $L(y) = b$. Sustituyendo en la expresión de $L_h(y)$ vemos que

$$L_h(f) = b\left(\frac{1}{b}b\right)',$$

y simplificando $L_h(f) = b \cdot (1)'$. Finalmente, por la Proposición 2.9, 1 es una constante y se cumple que $L_h(f) = 0$.

Recíprocamente, si suponemos que $L_h(v) = 0$ tenemos que

$$b\left(\frac{1}{b}L(v)\right)' = 0.$$

Dividiendo por $b \neq 0$, vemos que $(L(v)/b)' = 0$. Esto significa que $L(v)/b$ es una constante que denotamos por c. De forma que v es una solución de la ecuación $L(y) = cb$. ■

Concluimos esta sección con algunos ejemplos que nos muestran que no siempre podemos encontrar solución en K, ni en la clausura algebraica de K de ecuaciones diferenciales sencillas.

Ejemplo 3.3. Dado C un cuerpo algebraicamente cerrado de característica 0. Consideramos la derivación usual sobre el cuerpo $K = C((z))$ de las series de Laurent sobre C.

1. Dado $a \in K$ con $a \neq 0$ consideramos la ecuación $y' = a$. Como $a \neq 0$, $a = \sum_{n=n_0}^{\infty} a_n z^n$ con $n_0 \in \mathbb{Z}$ y $a_{n_0} \neq 0$. Buscamos soluciones de esta ecuación en K. Empleamos el método de Frobenius. Consideramos una serie de Laurent cualquiera $y(z) = \sum_{m=m_0}^{\infty} y_m z^m$ con $m_0 \in \mathbb{Z}$ e $y_m \in C$ para cada $m \geq m_0$. Entonces se tiene que $y'(z) = \sum_{m=m_0}^{\infty} m y_m z^{m-1}$, sustituyendo en la ecuación e igualando obtenemos que

$$\sum_{n=m_0-1}^{\infty} (n+1) y_{n+1} z^n = \sum_{n=n_0}^{\infty} a_n z^n,$$

comparando los coeficientes de z^n vemos que $(n+1)y_{n+1} = a_n$ para todo $n \in \mathbb{Z}$.

En particular, para $n = -1$ se tiene que $0 \cdot y_0 = a_{-1}$ y para $n \neq -1$, $y_{n+1} = a_n/(n+1)$, luego la ecuación tiene solución en K si y solo si $a_{-1} = 0$, es decir, si $a(z)$ no tiene término en z^{-1}.

Podríamos plantearnos si en el caso $a_{-1} \neq 0$ la ecuación tiene solución en la clausura algebraica de K. Recordamos que la clausura algebraica de K está dada por las series de Puisseux con coeficientes en C y cada extensión algebraica finita de K tiene la forma $C((z^{1/n}))$. Tomando $y(z) \in \bar{K}$ una cuenta similar nos permite concluir que hay solución en $\bar{K}$ si y solo si $a_{-1} = 0$.

Esta ecuación nos muestra en general que debemos de considerar extensiones de K más allá del cierre algebraico de K, es decir, extensiones trascendentes como las que construiremos en el capítulo siguiente.

2. Dado $a \in K$ con $a \neq 0$ consideramos la ecuación $y' = ay$ con la misma notación. Desarrollamos el producto

$$a(z)y(z) = \sum_{n=n_0+m_0}^{\infty} \left(\sum_{k=n_0}^{n-m_0} a_k y_{n-k} \right) z^n,$$

y de nuevo, aplicando el método de Frobenius tenemos que comparando los coeficientes de z^n para cada n obtenemos que

$$(n+1)y_{n+1} = \sum_{k=n_0}^{n-m_0} a_k y_{n-k}.$$

En particular, mirando el término de menor orden correspondiente a $n = n_0 + m_0$, tenemos que $(n_0 + m_0 + 1)y_{n_0+m_0+1} = a_{n_0} y_{m_0}$ y distinguimos tres casos:

- Si $n_0 < -1$ entonces vemos que $(n_0 + m_0 + 1) < m_0$ y por tanto, $a_{n_0} y_{m_0} = 0$, lo cual es absurdo porque sabemos que por hipótesis $y_{m_0} \neq 0$ y $a_{n_0} \neq 0$.

- Si $n_0 = -1$ se tiene que $a_{-1} = m_0$ entonces necesariamente se tiene que $a_{-1} \in \mathbb{Z}$. Veamos que esta condición es suficiente. En este caso, si miramos el término $n = m_0$ observamos que $(m_0+1)y_{m_0+1} = m_0 y_{m_0+1} + a_0 y_{m_0}$. Por consiguiente, $y_{m_0+1} = a_0 y_{m_0}$. Supongamos que y_{m_0+r} con $r \geq 1$ se puede expresar en términos de una cantidad finita de coeficientes de $a(z)$ y los elementos y_k con $k < m_0+r$ y veamos que ocurre lo mismo para el elemento y_{m_0+r+1}. Como $n_0 = -1$ tenemos que

$$(m_0+r+1)y_{m_0+r+1} = \sum_{k=-1}^{r} a_k y_{m_0+r-k} = m_0 y_{m_0+r+1} \sum_{k=0}^{r} a_k y_{m_0+r-k}.$$

  Como se puede despejar el término y_{m_0+r+1} porque $r+1 \neq 0$ aplicando la hipótesis de inducción concluimos que también se cumple nuestra hipótesis para y_{m_0+r+1}.

- Si $n_0 > -1$ entonces el producto empieza en un grado mayor que la derivada porque $(n_0+m_0) > m_0 - 1$ y se obtiene que $m_0 y_{m_0} = 0$ lo cual indica que hay dos opciones o que $y_{m_0} = 0$ que es absurdo como antes o que $m_0 = 0$ condición necesaria para que exista solución. Razonando por inducción como en el caso anterior se prueba que esta condición necesaria es suficiente, los detalles se muestran en una situación más general en el Ejemplo 3.10.

Si nos planteamos que pasa en el caso $a_{-1} \notin \mathbb{Z}$, la ecuación puede tener solución en la clausura algebraica de K. Tomando $y(z) \in \bar{K}$ una cuenta similar nos permite concluir que hay solución en $\bar{K}$ si y solo si $a_{-1} \in \mathbb{Q}$.

3.2. Sistemas de ecuaciones diferenciales lineales

Al igual que ocurre en la teoría clásica de ecuaciones diferenciales ordinarias podemos estudiar las ecuaciones diferenciales lineales de orden n por medio de sistemas de ecuaciones diferenciales. En esta sección vamos a introducir los sistemas de ecuaciones diferenciales (ordinarias homogéneas de primer orden). Vamos a probar algunas propiedades fundamentales de estos sistemas y veremos que existe una correspondencia entre sistemas de primer orden y las ecuaciones diferenciales lineales.

Para poder considerar los sistemas, extendemos la derivación de K a los vectores de K^n y a las matrices en $M_n(K)$ mediante la derivación componente a componente. Así, para un vector $y = (y_1, ..., y_n)^T \in K^n$ y $A = (a_{ij}) \in M_n(K)$, se escribe $y' = (y_1', ..., y_n')^T$ y $A' = (a_{ij}')$.

Vamos a estudiar sistemas de la forma

$$y' = Ay,$$

donde $A \in M_n(K)$ y tratamos de buscar soluciones $y = (y_1, ..., y_n) \in K^n$ o en alguna extensión de K.

Comenzamos probando algunas propiedades que relacionan la derivación con el producto de matrices.

Proposición 3.4. *Sean $A \in M_{m\times n}(K)$, $B \in M_{n\times l}(K)$, $P \in GL_n(K)$. Entonces*

(I) $(AB)' = A'B + BA'$.

(II) $(P^{-1})' = -P^{-1}P'P^{-1}$.

Demostración. (I) Se demuestra directamente usando la definición del producto de matrices y la regla de Leibniz.

(II) Como $PP^{-1} = Id$, donde Id es la matriz identidad. Derivamos ambos lados de esta ecuación $(PP^{-1})' = Id'$, como Id es constante, su derivada es cero y usando el apartado (I), $P'P^{-1} + P(P^{-1})' = 0$. Despejamos $(P^{-1})'$ obteniendo que $P(P^{-1})' = -P'P^{-1}$. Finalmente, multiplicamos por P^{-1} por la izquierda $(P^{-1})' = -P^{-1}P'P^{-1}$. ■

Estas fórmulas nos permiten describir como se transforma un sistema de ecuaciones diferenciales lineales cuando cambiamos de base.

Proposición 3.5. *Dada $A \in M_n(K)$ y $P \in GL_n(K)$. Tenemos que $y \in M_{n\times 1}(K)$ cumple la ecuación $y' = Ay$ si y solo si $\tilde{y} = P^{-1}y$ cumple la ecuación $\tilde{y}' = \tilde{A}\tilde{y}$ con $\tilde{A} = P^{-1}AP - P^{-1}P'$.*

Demostración. Observamos que $\tilde{y}' = (P^{-1}y)' = P^{-1}y' + (P^{-1})'y$. Sustituyendo $y' = Ay$ tenemos que $\tilde{y}' = (P^{-1}A + (P^{-1})')y$. Como $(P^{-1})' = -P^{-1}P'P^{-1}$ e $y = P\tilde{y}$ obtenemos que $\tilde{y}' = (P^{-1}AP - P^{-1}P')\tilde{y}$. Recíprocamente, con una cuenta similar, si $\tilde{y}$ es solución de $\tilde{y}' = \tilde{A}y$, entonces $y = P\tilde{y}$ es solución de $y' = Ay$. ■

Por tanto, dos ecuaciones diferenciales matriciales dadas por las matrices A y $\tilde{A}$ se dicen **equivalentes** si existe un $P \in \mathrm{GL}_n(K)$ tal que $\tilde{A} = P^{-1}AP - P^{-1}P'$. Obviamente, si los vectores $v_1, ..., v_r \in K^n$ son linealmente dependientes sobre el cuerpo de constantes también lo son sobre K. Cuando estos vectores son solución de un sistema, el recíproco es cierto.

Lema 3.6. *Sea $A \in M_n(K)$ y consideremos el sistema*

$$y' = Ay.$$

Suponemos que $v_1, \ldots, v_r \in K^n$ soluciones, es decir, $v_i' = Av_i$ para todo $i \in \{1,2,...,r\}$. Si los vectores $v_1, \ldots, v_r \in V$ son linealmente dependientes sobre K, entonces también son linealmente dependientes sobre C, el cuerpo de constantes de K.

Demostración. El lema se demuestra por inducción en r. Para el caso base $r = 1$, el resultado es trivial. Un solo vector es linealmente dependiente si y solo si, es el vector cero, lo cual es igual tanto sobre K como sobre C.
Supongamos que el resultado es cierto para conjuntos de menos de r vectores y que los vectores $v_1, \ldots, v_r$ son linealmente dependientes sobre K. Por hipótesis inductiva, podemos suponer que cualquier subconjunto propio de $\{v_1, \ldots, v_r\}$ es linealmente independiente sobre K porque en caso contrario, tendríamos un conjunto de menos de r vectores linealmente dependientes sobre K y por hipótesis de inducción, $\{v_1, \ldots, v_r\}$ serían también linealmente dependientes sobre C.

Sin pérdida de generalidad, podemos suponer que

$$v_1 = \sum_{i=2}^{r} a_i v_i,$$

donde $a_i \in K$ para cada $i \in \{2, \ldots, r\}$. Como v_1 es solución del sistema operando se tiene que

$$0 = v_1' - Av_1 = \sum_{i=2}^{r} a_i' v_i + \sum_{i=2}^{r} a_i (v_i' - Av_i).$$

Como para cada $i \in \{1,2,...,n\}$, v_i es solución, $0 = \sum_{i=2}^{r} a_i' v_i$ y como $v_2, ..., v_r$ son linealmente independientes sobre K, entonces para cada $i \in \{1,2,...,r\}$, $a_i' = 0$ luego $a_i \in C$. ■

En consecuencia, para encontrar la mayor cantidad de soluciones linealmente independientes sobre K, basta buscar que sean linealmente independientes sobre C.

Lema 3.7. *Dada la ecuación matricial*

$$y' = Ay,$$

con $A \in M_n(K)$. El espacio de soluciones V de $y' = Ay$ en K^n está definido como

$$V = \{v \in K^n \mid v' = Av\}.$$

Entonces, V es un espacio vectorial sobre C de dimensión menor o igual que n.

Demostración. Se comprueba de forma directa que V es un espacio vectorial sobre C. La cota para la dimensión se deduce del Lema 3.6, ya que cualquier conjunto de $n+1$ vectores en V son linealmente dependientes sobre K y por ello sobre C. ■

Si la dimensión del espacio de soluciones $V \subset K^n$ sobre C es n, es decir, $\dim_C(V) = n$ y tomamos una base $v_1, v_2, ..., v_n$ de V, entonces la matriz $B \in \mathrm{GL}_n(K)$ cuyas columnas son los vectores $v_1, v_2, ..., v_n$ cumple que $B' = AB$.

Como muestran los ejemplos de la Sección 3.1 en general la dimensión de V no es n y debemos buscar las soluciones en alguna extensión de K lo que nos lleva a considerar la siguiente definición.

Definición 3.8. Sea K un cuerpo diferencial, $A \in \mathrm{GL}_n(K)$ y R un anillo diferencial extensión de K. Decimos que $F \in \mathrm{GL}_n(R)$ es una **matriz fundamental** para la ecuación $y' = Ay$ si $F' = AF$.

La siguiente proposición muestra que dos matrices fundamentales de una misma ecuación están relacionadas.

Proposición 3.9. *Sea K un cuerpo diferencial, $A \in GL_n(K)$, R el anillo diferencial extensión de K con cuerpo de constantes C y $F \in GL_n(R)$ una matriz fundamental de la ecuación $y' = Ay$. Entonces $\tilde{F} \in GL_n(R)$ es otra matriz fundamental de la ecuación si y solo si $F^{-1}\tilde{F} \in GL_n(C)$, es decir, $\tilde{F} \in F \cdot GL_n(C)$.*

Demostración. Suponemos que $\tilde{F}$ es una matriz fundamental. Definimos $M = F^{-1}\tilde{F}$. Tenemos que

$$A\tilde{F} = \tilde{F}' = (FM)' = F'M + FM' = AFM + FM' = A\tilde{F} + FM'.$$

Por tanto, se tiene que $FM' = 0$ y como $F \in \mathrm{GL}_n(R)$ deducimos que $M' = 0$.
Recíprocamente, si $M \in \mathrm{GL}_n(C)$, operando de la misma forma, vemos que

$$\tilde{F}' = (FM)' = A\tilde{F} + FM' = A\tilde{F},$$

luego $\tilde{F}$ es otra matriz fundamental. ■

Como muestra el siguiente ejemplo para el anillo de series de potencias formales con la derivación usual (ver Ejemplo 2.2), podemos garantizar que siempre existe una matriz fundamental en dicho anillo y que sobre el cuerpo de series de Laurent podemos encontrar una matriz fundamental si y solo si el sistema es equivalente a un sistema sobre el anillo de series de potencias formales.

Ejemplo 3.10. Dada $A \in M_n(C[[z]])$ con C un cuerpo cualquiera tenemos que la ecuación $y' = Ay$ tiene una única matriz fundamental de la forma

$$B(z) = Id + \sum_{n=1}^{\infty} B_n z^n, \quad B_n \in M_n(C).$$

Para probar esta afirmación empleamos el método de Frobenius, es decir, sustituimos $B(z)$ en la ecuación $B'(z) = A(z)B(z)$ que debe cumplir toda matriz fundamental y obtenemos

$$\sum_{n=1}^{\infty} nB_n z^{n-1} = \left(\sum_{n=0}^{\infty} A_n z^n\right)\left(Id + \sum_{n=1}^{\infty} B_n z^n\right).$$

Igualamos los términos de mismo orden en z de ambos lados de la ecuación obteniendo el siguiente sistema de ecuaciones matriciales para los coeficientes de $B(z)$

$$(n+1)B_{n+1} = A_n + \sum_{m=0}^{n-1} A_m B_{n-m}, \quad \text{para } n \geq 0.$$

Para $n = 0$ tenemos que $B_1 = A_0$ y por inducción probamos que podemos calcular los coeficientes de $B(z)$ a partir de los coeficientes de $A(z)$, lo que garantiza la existencia y unicidad de la matriz fundamental en la forma buscada. Además, por la Observación 2.8 como el conjunto de constantes de $C[[z]]$ es C podemos garantizar que toda matriz fundamental tiene la forma $B(z)M$ con $M \in \mathrm{GL}_n(C)$.

Por otra parte, si consideramos una ecuación sobre el cuerpo de las series de Laurent, ver Ejemplo 2.3, es decir, $y' = Ay$ con la matriz $A \in M_n(C((z)))$, entonces hay una matriz fundamental de la ecuación en $\mathrm{GL}_n(C((z)))$ si y solo si el sistema es equivalente a un sistema $\tilde{y}' = \tilde{A}\tilde{y}$ con $\tilde{A} \in M_n(C[[z]])$. Para ver que se cumple esta equivalencia, consideramos la transformación $\tilde{y} = P^{-1}y$, para alguna matriz $P \in \mathrm{GL}_n(C[[z]])$. Por la Proposición 3.9, se tiene que $\tilde{A} = P^{-1}AP - P^{-1}P'$. Si $\tilde{A} \in M_n(C[[z]])$ por lo que hemos probado previamente, $\tilde{y}' = \tilde{A}\tilde{y}$ tiene una única matriz fundamental de la forma $\tilde{B}(z) = Id + \sum_{n=1}^{\infty} \tilde{B}_n z^n$, luego $P(z)\tilde{B}(z) \in M_n(C[[z]])$ es una matriz fundamental de $y' = Ay$ porque

$$\begin{aligned}(P\tilde{B})' &= P'\tilde{B} + P\tilde{B}' = P'\tilde{B} + P\tilde{A}\tilde{B} = P'\tilde{B} + P(P^{-1}AP - P^{-1}P')\tilde{B} \\ &= P'\tilde{B} + AP\tilde{B} - P'\tilde{B} = A(P\tilde{B}).\end{aligned}$$

Recíprocamente, si tenemos una matriz fundamental $F \in M_n(C((z)))$ de $y' = Ay$, tomamos $P = F$ e $\bar{y} = F^{-1}y$ tenemos que

$$\tilde{A} = F^{-1}AF - F^{-1}F' = F^{-1}F' - F^{-1}F' = 0,$$

luego el sistema es equivalente a $\tilde{y}' = 0$.

Tras establecer las propiedades fundamentales de los sistemas de ecuaciones diferenciales, observamos que hay una forma estándar de producir una ecuación diferencial matricial $y' = A_L y$ a partir de una ecuación diferencial escalar lineal homogénea

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

La matriz compañera A_L de L se define por

$$A_L = \begin{pmatrix} 0 & 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 1 \\ -a_0 & -a_1 & \cdots & \cdots & \cdots & -a_{n-1} \end{pmatrix}.$$

Se verifica fácilmente que esta matriz compañera tiene la siguiente propiedad: para cualquier extensión de anillos diferenciales $R \supset K$, la aplicación $y \to (y, y', \ldots, y^{(n-1)})^T$ es un isomorfismo del espacio de soluciones $\{y \in R \mid L(y) = 0\}$ de L al espacio de soluciones de $\{y \in R^n \mid y' = A_L y\}$ de la ecuación diferencial matricial $y' = A_L y$. En general, sabemos que el recíproco no es cierto, no toda matriz A puede transformarse mediante un cambio de base $P^{-1}AP - P^{-1}P'$ en la matriz compañera de un polinomio.

Ejemplo 3.11. Si K es un cuerpo con la derivación trivial el cambio de base solo produce matrices semejantes a A, luego la matriz Id_n con $n \geq 2$, que solo es semejante a si misma, no puede transformarse en la matriz compañera de un polinomio L.

Sin embargo, si el cuerpo K contiene algún elemento no constante, sí es posible encontrar un cambio de base $P^{-1}AP - P^{-1}P'$ que transforme A en la matriz compañera de un polinomio. Para probar este hecho, necesitamos garantizar la existencia de un vector cíclico. Existen diversas demostraciones de este teorema, ver [2] y [6, Capítulo 2]. Enunciamos el resultado aunque no entraremos en detalle sobre su demostración.

Teorema 3.12. *Sea K un cuerpo diferencial tal que existe $a \in K$ con $a' \neq 0$. Dado un sistema $y' = Ay$ con $A \in M_n(K)$. Entonces el sistema es equivalente a un sistema $y' = A_L y$ asociado a una ecuación escalar $L(y) = 0$.*

En otras palabras, se puede considerar una ecuación diferencial escalar como un caso especial de una ecuación diferencial matricial y si la derivación es no trivial entonces ambas formulaciones son equivalentes. Por lo tanto, el Lema 3.7 se aplica también para ecuaciones escalares homogéneas.

Lema 3.13. *Consideremos una ecuación escalar homogénea de orden n, $L(y) = 0$, sobre K. El espacio de soluciones V de $L(y) = 0$ en K se define como $V = \{v \in K \mid L(v) = 0\}$. Entonces, V es un espacio vectorial sobre C de dimensión menor o igual que n.*

3.3. Módulos diferenciales

Los módulos diferenciales nos proporcionan una forma alternativa de interpretar los sistemas de ecuaciones diferenciales. Esta forma es independiente de la elección de bases, lo que es útil tanto desde el punto de vista teórico como desde el punto de vista práctico, dado que si sabemos que una propiedad depende del módulo diferencial podemos escoger la base en la que realizar los cálculos.

Definición 3.14. Un **módulo diferencial** (M, ∂) (o simplemente M) de dimensión n es un espacio vectorial de dimensión n sobre K, equipado con un homomorfismo entre los grupos aditivos $\partial : M \to M$ que para todo $f \in K$ y todo $m \in M$ cumple que

$$\partial(fm) = f'm + f\partial(m).$$

Un módulo diferencial de dimensión uno tiene la forma $M = Ke$ y la aplicación ∂ está completamente determinada por el valor de $\partial(e)$. De hecho, como $\partial(e) = ae$ para algún $a \in K$ para todo $f \in K$ se tiene que $\partial(fe) = (f' + fa)e$. Más generalmente, dada $e_1, .., e_n$ una base de M sobre K, entonces ∂ está completamente determinado por $\partial(e_i)$ para cada índice $i \in \{1, 2, ..., n\}$.

Este hecho nos permite pasar de módulos diferenciales a sistemas de ecuaciones diferenciales y viceversa. Dado un módulo diferencial (M, ∂) definimos la matriz A_M como $A_M = (a_{ij})_{1 \le i,j \le n} \in M_n(K)$ mediante la condición $\partial(e_i) = -\sum_{j=1}^{n} a_{ij} e_j$. De esta forma, para cualquier elemento $m = \sum_{i=1}^{n} f_i e_i \in M$, el elemento $\partial(m)$ tiene la forma

$$\partial(m) = \sum_{i=1}^{n} f_i' e_i - \sum_{i=1}^{n} \left(\sum_{j=1}^{n} a_{ij} f_j \right) e_i.$$

Reagrupando los términos se tiene que

$$\partial(m) = \sum_{i=1}^{n} \left(f_i' - \sum_{j=1}^{n} a_{ij} f_j \right) e_i.$$

En consecuencia, se tiene que $\partial(m) = 0$ si y solo si $f = (f_1, ..., f_n)$ es solución del sistema $y' = Ay$. Recíprocamente, dado un sistema $y' = Ay$ con $A \in M_n(K)$ podemos considerar

$M = K^n$ y $\partial_A(e) = -Ae$. Comprobamos que $f = (f_1, ..., f_n)$ es solución del sistema, si y solo si $m = \sum_{i=1}^{n} f_i e_i$ cumple que $m \in \ker(\partial_A)$.

Como comentamos en la introducción de la sección, los módulos diferenciales nos permiten trabajar con las ecuaciones diferenciales con independencia de la elección de base. Además, podemos extender las construcciones fundamentales de álgebra lineal a este contexto. Por ejemplo, dados dos K-módulos diferenciales (M_1, ∂_1) y (M_2, ∂_2) sobre la suma directa de módulos $M_1 \oplus M_2$, la derivada se puede definir por $\partial(m_1 \oplus m_2) = \partial_1(m_1) \oplus \partial_2(m_2)$. De forma similar, si consideramos la derivación sobre un producto tensorial $M_1 \otimes M_2$, la expresión de la derivada es $\partial(m_1 \otimes m_2) = \partial_1(m_1) \otimes m_2 + m_1 \partial_2(m_2)$. El módulo de homomorfismos $\mathrm{Hom}_K(M_1, M_2)$, tiene estructura de módulo diferencial con la derivación $\partial(f)(m) = f(\partial_1(m)) - \partial_2(f(m))$.

3.4. Teorema de Ritt

Recordamos que para todo polinomio $P \in K[X_1, ..., X_n]$ no nulo con coeficientes en un cuerpo infinito, se cumple que existe $(a_1, ..., a_n) \in K^n$ tal que $f(a_1, ..., a_n) \neq 0$. Concluimos este capítulo con la versión diferencial de este teorema. Para realizar la demostración haremos uso del Wronskiano.

Del mismo modo que en la teoría elemental de ecuaciones diferenciales ordinarias podemos decidir caracterizar la dependencia lineal de un conjunto de elementos de K en términos del Wronskiano.

Definición 3.15. Sean K un cuerpo diferencial e $y_1, y_2, ..., y_n \in K$. La **matriz Wronskiana** de $y_1, y_2, ..., y_n$ es la matriz $n \times n$ con coeficientes en K dada por

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

El Wronskiano, $\mathrm{wr}(y_1, \ldots, y_n)$, de $y_1, \ldots, y_n$ es el determinante de $W(y_1, \ldots, y_n)$.

Lema 3.16. *Sea K un cuerpo diferencial y C su cuerpo de constantes. Los elementos del cuerpo $y_1, \ldots, y_n \in K$ son linealmente dependientes sobre C si y solo si* $\mathrm{wr}(y_1, \ldots, y_n) = 0$.

Demostración. En primer lugar, veamos que existe una ecuación diferencial escalar mónica $L(y) = 0$ de orden n sobre K, tal que $L(y_i) = 0$ para todo $i \in \{1, \ldots, n\}$. La construcción

de L se realiza por inducción. Primero, definimos:

$$L_1(y) = y' - \frac{y_1'}{y_1} y,$$

donde el término y_1'/y_1 se interpreta como 0 si $y_1 = 0$. Supongamos que hemos construido $L_m(y)$ tal que $L_m(y_i) = 0$ para todo $i \in \{1, \ldots, m\}$. Veamos que podemos extender la construcción para el caso $m+1$. La expresión de $L_{m+1}(y)$ es

$$L_{m+1}(y) = L_m(y)' - \frac{L_m(y_{m+1})'}{L_m(y_{m+1})} L_m(y),$$

donde se puede comprobar que si se sustituye y_{m+1}, se tiene que $L_{m+1}(y_{m+1}) = 0$. Además, de nuevo el término $L_m(y_{m+1})'/L_m(y_{m+1})$ se interpreta como 0 si $L_m(y_{m+1}) = 0$. De esta manera, $L_{m+1}(y_i) = 0$ para $i \in \{1, \ldots, m+1\}$. Finalmente, $L = L_n$ cumple con la propiedad requerida. Las columnas de la matriz Wronskiana son soluciones de la ecuación diferencial asociada a la matriz compañera $y' = A_L y$. Concluimos aplicando el Lema 3.6. ■

En consecuencia, si consideramos una extensión diferencial de K, la independencia o dependencia lineal de $y_1, y_2, ..., y_n$ sobre el cuerpo de constantes no se modifica puesto que el valor de $\mathrm{wr}(y_1, ..., y_n)$ es independiente del cuerpo en el que estemos trabajando.

Corolario 3.17. *Sean $K_1 \subset K_2$ cuerpos diferenciales con cuerpos de constantes $C_1 \subset C_2$. Los elementos $y_1, \ldots, y_n \in K_1$ son linealmente independientes sobre C_1 si y solo si son linealmente independientes sobre C_2.*

Comprobamos que la fórmula de Abel-Liouville también es válida en este contexto.

Teorema 3.18. *Sea $y' = Ay$ una ecuación diferencial matricial sobre un cuerpo diferencial K, donde $A \in M_n(K)$, y sea R una extensión diferencial de K y $Z \in M_n(R)$ una matriz fundamental de soluciones (es decir, $Z' = AZ$ y $\det Z \neq 0$). Entonces, la derivada del determinante de Z satisface:*

$$(\det Z)' = \mathrm{tr}(A) \cdot \det Z,$$

donde $\mathrm{tr}(A)$ denota la traza de la matriz A.

Demostración. Dados $Z = (z_{ij})$ y $A = (a_{ij})$ con $1 \leq i, j \leq n$, queremos demostrar la fórmula de Abel-Liouville. En primer lugar, calculamos la derivada del determinante de Z uti-

lizando la fórmula de Leibniz del determinante y la regla de Leibniz para las derivadas

$$(\det Z)' = \sum_{i=1}^{n} \det \begin{pmatrix} z_{11} & z_{12} & \cdots & z_{1n} \\ \vdots & \vdots & & \vdots \\ z'_{i1} & z'_{i2} & \cdots & z'_{in} \\ \vdots & \vdots & & \vdots \\ z_{n1} & z_{n2} & \cdots & z_{nn} \end{pmatrix}.$$

Por hipótesis, $Z' = AZ$, lo que para los z_{ij} componentes de la matriz se traduce como

$$z'_{ik} = \sum_{j=1}^{n} a_{ij} z_{jk}, \qquad \forall i,k \in \{1,\dots,n\}.$$

En cada sumando de la derivada de $\det Z$, sustraemos a la fila i una combinación lineal de las otras filas de manera que en la entrada (i,k) de la nueva matriz aparece

$$z'_{ik} - \sum_{j=1, i\neq j}^{n} a_{ij} z_{jk} = a_{ii} z_{ik}.$$

Esto nos permite extraer el coeficiente a_{ii} como factor

$$(\det Z)' = \sum_{i=1}^{n} a_{ii} \det Z = \operatorname{tr}(A) \cdot \det Z.$$

■

Aplicando este resultado al caso particular de las ecuaciones diferenciales lineales, obtenemos una ecuación escalar de orden 1.

Corolario 3.19. *Sea $L(y) = y^{(n)} + a_{n-1}y^{(n-1)} + \cdots + a_1 y' + a_0 y = 0$, una ecuación diferencial lineal homogénea de orden n sobre K, y sea $\{y_1,\dots,y_n\} \subset K$ un conjunto fundamental de soluciones. Entonces, su Wronskiano $w = \operatorname{wr}(y_1,\dots,y_n)$ satisface la siguiente ecuación diferencial $w' = -a_{n-1}w$.*

Demostración. Como en este caso $y_1,\dots,y_n$ es un conjunto fundamental de soluciones entonces W la matriz del Wronskiano es una matriz fundamental del sistema $y' = A_L y$ donde A_L es la matriz compañera de L. Si aplicamos el apartado anterior tenemos que $(\det W)' = tr(A_L) \cdot \det(W)$, es decir, que $w' = -a_{n-1}w$ como queríamos demostrar. ■

Recordamos que todo polinomio no nulo con coeficientes en un cuerpo infinito define una función polinomial no nula, luego polinomios diferentes definen funciones polinomiales diferentes.

Como consecuencia de las propiedades del Wronskiano podemos extender este teorema a polinomios diferenciales. Aunque no lo emplearemos en el Capítulo 4 se trata de un resultado clave de la teoría de Galois diferencial y de la Geometría Algebraica diferencial que aparece de manera natural al estudiar ecuaciones diferenciales no lineales. La demostración que presentamos a continuación está basada en la versión planteada en [7].

Teorema 3.20 (Teorema de Ritt)**.** *Sea K un cuerpo diferencial con cuerpo de constantes C, y supongamos que $K \neq C$. Sea $P \in K\{\{y_1, \ldots, y_n\}\}$ un elemento no nulo. Para cualesquiera $u_1, \ldots, u_n \in K$, existe un único homomorfismo K-lineal de anillos diferenciales*

$$\varphi : K\{\{y_1, \ldots, y_n\}\} \to K$$

tal que $\varphi(y_i) = u_i$ para todo i. Denotamos $\varphi(P) = P(u_1, \ldots, u_n)$. Entonces:

Existen elementos $u_1, \ldots, u_n \in K$ tales que $P(u_1, \ldots, u_n) \neq 0$.

Demostración. Veamos que si el resultado es cierto para $n = 1$, entonces es cierto para todo $n \geq 1$. Para justificar esta observación, supongamos que el resultado se cumple para $n = 1$, es decir, dado cualquier $Q \in K\{\{y\}\}$, podemos encontrar $u \in K$ tal que $\varphi(Q) \neq 0$, donde $\varphi : K\{\{y\}\} \to K$ es el homomorfismo diferencial definido por $\varphi(y) = u$. Razonamos por inducción, suponemos que es cierto también para valores menores o iguales que $n-1$ y veamos que se satisface para n. Tomemos $P \in K\{\{y_1, \ldots, y_n\}\}$ y lo podemos escribir como un polinomio diferencial en y_n con coeficientes en $K\{\{y_1, ..., y_{n-1}\}\}$, es decir,

$$P(y_1, ..., y_n) = \sum_{i=1}^{m} A_i(y_1, ..., y_{n-1})(y_n)^{l_{i,0}}(y_n')^{l_{i,1}} \cdots (y_n^{(r)})^{l_{i,r}},$$

con $l_{i,j} \in \mathbb{N}$ y $A_i(y_1, ..., y_{n-1}) \in K\{\{y_1, ..., y_{n-1}\}\}$ para cada $i \in \{1, ..., m\}$ y cada $j \in \{1, ..., r\}$ y tales que $(l_{i,0}, ..., l_{i,r}) \neq (l_{k,0}, ..., l_{k,r})$ si $i \neq k$.

Como $P(y_1, ..., y_n) \neq 0$, entonces para algún $i \in \{1, ..., m\}$, $A_i(y_1, ..., y_{n-1}) \neq 0$ y por hipótesis de inducción existen $u_1, .., u_{n-1} \in K$ tal que $A_i(u_1, ..., u_{n-1}) \neq 0$. Por consiguiente, $P(u_1, ..., u_{n-1}, y_n) \in K\{\{y_n\}\}$ es un polinomio no nulo, y por el caso $n = 1$, existe $u_n \in K$ tal que $P(u_1, ..., u_{n-1}, u_n) \neq 0$.

En segundo lugar, veamos que se cumple el resultado del teorema para $n = 1$. Fijamos $v \in K$ no constante, $v' \neq 0$ y vamos a probar que si $P \in K\{\{y\}\}$ con orden menor o igual que $m \in N$ entonces existe $u \in K$ de la forma $u = c_0 + c_1 v + c_2 v^2 + \cdots + c_m v^m$ con $c_i \in C$ para cada $i \in \{0, ..., n\}$ tal que $P(u) \neq 0$.

Para ello necesitamos demostrar que si $v \in K$ cumple que $v' \neq 0$, entonces para todo $m \geq 1$ se tiene que $\mathrm{wr}(1, v, v^2, \ldots, v^m) \neq 0$. Razonamos por reducción al absurdo, suponga-

mos que $v \in K$ cumple que $v' \neq 0$ y que $\mathrm{wr}(1, v, v^2, \ldots, v^m) = 0$ para algún $m \geq 1$. Esto significa que los elementos $1, v, v^2, \ldots, v^m$ son linealmente dependientes sobre el cuerpo de constantes C, luego sabemos que existen $c_0, ..., c_n \in C$ tales que $0 = c_0 + c_1 v + c_2 v^2 + \cdots + c_m v^m$. Entonces v es algebraico sobre C y por la Proposición 2.19 obtenemos que $v' = 0$, lo que es absurdo por hipótesis.

Sea A la matriz Wronskiana $A = W(1, v, v^2, \ldots, v^m)$, la cual es invertible por lo que acabamos de ver. Tomamos $z_0, \ldots, z_m$ indeterminados, y definimos el homomorfismo entre las K-álgebras:

$$\Phi : K[y, y', \ldots, y^{(m)}] \to K[z_0, \ldots, z_m]$$

dado por

$$\Phi\left(\begin{pmatrix} y \\ y' \\ \vdots \\ y^{(m)} \end{pmatrix}\right) = A \begin{pmatrix} z_0 \\ z_1 \\ \vdots \\ z_m \end{pmatrix}.$$

Como A es invertible, Φ es un isomorfismo. Entonces, para todo $P \in K\{\{y\}\}$ de orden m, $\Phi(P) \in K[z_0, .., z_m]$ entonces por el resultado clásico existen constantes $(c_0, \ldots, c_m) \in C^{m+1}$ tal que $\Phi(P)(c_0, \ldots, c_m) \neq 0$.

Tomamos $u = c_0 + c_1 v + c_2 v^2 + \cdots + c_m v^m$. Entonces $P(u) = \Phi(P)(c_0, \ldots, c_m)$. Esto se debe a que u es una combinación lineal de la primera fila de A con coeficientes $c_0, \ldots, c_m$. Concluimos que entonces existe $u \in K$ tal que $P(u) \neq 0$. ■

La condición de que K contenga un elemento no constante es necesaria. Por ejemplo, para $K = \mathbb{C}$ con la derivación trivial, si tomamos $P = y'$ con $P \in \mathbb{C}\{\{y\}\}$, no se puede construir un elemento $u \in \mathbb{C}$ para hacer que $P(u) \neq 0$.

CAPÍTULO 4

ANILLOS Y EXTENSIONES DE PICARD-VESSIOT

En el Ejemplo 3.3 del capítulo anterior hemos visto que dada una ecuación diferencial sobre un cuerpo K puede ser que dicha ecuación no tenga soluciones ni en la clausura algebraica de K. El objetivo de este capítulo es construir la menor extensión de K que contiene a las soluciones de dicha ecuación. Esta extensión tendrá de manera natural estructura de anillo y la minimalidad la caracterizamos mediante la noción de ser un anillo diferencial simple que introduciremos en la primera sección. En la segunda, se presentará el concepto de anillo de Picard-Vessiot, mostraremos su existencia y unicidad y veremos cómo construirlo en ejemplos concretos. En la tercera sección, estudiaremos las extensiones de Picard-Vessiot y veremos que las extensiones de Galois finitas son un tipo particular de este tipo de extensiones. Finalmente, definiremos el grupo de Galois diferencial, probaremos que es un subgrupo algebraico del conjunto de matrices invertibles sobre el cuerpo de constantes y enunciaremos sin demostrar la correspondencia de Galois.

En este capítulo, K denotará un cuerpo diferencial con $car(K) = 0$ y la derivada de un elemento $a \in K$ se denotará por a'. Además, supondremos que su cuerpo de constantes C es algebraicamente cerrado.

La hipótesis de que C sea algebraicamente cerrado puede parecer arbitraria pero, es esencial en los razonamientos y estándar en este contexto. Si se elimina esta condición, los anillos de Picard-Vessiot pueden no existir o no ser únicos. Por ello, las generalizaciones que existen de esta noción siempre necesitan hipótesis adicionales, ver [4].

4.1. Anillos diferenciales simples

En esta sección estudiaremos los anillos diferenciales simples y sus propiedades.

Definición 4.1. Sea R un anillo diferencial con derivada $'$. Un **ideal diferencial** I en R es un ideal que satisface que $f' \in I$ para todo $f \in I$.

Relacionándolo con el Teorema 2.12 vemos que un ideal es diferencial cuando podemos inducir una estructura diferencial en el anillo cociente. La demostración de la siguiente proposición se obtiene como resultado de este mismo teorema.

Proposición 4.2. *Si R es un anillo diferencial sobre un cuerpo diferencial K, es decir, es una extensión diferencial de K e I es un ideal diferencial de R, $I \neq R$, entonces el anillo cociente R/I es nuevamente un anillo diferencial sobre K*

Demostración. Por el Teorema 2.12, R/I es un anillo diferencial, veamos que también R/I es una extensión de K. Por el Segundo Teorema de Isomorfía, como $K \cap I = \{0\}$ porque $I \neq R$, se tiene que $(K+I)/I \simeq K/(K \cap I)$, y entonces K es isomorfo a un subcuerpo de R/I. ■

Ejemplo 4.3.

- (0) y R son siempre ideales diferenciales de R.
- En $\mathbb{Q}[X]$ con la derivación usual, es decir, $X' = 1$ observamos que (0) y $\mathbb{Q}[X]$ son de hecho los únicos ideales diferenciales porque si $I = (f)$ con $gr(f) \geq 1$, entonces se cumple que $gr(f') < gr(f)$, luego $f' \notin I$ y por tanto, I no es diferencial.

Lema 4.4. *Sea $\varphi : R \to S$ un homomorfismo de anillos diferenciales entonces $ker(\varphi)$ es un ideal diferencial.*

Demostración. El $\ker(\varphi)$ es un ideal por ser la contraimagen del ideal (0). Además, si tomamos $a \in \ker(\varphi)$ y aplicamos φ sobre la derivada a' se tiene que $\varphi(a') = (\varphi(a))' = 0$ y por lo tanto, $a' \in \ker(\varphi)$. ■

Estamos interesados en los anillos que no tienen ideales diferenciales propios no triviales.

Definición 4.5. Un **anillo diferencial simple** es un anillo diferencial cuyos únicos ideales diferenciales son (0) y R.

Veamos que la condición de ser un anillo diferencial simple nos garantiza que el anillo es un dominio, luego podemos considerar su cuerpo de fracciones y extender allí la derivación de forma única por el Teorema 2.14.

Lema 4.6. *Sea R un anillo diferencial simple, entonces R no tiene divisores de cero.*

Demostración. Primero mostraremos que todo divisor del cero en R es nilpotente. Razonamos por contrarrecíproco tomamos $a \in R$ no nilpotente, y vemos que no es un divisor de cero. Consideremos el ideal formado por los elementos que se anulan al multiplicarlos por alguna potencia de a

$$I = \{b \in R \mid \exists n \geq 1 \text{ con } a^n b = 0\}.$$

Observamos que los elementos de I son divisores del cero y como a no es nilpotente $1 \notin I$, es decir, $I \neq R$. Además, I es ideal porque si $a^n b = 0$ y $a^m \tilde{b} = 0$, entonces $a^{n+m}(b - \tilde{b}) = 0$, y para $r \in R$, $r a^n b = 0$. Por otro lado, I es diferencial porque aplicando (2.2) se tiene que

$$0 = (a^n b)' = a' n a^{n-1} b + a^n b',$$

y multiplicando por a como $a^n b = 0$, se concluye $a^{n+1} b' = 0$, y por tanto $b' \in I$. Como R es simple se cumple que $I = (0)$ y a no es un divisor del cero.
Veamos que el nilradical $\sqrt{(0)}$, el ideal formado por todos los elementos nilpotentes, es un ideal diferencial. Tomamos $a \in R$, $a \neq 0$, nilpotente. Mostraremos que a' también es nilpotente. Elegimos $n > 1$ mínimo tal que $a^n = 0$. Al derivar por (2.2) obtenemos $a' n a^{n-1} = 0$. Como $n a^{n-1} \neq 0$, porque $car(R) = 0$ tenemos que a' es un divisor de cero y, por lo probado antes, a' es nilpotente. En consecuencia, el ideal $\sqrt{(0)}$ es un ideal diferencial y, como $1 \notin \sqrt{(0)}$ y R es simple, entonces, $\sqrt{(0)} = (0)$ y concluimos que 0 es el único divisor del cero.
■

Observamos que, dado un ideal maximal I de un anillo diferencial R, si es ideal diferencial es maximal también entre los ideales diferenciales de R. Sin embargo, no todo ideal diferencial maximal entre los ideales diferenciales de R, es maximal, como veremos en los ejemplos de la siguiente sección. El siguiente lema relaciona ideales diferenciales maximales y anillos diferenciales simples.

Lema 4.7. *Sea R un anillo diferencial e I un ideal diferencial maximal de R, entonces el cociente R/I es un anillo diferencial simple.*

Demostración. Como $I \subset R$ es un ideal diferencial, por el Teorema 2.12, R/I es un anillo diferencial para la derivación $(r + I)' := r' + I$.
Queremos demostrar que R/I es un anillo diferencial simple, es decir, que no tiene ideales diferenciales propios. Como los ideales de R/I son de la forma J/I con $J \subset R$ un ideal que contiene a I, si suponemos que J/I es un ideal diferencial, entonces para cada $x \in J$,

$x' + I \in J/I$, luego $x' + I = y + I$ con $y \in I$, luego $x' - y \in J$. Como $y \in I \subset J$, decimos que $x' \in J$. Por lo que J es también un ideal diferencial de R.
Como I es maximal entre los ideales diferenciales de R, se sigue que $J = I$ o $J = R$. En el primer caso, $J/I = \{0\}$, y en el segundo, $J/I = R/I$. Por lo tanto, los únicos ideales diferenciales en R/I son el cero y el total, lo que implica que R/I no tiene ideales diferenciales propios no triviales.
Concluimos así que R/I es un anillo diferencial simple. ■

Concluimos la sección probando que si K es un cuerpo diferencial con cuerpo de constantes algebraicamente cerrado y R es un anillo extensión diferencial de K que es una K-álgebra finitamente generada, lo que abreviaremos diciendo que R es finitamente generado sobre K y además, R es un anillo diferencial simple entonces, el cuerpo de constantes de R y de su cuerpo de fracciones es C. Para ello, necesitamos emplear el siguiente lema atribuido a M.Rosenlicht (ver [8, Lema A.4]).

Lema 4.8. *Sea F un cuerpo de característica cero, R un dominio finitamente generado sobre F y $x \in R$ tal que $S = \{c \in F : x - c$ es invertible en $R\}$ es infinito, entonces x es un elemento algebraico sobre F.*

Demostración. Como R está finitamente generado sobre F podemos escribir para ciertos $X_i \in R$ y con $X_1 = x$, $R = F[X_1, \ldots, X_n]$. Supongamos que X_1 no es algebraico sobre F, y sea L el cuerpo de fracciones de R. Reordenando, suponemos que $X_1, \ldots, X_r$ es una base de trascendencia de L sobre F, y por el Teorema del Elemento Primitivo, sabemos que existe $y \in R$ un elemento primitivo de L sobre $F(X_1, \ldots, X_r)$.

Tomamos $G \in F[X_1, \ldots, X_r]$ elegido de modo que sea múltiplo del coeficiente principal del polinomio mínimo de y sobre el anillo $F[X_1, \ldots, X_r]$, y de forma que se garantiza que los elementos $X_1, \ldots, X_n \in F[X_1, \ldots, X_r, y, G^{-1}]$.

Dado que S es infinito, existen $c_1, \ldots, c_r \in S$ tales que $G(c_1, \ldots, c_r) \neq 0$. Entonces se puede definir un homomorfismo de $F[X_1, \ldots, X_r, y, G^{-1}]$ en $\bar{F}$, la clausura algebraica de F, tal que $X_i \mapsto c_i$ para $i \in \{1, \ldots, r\}$. Esto es posible porque si $P(T)$ es el polinomio mínimo de y sobre $F[X_1, ..., X_r]$, $P(c_1, ..., c_r, T)$ es un polinomio no nulo de $F[T]$ por la elección de G como múltiplo del coeficiente director, luego existe una raíz de $P(c_1, ..., c_r, T)$ en $\bar{F}$ que denotamos por $\bar{y}$ y enviamos y en $\bar{y}$ y G^{-1} en $(G(c_1, ..., c_r))^{-1}$.

Como $R \subset F[X_1, \ldots, X_r, y, G^{-1}]$, el homomorfismo inducido de R en $\bar{F}$ envía $X_1 - c_1$ que es una unidad en R en 0, lo que es absurdo. ■

Teorema 4.9. *Sea R un anillo diferencial simple que está finitamente generado sobre K. Entonces, R y su cuerpo de fracciones, tiene a C como conjunto de constantes.*

Demostración. Consideramos L el cuerpo de fracciones de R y tomamos $a \in L$ con su derivada $a' = 0$. En primer lugar, veamos que a es una constante sobre R, es decir, veamos que $a \in R$. Podemos suponer $a \neq 0$, consideramos el conjunto $I = \{b \in R \mid ba \in R\}$ comprobamos que I es un ideal diferencial. Como $a \in L$ tenemos que $a = n/d$ con $n, d \in R$ y $d \neq 0$ luego $da = n \in R$ y deducimos que I es no nulo. Además, I es ideal pues si $b, \tilde{b} \in I$ y $r \in R$, entonces $(b - \tilde{b})a \in R$ y $r(ba) \in R$. Por último, I es diferencial porque si $b \in I$, $(ba)' = b'a + ba'$. Por tanto, $b'a \in R$ porque $a' = 0$ y $ba \in R$ entonces $b' \in I$. Como R es simple, todo ideal diferencial no trivial es $I = R$, luego $1 \in I$ y por ello $a \in R$.

Razonamos por contradicción y suponemos que $a \notin C$. Entonces, para todo $c \in C$, consideramos $(a - c)R$ que es un ideal de R no nulo porque $a - c$ es distinto de cero y es diferencial porque tomando $r \in R$, se tiene que, $((a - c)r)' = (a - c)'r + (a - c)r'$. Como $c \in C$ y se cumple que $a' = 0$ entonces se concluye que $((a - c)r)' \in (a - c)R$. Como R es simple para cada $c \in C$, $(a - c)R = R$, luego $(a - c)$ es una unidad en R. Como C es un cuerpo de característica cero, es infinito y por el Lema 4.8, tenemos que a es algebraico sobre K.
Por la Proposición 2.19 como a es algebraico sobre K y $a' = 0$, tenemos que a es algebraico sobre C, lo que es imposible porque C es algebraicamente cerrado y estamos suponiendo $a \notin C$. ■

Este teorema nos permite aplicar los resultados del Capítulo 3 relativos a la dependencia lineal de las soluciones sobre el cuerpo de constantes, aunque dichas soluciones estén en un anillo diferencial simple R extensión de K.

4.2. Anillos de Picard-Vessiot

Esta sección se centrará en los anillos de Picard-Vessiot, sus propiedades algebraicas y su construcción explícita, así como su relación con módulos diferenciales.

Definición 4.10. Un **anillo de Picard-Vessiot sobre K para la ecuación** $y' = Ay$, con la matriz $A \in M_n(K)$, es un anillo diferencial R sobre K que satisface que:

(I) R es un anillo diferencial simple.

(II) Existe una matriz fundamental F para $y' = Ay$ con coeficientes en R, es decir, la matriz $F \in \mathrm{GL}_n(R)$ satisface $F' = AF$.

(III) R está generado sobre K, las entradas de F y el inverso del determinante de F.

Empleando la relación entre sistemas de ecuaciones diferenciales y módulos diferenciales de la Sección 3.3, un anillo de Picard-Vessiot para un módulo diferencial M sobre K se define como un anillo de Picard-Vessiot de una ecuación diferencial matricial $y' = Ay$ asociada a M. Con ello podemos probar que la noción de anillo de Picard-Vessiot es independiente de los cambios de base.

Proposición 4.11. *Sea (M,∂) un módulo diferencial de dimensión finita sobre un cuerpo diferencial K con cuerpo de constantes C. Sean $y' = Ay$ e $\tilde{y}' = \widetilde{A}\tilde{y}$ dos ecuaciones diferenciales matriciales asociadas al mismo módulo diferencial M. Un anillo diferencial R sobre K es un anillo de Picard-Vessiot para $y' = Ay$ si y solo si lo es también para $\tilde{y}' = \widetilde{A}\tilde{y}$.*

Demostración. Por la Proposición 3.5, las ecuaciones $y' = Ay$ e $\tilde{y}' = \widetilde{A}\tilde{y}$ representan el mismo módulo diferencial M bajo diferentes bases, relacionadas por una matriz invertible $P \in \mathrm{GL}_n(K)$, de modo que $\widetilde{A} = P^{-1}AP - P^{-1}P'$.

Sea $R = K\langle (F_{ij})_{1\leq i,j\leq n}, (\det F)^{-1}\rangle$ un anillo de Picard-Vessiot para $y' = Ay$, donde la matriz $F \in \mathrm{GL}_n(R)$ es una matriz fundamental. Definimos $\widetilde{F} := P^{-1}F$ y observamos que

$$\widetilde{F}' = (P^{-1})'F + P^{-1}F' = -P^{-1}P'P^{-1}F + P^{-1}AF = \widetilde{A}\widetilde{F}.$$

Así, $\widetilde{F}$ es matriz fundamental para $\tilde{y}' = \widetilde{A}\tilde{y}$ y genera el mismo anillo R porque $\tilde{F} = P^{-1}F$ con $P \in \mathrm{GL}_n(K)$, por lo que R es también un anillo de Picard-Vessiot para $\tilde{y}' = \tilde{A}\tilde{y}$. ■

Como en la Sección 3.3, recordamos que dado un módulo diferencial (M,∂) sobre K si R es una extensión de K entonces es también un K-módulo y podemos definir sobre el producto $R \otimes M$ la derivación $\tilde{\partial}(r \otimes m) = r' \otimes m + r \otimes \partial(m)$. Cuando no haya ambigüedad denotaremos a esta derivación como ∂ abusando de la notación.

Por otro lado, observamos que $R \otimes M$ tiene estructura de R-módulo con el producto $r_1(r_2 \otimes m) = (r_1 r_2) \otimes m$. Además, dado un elemento $r \otimes m \in R \otimes M$ y una base $e_1, \ldots, e_n$ de M como K-módulo, escribimos $m = \sum_{i=1}^{n} \alpha_i e_i$ con $\alpha_1, \ldots, \alpha_n \in K$ y tenemos que

$$r \otimes m = \sum_{i=1}^{n} \alpha_i (r \otimes e_i) = \sum_{i=1}^{n} r\alpha_i (1 \otimes e_i).$$

Los vectores $1 \otimes e_1, \ldots, 1 \otimes e_n$ forman una base de $R \otimes M$ como R-módulo libre y podemos describir la derivación en términos de esta base: si escribimos $r_i = r\alpha_i$ para cada $i \in \{1, 2, \ldots, n\}$, tenemos que

$$\tilde{\partial}(r \otimes m) = \tilde{\partial}\Big(\sum_{i=1}^{n} r_i \otimes e_i\Big) = \sum_{i=1}^{n} \tilde{\partial}(r_i \otimes e_i) = \sum_{i=1}^{n} [r_i'(1 \otimes e_i) + r_i(1 \otimes \partial(e_i))]. \tag{4.1}$$

Proposición 4.12 (Caracterización de los anillos de Picard-Vessiot para módulos diferenciales)**.** *Un anillo diferencial R es un anillo de Picard-Vessiot para (M,∂) si y solo si cumple las siguientes condiciones:*

(I) *R es un anillo diferencial simple.*

(II) *$V := \ker(\partial, R\otimes M)$ tiene dimensión igual a $\dim_K M$ sobre C.*

(III) *Dada $\{e_1, e_2, ..., e_n\}$ cualquier base de M sobre K y cualquier base $\{v_1, v_2, ..., v_n\}$ de V como C-espacio vectorial, denotamos por H a la matriz que resulta de expresar los vectores de la base de V en términos de la base libre $\{1\otimes e_1, 1\otimes e_2, ..., 1\otimes e_n\}$ de $R\otimes M$ sobre R. Entonces R está generado sobre K por las entradas de H y $(\det H)^{-1}$.*

Demostración. Supongamos primero que R es un anillo de Picard-Vessiot en el sentido de la Definición 4.10. Entonces existe una matriz fundamental $F \in \mathrm{GL}_n(R)$. Tomamos un elemento $v = r\otimes m \in R\otimes M$ y lo escribimos en términos de la base $1\otimes e_1, ..., 1\otimes e_n$ de $R\otimes M$ como R-módulo entonces $v = \sum_{i=1}^n r_i(1\otimes e_i)$ con $r_i \in R$. Veamos que $v \in ker(\partial, R\otimes M)$ si y solo si $(r_1, ..., r_n) \in R^n$ es solución de $y' = Ay$ donde A es la matriz asociada en la base $e_1, ..., e_n$. Por (4.1), tenemos que $\partial(v) = 0$ si y solo si

$$\sum_{i=1}^n r_i'(1\otimes e_i) + \sum_{i=1}^n r_i(1\otimes \partial(e_i)) = 0.$$

Como $\partial(e_i) = -\sum_{k=1}^n a_{ki}e_k$, tenemos que

$$\sum_{i=1}^n \left(r_i' - \sum_{j=1}^n a_{ij}r_j \right)(1\otimes e_i) = 0.$$

Además, como $1\otimes e_1, ..., 1\otimes e_n$ es base de $R\otimes M$ como R-módulo, deducimos que $\partial(v) = 0$ si y solo si $(r_1, ..., r_n)$ es solución de $y = Ay$. Como $F \in \mathrm{GL}_n(R)$ es una matriz fundamental del sistema $y' = Ay$ deducimos que $\dim_C(ker(\partial, R\otimes M)) = n$. Finalmente, elegimos una base $\{v_1, v_2, .., v_n\}$ cualquiera de V y veamos que R está generado por las entradas de la matriz H y $(\det H^{-1})$ donde H es la matriz construida como en el enunciado. Para cada $j \in \{1, ..., n\}$ como $v_i \in R\otimes M$ podemos tomar $v_j = \sum_{i=1}^n h_{ij}\otimes e_i$ con $h_{ij} \in R$ para cada $i \in \{1, ..., n\}$.
Como $v_j \in V$, tenemos que $(h_{1j}, ..., h_{nj}) \in R^n$ es solución de $y' = Ay$. Por el Teorema 4.9 sabemos que el cuerpo de constantes de R es también C. Como $v_1, ..., v_n$ son linealmente independientes sobre C, por el Lema 3.7, $v_1, v_2, ..., v_n$ son linealmente independientes sobre R, luego $\det H \neq 0$ y $H \in \mathrm{GL}_n(R)$ es una matriz fundamental del sistema $y' = Ay$. Por la Proposición 3.9, $H = FM$ con $M \in \mathrm{GL}_n(C)$ y por lo tanto, R está generado sobre K por las entradas de H y $(\det H)^{-1}$.

Para comprobar el recíproco queremos ver que si se cumplen las condiciones entonces es un anillo de Picard-Vessiot. Por la condición (III) sabemos que H es una matriz cuyas columnas son las soluciones linealmente independientes de $y' = Ay$, es decir, es una matriz fundamental de la ecuación y además se cumple (II) porque R está generado sobre K por las entradas de H y $(\det H)^{-1}$. Añadiendo que se satisface también la condición (I) de ser un anillo simple entonces se cumple la Definición 4.10. ■

Proposición 4.13. *Si R_1 y R_2 son dos anillos de Picard-Vessiot para M, entonces cualquier isomorfismo de anillos diferenciales $\phi : R_1 \to R_2$ sobre K induce un isomorfismo C-lineal $\varphi : V_1 \to V_2$ entre los respectivos espacios de soluciones.*

Demostración. Definimos:

$$\varphi := \phi \otimes \mathrm{id}_M : R_1 \otimes M \to R_2 \otimes M.$$

Si $v \in V_1 := \ker(\partial, R_1 \otimes M)$, entonces $\varphi(v) \in V_2$, ya que $\partial(\varphi(v)) = (\phi \otimes \mathrm{id})(\partial v) = 0$.
Como φ es inyectivo por serlo ϕ y como $\dim_c V_1 = \dim_C V_2$, deducimos que φ es un isomorfismo C-lineal entre los espacios de soluciones V_1 y V_2. ■

Sin embargo, esta correspondencia depende, en general, de la elección del isomorfismo ϕ, y distintas elecciones de ϕ pueden inducir automorfismos C-lineales distintos sobre V_2. Veremos que estos automorfismos forman parte de la acción del grupo de Galois diferencial sobre el espacio de soluciones.

Ejemplo 4.14. Dado $a \in K$ consideramos la ecuación matricial

$$\begin{pmatrix} y_1 \\ y_2 \end{pmatrix}' = \begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}.$$

Vamos a ver cómo construir el anillo de Picard-Vessiot de está ecuación. Distinguimos dos casos:

- Si tenemos $b \in K$ tal que $b' = a$, una matriz fundamental del sistema es $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$.
  En este caso, $R = K$ es un anillo de Picard-Vessiot para el sistema como ocurría para la ecuación $y' = a$ en el Ejemplo 3.3 cuando $a_{-1} = 0$.

- Supongamos que la ecuación escalar $y' = a$ no tiene solución en K. Definimos el anillo diferencial $R = K[T]$ con la derivación $'$ que extiende a $'$ sobre K con $T' = a$ por

el Teorema 2.16. Entonces, R contiene una solución obvia de la ecuación escalar y

$$\begin{pmatrix} 1 & T \\ 0 & 1 \end{pmatrix},$$

es una matriz fundamental para la ecuación matricial.
Queremos mostrar que R solo tiene ideales diferenciales propios triviales. Tomamos I un ideal propio de $K[T]$. Entonces, I está generado por algún

$$F = T^n + \cdots + f_1 T + f_0 \quad \text{con} \quad n > 0.$$

La derivada de F es $F' = (na + f'_{n-1})T^{n-1} + \cdots + f_1 a + f'_0$. Si I es un ideal diferencial, entonces $F' \in I$ y, por lo tanto, $F' = 0$. En particular, se cumple que $na + f'_{n-1} = 0$, luego $-(f_{n-1}/n)' = a$. Esto contradice nuestra hipótesis sobre a, por lo que concluimos que $R = K[T]$ es un anillo de Picard-Vessiot para $y' = a$.

A continuación mostramos el cálculo del anillo Picard-Vessiot empleando la caracterización de la Proposición 4.12.
Consideramos el módulo diferencial M asociado al sistema previo cuya derivación está dada por $\partial(e_1) = 0, \partial(e_2) = -ae_1$. Si existe $b \in K$ tal que $b' = a$, tomamos $R = K$.
Entonces $K \otimes M \simeq M$ y $\tilde{\partial} = \partial$. En consecuencia $V = \ker(\partial)$, está generado por e_1 y $be_1 + e_2$ como C-espacio vectorial y

$$H = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}.$$

Se cumple que para $R = K$ está generado sobre K por las entradas de H y $(\det H)^{-1}$.

Si no existe $b \in K$ tal que $b' = a$, tomamos $R = K[T]$ extendiendo la derivación considerando $T' = a$. Como hemos visto antes R es un anillo diferencial simple y $\tilde{\partial} : R \otimes M \to R \otimes M$ está dada por $\tilde{\partial}(r \otimes m) = r' \otimes m + r \otimes \partial(m)$.
Por lo tanto, dado $v \in V = \ker(\tilde{\partial})$, escribimos $v = r_1 \otimes e_1 + r_2 \otimes e_2$ y tenemos que

$$\begin{aligned} \tilde{\partial}(v) &= r'_1 \otimes e_1 + r'_2 \otimes e_2 + r_1 \otimes \partial e_1 + r_2 \otimes \partial e_2 \\ &= r'_1 \otimes e_1 + r'_2 \otimes e_2 - ar_2 \otimes e_1 = r'_2 \otimes e_2 + (r'_1 - ar_2) \otimes e_1, \end{aligned}$$

luego $\tilde{\partial}(v) = 0$ si y solo si $r'_2 = 0$ y $r'_1 = ar_2$, es decir, coincide con el espacio de soluciones de $y' = Ay$. Una base de V está dada por $v_1 = 1 \otimes e_1$ y $v_2 = T \otimes e_1 + 1 \otimes e_2$ y R está generado por las entradas de $H = \begin{pmatrix} 1 & T \\ 0 & 1 \end{pmatrix}$ y $(\det H)^{-1}$.

Ejemplo 4.15. Consideremos ahora la ecuación diferencial $y' = ay$ con $a \in K^*$. Definimos el anillo diferencial $R = K[T, T^{-1}]$ con la derivación $'$ que extiende $'$ por el Teorema 2.17 sobre K y $T' = aT$.
Como $K[T, T^{-1}]$ es la localización del dominio de ideales principales $K[T]$ en S, donde $S = \{T^n : n \in \mathbb{N}\}$, tenemos que $K[T, T^{-1}]$ es también dominio de ideales principales. Por construcción, R contiene una solución no nula de $y' = ay$, luego cumple (II) y (III) de la Definición 4.10. Por tanto, el anillo R sería la respuesta a nuestro problema si no tiene ideales diferenciales propios no triviales. Para estudiar esto, debemos plantear dos casos:

(a) Caso 1: para todo $n \in \mathbb{Z}, n \neq 0$, la ecuación $y' = nay$ no tiene soluciones $y \neq 0$ en K. Tomamos $I \neq 0$ un ideal diferencial de R. Como $R[T, T^{-1}]$ es un D.I.P, entonces I está generado por algún $F = T^m + a_{m-1}T^{m-1} + \cdots + a_0$, con $m \geq 0$ y, como T es una unidad, podemos suponer $a_0 \neq 0$. Empleando que $T' = aT$, calculamos F' y obtenemos que

$$F' = maT^m + ((m-1)aa_{m-1} + a'_{m-1})T^{m-1} + \cdots + a'_1 T + a'_0$$

Como I es diferencial $F' \in I = (F)$ y como $gr(F) = gr(F') = m$, se tiene que la derivada $F' = maF$. Para $m > 0$, mirando el término independiente se obtiene la contradicción $a'_0 = maa_0$ con $a_0 \neq 0$. Por lo tanto, $m = 0$ y deducimos que $I = R$. Concluimos que $R = K[T, T^{-1}]$ es un anillo de Picard-Vessiot para la ecuación $y' = ay$.

(b) Caso 2: Existe $n \in \mathbb{Z}$, $n \neq 0$, tal que la ecuación $y' = nay$ tiene una solución $y \in K^*$. Suponemos que $n > 0$ es el valor mínimo para el cual la ecuación $y' = nay$ tiene una solución $y_0 \in K^*$.
Observamos que en este caso el anillo $R[T, T^{-1}]$ tiene un ideal diferencial I no trivial dado por $I = (F)$ con $F = T^n - y_0$. Comprobamos que I es diferencial porque $F' = naT^n - nay_0 = naF$, usando que $T' = aT$ y que $y'_0 = nay_0$.
Consideramos el anillo cociente $K[T, T^{-1}]/(T^n - y_0)$ que denotamos por $K[t, t^{-1}]$ donde t es la imagen de T en el cociente.
Por la Proposición 4.2, como I es diferencial, $K[t, t^{-1}]$ es un anillo diferencial, extensión diferencial de K. Con esta notación se tiene que $t^n = y_0$, $t' = at$ y cada elemento de $K[t, t^{-1}]$ puede escribirse de manera única como $\sum_{i=0}^{n-1} a_i t^i$, con $a_i \in K$ para cada $i \in \{0, ..., n-1\}$. Veamos que $K[t, t^{-1}]$ es un anillo de Picard-Vessiot para $y' = ay$. Debemos probar que $K[t, t^{-1}]$ no tiene ideales diferenciales propios no triviales.

Tomamos $J \subset K[t, t^{-1}], J \neq 0$ un ideal diferencial. Sea $0 \leq d < n$ el valor mínimo tal que J contiene un G no nulo de la forma $G = \sum_{i=0}^{d} a_i t^i$. Supongamos que $d > 0$. Podemos asumir que $a_d = 1$. La minimalidad de d implica que $a_0 \neq 0$, porque t es unidad

en $K[t,t^{-1}]$. Derivando obtenemos

$$G' = daat^d + \left((d-1)aa_{d-1} + a'_{d-1}\right)t^{d-1} + \cdots + a'_0.$$

Como $G', G \in J$ el elemento $G' - daG$ pertenece a J debe ser igual a 0, puesto que d es mínimo. Entonces $a'_0 = daa_0$, lo cual contradice nuestra suposición sobre n. Por lo tanto, $d = 0$ y $J = K[t,t^{-1}]$.

Observación 4.16. Observamos que en el primer caso del segundo ejemplo necesitamos añadir a K una función que se comporta como una exponencial, esto ocurre por ejemplo para $K = \mathbb{C}(z)$ con la derivación usual (ver Ejemplo 2.3) y la ecuación $y' = y$. En este caso, añadimos una solución formal T que cumple que $T' = T$, es decir, una exponencial formal. Por otro lado, en el segundo caso ya disponemos de una función exponencial, por ejemplo para $K = \mathbb{C}(z, e^{3z})$ donde la derivación se extiende empleando el Teorema 2.16 de manera que $(e^{3z})' = 3e^{3z}$. En este caso, para resolver la ecuación $y' = y$ solo necesitamos añadir una raíz cúbica a nuestro cuerpo.
Por lo visto en el ejemplo, sabemos que $I = (T^3 - e^{3z})$ es un ideal diferencial no trivial de $K[T,T^{-1}]$ y el anillo de Picard-Vessiot está dado por $K[T,T^{-1}]/I$, es decir, añadimos a K una solución t que cumple que $t^3 = e^{3z}$. Si en lugar de considerar la ecuación $y' = y$, estudiamos otro tipo de ecuaciones también podemos hallar el anillo de Picard-Vessiot como muestra el siguiente ejemplo.

Ejemplo 4.17. Consideremos $K = \mathbb{C}(z)$, con la derivación usual, ver Ejemplo 2.3, $\alpha \in \mathbb{C}$, y la ecuación $y' = (\alpha/z)y$. Como en los ejemplos previos consideramos el anillo $R = K[T,T^{-1}]$ extendiendo la derivación por el Teorema 2.17, con $T' = (\alpha/z)T$. Veamos si R es un anillo de Picard-Vessiot para la ecuación. Distinguimos dos casos:

(a) Caso 1: $\alpha \in \mathbb{Q}$. Escribimos $\alpha = n/m$ con $mcd(n,m) = 1$. En este caso existe un ideal no nulo propio $I = (T^m - z^n)$ que es diferencial razonando como en el Ejemplo 4.15 para $y_0 = z^n$. Además, I es maximal porque como $mcd(n,m) = 1$ el polinomio $T^m - z^n$ no se puede poner como producto de polinomios de grado menor. Por el Lema 4.7 haciendo el cociente por $(T^m - z^n)$ se tiene que $R = K[T,T^{-1}]/(T^m - z^n)$ es un anillo de Picard Vessiot.

(b) Caso 2: $\alpha \notin \mathbb{Q}$. En este caso, nuestro objetivo es probar que $K[T,T^{-1}]$ es simple. Veamos que para todo $N \in \mathbb{Z}$, $N \neq 0$, la ecuación $y' = (N\alpha/z)y$ solo tiene soluciones triviales en $K = \mathbb{C}(z)$.

Para probar esto tomamos $f \in \mathbb{C}(z)$, luego $f(z) = P(z)/Q(z)$ con $P, Q \in \mathbb{C}[z]$. Escribimos P, Q en términos de factores de grado 1 y derivamos para obtener que

$$\frac{f'}{f} = \frac{P'(z)}{P(z)} - \frac{Q'(z)}{Q(z)} = \sum_{i=1}^{m} \frac{n_i}{z - \alpha_i},$$

con $n_i \in \mathbb{Z}$ y $\alpha_i \in \mathbb{C}$ para cada $i \in \{1, 2, ..., n\}$. Por lo tanto, f'/f no puede ser igual a $N\alpha/z$ para ningún $N \in \mathbb{Z}$, $N \neq 0$. Por el caso 1, del Ejemplo 4.15, $K[T, T^{-1}]$ con $T' = (\alpha/z)T$ es el anillo de Picard-Vessiot de la ecuación.

Las construcciones de los ejemplos previos se pueden generalizar y nos permiten probar la existencia de los anillos de Picard-Vessiot. Para ello, dado un anillo R vamos a construir el anillo de polinomio en n^2 variables $(X_{ij})_{1 \leq i,j \leq n}$ que denotamos por $R[X_{ij}]$ por simplicidad. Sabemos que $\det = \det((X_{ij})_{1 \leq i,j \leq n})$ es un elemento de $R[X_{ij}]$. El anillo localizado respecto de $\{\det^n : n \in \mathbb{N}\}$ lo denotamos por $R[X_{ij}, 1/\det]$.

Teorema 4.18. *Sea $y' = Ay$ una ecuación diferencial matricial sobre K.*

I. Existe un anillo de Picard-Vessiot para la ecuación.

II. Cualquier par de anillos de Picard-Vessiot para la ecuación son isomorfos.

III. Las constantes del cuerpo de fracciones de un anillo de Picard-Vessiot es también C.

Demostración. I. Consideramos el anillo diferencial $R_0 = K[X_{ij}, 1/\det]$ con la derivación extendida de K, dada por $(X'_{ij}) = A(X_{ij})$. El Teorema 2.17 muestra la existencia y unicidad de tal derivación. Tomamos $I \subset R_0$ un ideal diferencial maximal. Entonces, se comprueba que $R = R_0/I$ es un anillo de Picard-Vessiot para la ecuación por el Lema 4.7.

II. Dados R_1, R_2 dos anillos de Picard-Vessiot para la ecuación. Sea F_1, F_2 las dos matrices fundamentales. Consideramos el anillo diferencial $R_1 \otimes R_2$ con la derivación dada por $(r_1 \otimes r_2)' = r_1' \otimes r_2 + r_1 \otimes r_2'$ (ver (4.1)). Elegimos un ideal diferencial $I \subset R_1 \otimes R_2$ maximal y definimos $R_3 := (R_1 \otimes R_2)/I$. Sabemos que existe porque consideramos los morfismos naturales de anillos diferenciales $\varphi_i : R_i \to R_3$ dados por la inclusión y el paso al cociente para cada $i \in \{1, 2\}$. Como φ_i no es idénticamente nulo, se tiene que $\ker(\varphi_i) \neq R_i$ y como R_i es simple, $\ker(\varphi_i) = (0)$, luego $\varphi_i : R_i \to \varphi(R_i)$ es un isomorfismo. La imagen de φ_i es generada sobre K por los coeficientes de $\varphi_i(F_i)$ y $\varphi_i((\det F_i)^{-1})$. Las matrices $\varphi_1(F_1)$ y $\varphi_2(F_2)$ son matrices fundamentales sobre el

anillo R_3. Por el Lema 4.9, el conjunto de las constantes de R_3 es C, y por la Proposición 3.9 se tiene que $\varphi_1(F_1) = \varphi_2(F_2)M$, donde $M \in \mathrm{GL}_n(C)$. Esto implica que $\varphi_1(R_1) = \varphi_2(R_2)$, y por lo tanto, R_1 y R_2 son isomorfos.

III. Directo por el Lema 4.9 ■

4.3. Cuerpo de Picard-Vessiot

En esta sección nos centraremos en el estudio de extensiones diferenciales de Picard-Vessiot. A diferencia de la teoría de Galois clásica, que se desarrolla en el contexto de extensiones de cuerpos, la teoría de Picard-Vessiot se formula de manera natural en términos de anillos diferenciales. Esto se debe a que, al añadir las soluciones de una ecuación diferencial lineal, no siempre se obtiene un cuerpo, sino un anillo diferencial. En contraste, la teoría clásica se basa en el siguiente resultado fundamental que podemos encontrar en [3]:

Teorema 4.19. *Sea R una extensión de K. Entonces, el conjunto de los elementos de R que son algebraicos sobre K forma un subcuerpo de R.*

Este teorema justifica que, en el caso clásico, sea suficiente trabajar con cuerpos. En cambio, en el marco diferencial, el objeto que contiene las soluciones no necesariamente es un cuerpo, por lo que resulta natural trabajar con anillos. De hecho, aunque en esta memoria hemos mantenido el enfoque clásico, la teoría de Picard-Vessiot se puede plantear sobre anillos diferenciales simples, es decir, considerando ecuaciones diferenciales sobre este tipo de anillos en lugar de sobre cuerpos, ver [4].

Sin embargo, recordamos que los anillos de Picard-Vessiot son dominios por el Teorema 4.6 lo que nos permite considerar su cuerpo de fracciones.

Definición 4.20. Un cuerpo de Picard-Vessiot para la ecuación $y' = Ay$ sobre K (o para un módulo diferencial M sobre K) es el cuerpo de fracciones de un anillo de Picard-Vessiot para esta ecuación.

Existe una definición equivalente de cuerpo de Picard-Vessiot que habitualmente aparece en los textos sobre teoría de Galois diferencial. Para demostrar la equivalencia entre ambas definiciones haremos uso del siguiente lema.

Lema 4.21. *Sea L cualquier cuerpo diferencial con cuerpo de constantes C. La derivación denotada por $'$ sobre L se extiende a una derivación sobre $L[Y_{ij}, 1/\det]$ definiendo $Y'_{ij} = 0$ por el Teorema 2.17 para todos los $i, j \in \{1, 2, ..., n\}$. Se considera $C[Y_{ij}, 1/\det]$ como un subanillo de*

$L[Y_{ij}, 1/\det]$. *La aplicación del conjunto de ideales de* $C[Y_{ij}, 1/\det]$ *al conjunto de los ideales diferenciales de* $L[Y_{ij}, 1/\det]$ *que lleva cada ideal* I *en su extendido* (I) *es una biyección. La aplicación inversa está dado por* $J \to J \cap C[Y_{ij}, 1/\det]$.

Demostración. Elegimos una base $\{\ell_s\}_{s\in S}$, con $\ell_{s_0} = 1$, de L sobre C. Entonces $\{\ell_s\}_{s\in S}$ es también una base libre del módulo $L[Y_{ij}, 1/\det]$ como $C[Y_{ij}, 1/\det]$-módulo. El ideal (I) es diferencial porque los elementos de (I) son sumas finitas de productos $a_s\ell_s$ con $a_s \in I$ y al derivar uno de estos elementos se obtiene otro elemento de (I). Por lo tanto, se cumple que $(I) \cap C[Y_{ij}, 1/\det] = I$.
Terminamos la demostración mostrando que cualquier ideal diferencial $J \subset L[Y_{ij}, 1/\det]$ está generado por $I := J \cap C[Y_{ij}, 1/\det]$. Tomamos $\{e_b\}_{b\in B}$ una base de $C[Y_{ij}, 1/\det]$ sobre C. Cualquier elemento $f \in J$ puede escribirse de manera única como una suma finita como $f = \sum_b \ell_b e_b$ con $\ell_b \in L$. Denotaremos por la longitud $l(f)$ al número de b para los cuales $\ell_b \neq 0$. Veamos que $f \in (I)$ por inducción en la longitud de f. Cuando $l(f) = 0$ o $l(f) = 1$, el resultado es directo, porque $f = \ell_b e_b$ entonces f tiene la forma de un elemento de (I) porque $e_b \in C[Y_{ij}, 1/\det]$, $e_b = f/\ell_b \in I$.
Supongamos que $l(f) > 1$ y que la hipótesis es cierta para todo g con $l(g) < l(f)$. Podemos suponer que $\ell_c = 1$ para algún $c \in B$ y $\ell_d \in L \setminus C$ para algún $d \in B$. Entonces, tenemos que $f' = \sum_b \ell'_b e_b$ tiene una longitud menor que $l(f)$ y, por lo tanto por la hipótesis inductiva, pertenece a (I).
De manera similar, $(\ell_d^{-1} f)' \in (I)$. Por lo tanto, $(\ell_d^{-1})' f = (\ell_d^{-1} f)' - \ell_d^{-1} f'$, que está en (I). Dado que C es el cuerpo de constantes, $\ell'_d \neq 0$, y por lo tanto, $f \in (I)$. ■

Gracias a este lema auxiliar y al Lema de Zariski (ver [1]) podemos caracterizar los cuerpos de Picard-Vessiot.

Teorema 4.22. *Sea* $y' = Ay$ *una ecuación diferencial matricial sobre* K *y sea* $L \supset K$ *una extensión de cuerpos diferenciales. El cuerpo* L *es un cuerpo de Picard-Vessiot para esta ecuación si y solo si se satisfacen las siguientes condiciones:*

(I) El cuerpo de las constantes de L *es* C.

(II) Existe una matriz fundamental $F \in GL_n(L)$ *para la ecuación.*

(III) L *está generado sobre* K *por las entradas de* F.

Demostración. Si L es el cuerpo de fracciones del anillo de Picard-Vessiot, entonces por el Teorema 4.18, cumple (I) y por ser el cuerpo de fracciones cumple (II) y (III).

Recíprocamente, si L es una extensión diferencial de K que cumple estas condiciones (I),(II) y (III) veamos que es el cuerpo de fracciones del anillo de Picard-Vessiot.
Como en el Teorema 4.18, consideramos el anillo diferencial $R_0 = K[X_{ij}, 1/\det]$ con derivada $(X'_{ij}) = A(X_{ij})$. Consideramos la extensión de anillos diferenciales dada por la expresión $R_0 \subset L \otimes_K R_0 = L[X_{ij}, 1/\det]$. Definimos un conjunto de n^2 nuevas variables Y_{ij} que cumplen que $(X_{ij}) = F \cdot (Y_{ij})$, donde F es la matriz dada por (II). Entonces, como $F \in \mathrm{GL}_n(L)$ se tiene que $L \otimes_K R_0 = L[Y_{ij}, 1/\det]$ para todos $i, j \in \{1, ..., n\}$ y como F es una matriz fundamental,

$$\begin{aligned} Y'_{ij} &= (F^{-1}X_{ij})' = (F^{-1})'X_{ij} + F^{-1}X'_{ij} = -F^{-1}F'F^{-1}X_{ij} + F^{-1}AX_{ij} \\ &= -F^{-1}AFF^{-1}X_{ij} + F^{-1}AX_{ij} = 0. \end{aligned}$$

Tomamos P un ideal diferencial maximal de R_0 y consideramos el ideal que genera en $L \otimes_K R_0$, denotado por (P). Dado que $L \otimes_K R_0/(P) \simeq L \otimes_K (R_0/P) \neq \{0\}$, el ideal (P) es un ideal diferencial propio. Como $L \otimes_K R_0 = L[Y_{ij}, 1/\det]$ y, por (I), $L \otimes_C C[Y_{ij}, 1/\det] = L[Y_{ij}, 1/\det]$ identificamos $L \otimes_K R_0$ con $L \otimes_C R_1$ donde definimos $R_1 := C[Y_{ij}, 1/\det]$. Definimos el ideal $\tilde{P} \subset R_1$ por $\tilde{P} = (P) \cap R_1$. Como $Y'_{ij} = 0$, por el Lema 4.21, el ideal (P) está generado por $\tilde{P}$. Si M es un ideal maximal de R_1 que contiene $\tilde{P}$, entonces por el Lema de Zariski $R_1/M = C$. El homomorfismo de paso al cociente en M de C-álgebras $R_1 \to C$ se extiende a un homomorfismo diferencial de L-álgebras $L \otimes_C R_1 \to L \otimes_C C = L$. El núcleo de este homomorfismo contiene a $(P) \subset L \otimes_K R_0 = L \otimes_C R_1$. Por lo tanto, componiéndolo con la inclusión $R_0 \subset L \otimes_K R_0$, tenemos un homomorfismo diferencial $\psi : R_0 \to L$ que cumple que $P \subset \ker(\psi)$. El núcleo de ψ es un ideal diferencial (ver Lema 4.4), y por la maximalidad, $P = \ker(\psi)$.
El subanillo $\psi(R_0) \subset L$ es isomorfo a R_0/P y, por lo tanto, es un anillo de Picard-Vessiot. La matriz $(\psi(X_{ij}))$ es una matriz fundamental en $\mathrm{GL}_n(L)$ y debe tener la forma $F \cdot (c_{ij})$ con $(c_{ij}) \in \mathrm{GL}_n(C)$, porque el cuerpo de las constantes de L es C. Por (III) L está generado sobre K por los coeficientes de F, luego se tiene que L es el cuerpo de fracciones de $\psi(R_0)$. Por lo tanto, L es un cuerpo de Picard-Vessiot para la ecuación. ■

Los cuerpos de Picard-Vessiot nos permiten hablar de extensiones de Picard-Vessiot.

Definición 4.23. Sea $K \subseteq L$ una extensión de cuerpos diferenciales. Se dice que L es una **extensión de Picard–Vessiot** de K si L es un cuerpo de Picard-Vessiot para una ecuación diferencial $y' = Ay$ con $A \in M_n(K)$.

Veamos que las extensiones de Picard-Vessiot generalizan las extensiones de Galois.

Teorema 4.24 (Extensiones de Galois finitas son extensiones de Picard-Vessiot)**.** *Sea L una extensión de Galois finita de K, con grupo de Galois* $= \mathrm{Aut}(L/K)$. *Entonces, L es una extensión de Picard-Vessiot de K.*

Demostración. Dado que L/K es una extensión de Galois finita, el Teorema 2.20 garantiza que la derivación en K se extiende de manera única a L.

Veamos la compatibilidad de la derivación con el grupo de Galois $= \mathrm{Aut}(L/K)$. Para todo $\sigma \in G$ y $v \in L$, definimos la función $f(v) = \sigma^{-1}(\sigma(v)')$. Se puede verificar que f es una derivación en L porque satisface

$$\begin{aligned} f(v+w) &= \sigma^{-1}((\sigma(v+w))') = \sigma^{-1}((\sigma(v)+\sigma(w))') = \sigma^{-1}(\sigma(v)'+\sigma(w)') \\ &= \sigma^{-1}(\sigma(v)') + \sigma^{-1}(\sigma(w)') = f(v) + f(w). \\ f(vw) &= \sigma^{-1}((\sigma(vw))') = \sigma^{-1}((\sigma(v)\sigma(w))') = \sigma^{-1}(\sigma(v)'\cdot\sigma(w) + \sigma(v)\cdot\sigma(w)') \\ &= \sigma^{-1}(\sigma(v)')\cdot\sigma^{-1}(\sigma(w)) + \sigma^{-1}(\sigma(v))\cdot\sigma^{-1}(\sigma(w)') = f(v)\cdot w + v\cdot f(w). \end{aligned}$$

Por unicidad de la derivación, concluimos que $f(v) = v'$, es decir, $\sigma(v') = \sigma(v)'$, los automorfismos de G son diferenciales.

Como L/K es finita, existe un conjunto finito de elementos $w_1, \ldots, w_m \in L$ tal que escribimos $L = K(w_1, \ldots, w_m)$, y el grupo G permuta estos generadores. Por tanto, el espacio vectorial V generado sobre C por los w_i es invariante por la acción de G, es decir, para cada $v \in V$, $\sigma(v) \in V$.

Tomamos $\{v_1, \ldots, v_n\}$ una base de V sobre C, y consideramos $W = W(v_1, ..., v_n)$ la matriz Wronskiana. Calculamos $\sigma(W)$ aplicando σ a cada una de las entradas de W para un $\sigma \in G$

$$\sigma(W) = \begin{pmatrix} \sigma(v_1) & \cdots & \sigma(v_n) \\ \sigma(v_1') & \cdots & \sigma(v_n') \\ \vdots & & \vdots \\ \sigma(v_1^{(n-1)}) & \cdots & \sigma(v_n^{(n-1)}) \end{pmatrix} = \begin{pmatrix} \sigma(v_1) & \cdots & \sigma(v_n) \\ \sigma(v_1)' & \cdots & \sigma(v_n)' \\ \vdots & & \vdots \\ \sigma(v_1)^{(n-1)} & \cdots & \sigma(v_n)^{(n-1)} \end{pmatrix}.$$

Como V es invariante por G, $\sigma(v_j)$ es una combinación lineal sobre C de $v_1, v_2, ..., v_n$, luego existe $A_\sigma \in M_n(C)$ tal que $(\sigma(v_1), \sigma(v_2), ..., \sigma(v_n)) = (v_1, ..., v_n)A_\sigma$. Observamos que esta ecuación nos da una igualdad entre la primera fila de $\sigma(W)$ y la primera fila de WA_σ. Derivando A_σ, que es una matriz de constantes, $(\sigma^{(j)}(v_1), ..., \sigma^{(j)}(v_n)) = (v_1^{(j)}, ..., v_n^{(j)})A_\sigma$ para cada $j \in \{0, ..., n-1\}$, luego $\sigma(W) = WA_\sigma$.

Además, los vectores $v_1, \ldots, v_n$ son linealmente independientes sobre C, por lo que su Wronskiano no se anula $\det(W) \neq 0$ (Lema 3.16). Por tanto, W es invertible.

Para probar que L es una extensión de Picard-Vessiot de K debemos construir la ecuación diferencial asociada. Consideramos la matriz $B := W'W^{-1}$. Al derivar $\sigma(W) = WA_\sigma$, se

obtiene $\sigma(W)' = W'A_\sigma + WA'_\sigma$. Multiplicando por $\sigma(W)^{-1} = A_\sigma^{-1}W^{-1}$ se deduce que

$$\sigma(B) = \sigma(W')\sigma(W^{-1}) = (\sigma(W))'\sigma(W)^{-1} = (W'A_\sigma + WA'_\sigma)A_\sigma^{-1}W^{-1} = B + WA'_\sigma A_\sigma^{-1}W^{-1}.$$

Como A_σ tiene entradas constantes, es decir, en C, se tiene que $A'_\sigma = 0$, y por tanto como $\sigma(B) = B$ para todo $\sigma \in G$, tenemos que las entradas de B permanecen fijas para todos los automorfismos de G luego necesariamente están en el cuerpo base K, es decir, $B \in M_n(K)$.

Además, como $W' = BW$, la matriz $W \in \mathrm{GL}_n(K)$ es una matriz fundamental para la ecuación diferencial matricial $y' = By$, con $B \in M_n(K)$.
Conclusión como L está generado por las entradas de W sobre K, el cuerpo de constantes de L sobre K es C por la Proposición 2.19 y por ser C algebraicamente cerrado, entonces por el Teorema 4.22, se concluye que L es el cuerpo de Picard-Vessiot de la ecuación. ■

Podría parecer que la construcción de la ecuación diferencial realizada en el teorema anterior es arbitraria, sin embargo, resulta natural si se emplea el lenguaje de módulos diferenciales.

Corolario 4.25. *Sea L una extensión de Galois finita de K. Construimos el K-módulo diferencial $M = L$ y ∂ la única derivación sobre L que extiende a la derivación de K. Entonces L es el cuerpo de Picard-Vessiot del módulo diferencial (M, ∂).*

Demostración. Usaremos la caracterización de la Proposición 4.12. En primer lugar, queremos ver que se tiene que $\ker(\partial, L \otimes L)$ tiene dimensión $n = [L : K]$ sobre C. Como L/K es una extensión de Galois finita, hay un isomorfismo Φ de $K-$álgebras, $\Phi : L \otimes L \to \prod_{\sigma\in G} L$ dado por $\Phi(v \otimes w) = (\sigma(v)w)_{\sigma\in G}$.
Como $\prod_{\sigma\in G} L \simeq L^n$ puesto que $n = [L : K] = |G|$, tomamos una base canónica $e_1, ..., e_n$ de L, el producto en L^n se define coordenada a coordenada $e_i^2 = e_i$ para cada $i \in \{1, ..., n\}$. En otras palabras, $L \otimes L \simeq Le_1 \oplus Le_2, ... \oplus Le_n$ con $e_i^2 = e_i$.

Observamos que si e es un elemento idempotente de $L \otimes L$, es decir, $e^2 = e$, entonces $\partial(e^2) = \partial(e)$, luego $(2e-1)\partial(e) = 0$. Como $1 = (1, 1, ..., 1)$, $2e_i - 1 \neq 0$ y deducimos que $\partial(e) = 0$.

Por consiguiente, cada e_i está en el núcleo de ∂, y son linealmente independientes sobre C. Por tanto, $\ker(\partial, L \otimes L)$ tiene dimensión n sobre C. En segundo lugar, como en el teorema anterior, probamos que C es el cuerpo de constantes de L usando que es algebraicamente cerrado.

Se comprueba también que si $\tilde{L}$ es un subcuerpo propio de L que contiene a K, se tiene que $\tilde{L} \otimes L \simeq \prod_{\sigma\in\tilde{G}} L$ con $\tilde{G} = Gal(\tilde{L}/K)$. Como $[\tilde{L} : K] = m < n$, $\ker(\partial, \tilde{L} \otimes L)$ tiene dimensión menor que n, luego no es una extensión de Picard-Vessiot de K porque no contiene todas las proyecciones e_i. ■

4.4. Introducción al Grupo Diferencial de Galois

En esta sección introducimos el grupo diferencial de Galois de una ecuación diferencial lineal en forma matricial, o en forma de módulo, y desarrollamos la teoría para demostrar algunas de sus principales características.

Definición 4.26. El grupo Galois diferencial de una ecuación $y' = Ay$ sobre K, o de un módulo diferencial sobre K, se define como el grupo $\mathrm{DGal}(R/K)$ de los automorfismos de la K-álgebra diferencial de un anillo Picard-Vessiot R para la ecuación. Más precisamente, $\mathrm{DGal}(R/K)$ consiste en los automorfismos de R que cumplen la relación $\sigma(f') = \sigma(f)'$ para todo $f \in R$.

Como hemos visto en el Teorema 4.24, una extensión Galois finita L/K es el anillo Picard-Vessiot de una cierta ecuación diferencial matricial sobre K. Observamos que este teorema también establece que el grupo Galois ordinario de L/K coincide con el grupo Galois diferencial. Sin embargo, existen extensiones de Picard-Vessiot que no son extensiones de Galois, es decir, el grupo de automorfismos y el grupo de automorfismos diferenciales pueden ser distintos, porque podrían aparecer automorfismos que no respetan la derivación.

Por ejemplo, $\mathbb{C}(z, e^z)$ extensión de $\mathbb{C}(z)$ construida con $(e^z)' = e^z$ como en el Ejemplo 4.15 es de Picard-Vessiot pero no es de Galois porque no es algebraica.
De hecho, se puede probar que $\mathrm{Aut}(\mathbb{C}(z, e^z)/\mathbb{C}(z)) \simeq \mathrm{PGL}_2(\mathbb{C}(z))$ donde $\mathrm{PGL}_2(\mathbb{C}(z))$ es el grupo lineal general proyectivo. Mientras que $\mathrm{DGal}(\mathbb{C}(z, e^z)/\mathbb{C}(z)) \simeq \mathbb{C}^*$.

Proposición 4.27. *Sea R una extensión de Picard-Vessiot de K fijamos una matriz fundamental $F \in M_n(R)$. Podemos identificar $DGal(R/K)$ como un subgrupo de $GL_n(C)$ enviando cada automorfismo $\sigma \in DGal(R/K)$ en la única matriz constante que cumple que $\sigma(F) = FC_\sigma$. Esto nos proporciona una representación inyectiva $\rho : DGal(R/K) \to GL(V)$ donde V es el espacio de soluciones de la ecuación.*

Demostración. El grupo Galois diferencial $G = \mathrm{DGal}(R/K)$ puede ser definido de la siguiente manera: como en la Proposición de caracterización 4.12, se considera el espacio de soluciones $V := \ker(\partial, R \otimes M)$. La acción K-lineal de G sobre R se extiende a una acción K-lineal sobre $R \otimes M$ de manera que $\sigma(r \otimes m) := \sigma(r) \otimes m$, la cual está bien definida porque σ fija K y respeta las relaciones de $R \otimes M$. Como σ es automorfismo diferencial, conmuta

con la derivación ∂, y en el producto tensorial se tiene $\partial(r\otimes m) = r'\otimes m + r\otimes\partial(m)$, entonces

$$\begin{aligned}\sigma\circ\partial(r\otimes m) &= \sigma(r'\otimes m + r\otimes\partial(m)) = \sigma(r')\otimes m + \sigma(r)\otimes\partial(m)\\ &= (\sigma(r))'\otimes m + \sigma(r)\otimes\partial(m) = \partial(\sigma(r\otimes m)).\end{aligned}$$

Por ello, si restringimos la acción de G sobre $R\otimes M$ a V, tenemos que induce una acción C-lineal sobre V. Por la Proposición 4.12 si fijamos una base de V sobre C y una base de M sobre K y F es la matriz que expresa la primera base en términos de la base de $R\otimes M$, entonces, R está generado sobre K por las entradas de F y el inverso del determinante de F. Calculamos la derivada de $F^{-1}\sigma(F)$ y vemos que

$$\begin{aligned}(F^{-1}\sigma(F))' &= (F^{-1})'\sigma(F) + F^{-1}(\sigma(F))' = -F^{-1}F'F^{-1}\sigma(F)' + F^{-1}(\sigma(F'))\\ &= -F^{-1}A\sigma(F) + F^{-1}\sigma(AF) = -F^{-1}A\sigma(F) + F^{-1}A\sigma(F) = 0,\end{aligned}$$

en la penúltima igualdad hemos usado que $\sigma(A) = A$ porque $A\in M_n(K)$. Por tanto, obtenemos que $C_\sigma = F^{-1}\sigma(F)$ es una matriz de $\mathrm{GL}_n(C)$ unívocamente determinada por F y σ. Por la Proposición 3.9, $\sigma(F)$ es una matriz fundamental de $y' = Ay$ y se define una aplicación $\rho : \mathrm{DGal}(R/K)\to\mathrm{GL}(V)$ dada por $\rho(\sigma) = C_\sigma$. Veamos que ρ es un homomorfismo de grupos inyectivo. Dados $\sigma_1,\sigma_2\in\mathrm{DGal}(R/K)$ tenemos que

$$C_{\sigma_1\circ\sigma_2} = F^{-1}\sigma_1\sigma_2(F) = F^{-1}\sigma_1(\sigma_2(F)) = F^{-1}\sigma_1(F\cdot C_{\sigma_2}) = F^{-1}\sigma_1(F)\cdot C_{\sigma_2} = C_{\sigma_1}\cdot C_{\sigma_2}$$

Para comprobar que es inyectivo observamos que si $C_\sigma = Id$, entonces $\sigma(F) = F$, como las entradas de F y el inverso del determinante de F generan R, entonces $\sigma(r) = r$ para todo $r\in R$. En conclusión, $\sigma = Id_R$ y ρ es inyectivo. ■

Observación 4.28. Podemos considerar también el grupo de Galois diferencial sobre el cuerpo de fracciones L de R que denotamos por $\mathrm{DGal}(L/K)$. Se puede comprobar que todo elemento de $\mathrm{DGal}(R/K)$ se extiende de manera única a un elemento $\mathrm{DGal}(L/K)$ y que todo elemento de $\mathrm{DGal}(L/K)$ procede de una de estas extensiones, luego se tiene que $\mathrm{DGal}(L/K)\simeq\mathrm{DGal}(R/K)$.

Para concluir la memoria vamos a enunciar el teorema fundamental de la Teoría de Galois Diferencial, tratando de entender los elementos que intervienen en él. Los grupos de Galois diferenciales resultan ser grupos algebraicos y la correspondencia del teorema se establece entre entre subgrupos cerrados para la topología Zariski y subcuerpos diferenciales. Para precisar la primera de estas nociones, recordamos algunos aspectos elementales de la geometría algebraica. Dado que no es el tema fundamental de esta memoria incluimos los resultados sin demostración, para más información ver [8].

Definición 4.29. Un subconjunto cerrado de la topología de Zariski $V \subset K^n$ se llama una **variedad definida sobre** K, o una K**-variedad**, si es el conjunto de ceros comunes de un conjunto de polinomios en $K[X_1, \ldots, X_n]$. Sea $S \subseteq K[X_1, \ldots, X_n]$ un subconjunto de polinomios. El conjunto de ceros de S en K^n se denota por:

$$V(S) = \{X \in K^n \mid f(X) = 0 \text{ para todo } f \in S\}.$$

Lema 4.30. *El conjunto de ceros de S en K^n solo depende del ideal generado por S, es decir, $V(S) = V((S))$, donde (S) es el ideal generado por S.*

Definición 4.31. Dado un subconjunto $U \subseteq K^n$, el **ideal de polinomios que se anulan en** U se define por

$$I(U) = \{f \in K[X_1, \ldots, X_n] \mid f(X) = 0 \text{ para todo } X \in U\}.$$

Por lo tanto, tenemos una correspondencia entre los ideales de $K[X_1, \ldots, X_n]$ y los subconjuntos algebraicos de K^n que está dada por $I \mapsto V(I)$, y $V \mapsto I(V)$, donde I es un ideal en $K[X_1, \ldots, X_n]$ y V es un subconjunto algebraico de K^n. La correspondencia se trata de una biyección si y solo si K es un cuerpo algebraicamente cerrado.

La demostración se sigue del siguiente teorema que podemos encontrar en [1].

Teorema 4.32. *Teorema de los Ceros de Hilbert (Nullstellensatz)*

1. *Si $I \subseteq K[X_1, \ldots, X_n]$ es un ideal propio, es decir, $I \neq K[X_1, \ldots, X_n]$, entonces el conjunto de ceros $V(I)$ es no vacío $V(I) \neq \emptyset$.*

   Es decir, todo sistema de ecuaciones polinómicas no trivial tiene una solución en K^n.

2. *Sea $I \subseteq K[X_1, \ldots, X_n]$ un ideal. Entonces, el ideal de todos los polinomios que se anulan en el conjunto de ceros de I es igual al radical de I, es decir $I(V(I)) = \sqrt{(I)}$. donde $\sqrt{(I)}$ es el radical de I, es decir, el conjunto de todos los polinomios f tales que algún $f^m \in I$ para algún $m \in \mathbb{N}$.*

Volviendo al estudio del grupo de Galois diferencial, podemos definir los subgrupos algebraicos de matrices.

Definición 4.33. Sea K un cuerpo diferencial con cuerpo de constates C algebraicamente cerrado. Un subgrupo $G \subset \mathrm{GL}_n(C)$ se dice que es algebraico si es el conjunto de ceros de un ideal $I \subset C[X_{ij}]$.

Con la identificación de $\mathrm{DGal}(R/K)$ como subgrupo de $\mathrm{GL}_n(C)$ tenemos el siguiente resultado.

Proposición 4.34. *Sea R un anillo de Picard-Vessiot de K entonces $DGal(R/K)$ es un subgrupo algebraico de $GL_n(C)$.*

Demostración. Por los teoremas de existencia y unicidad del anillo de Picard-Vessiot sabemos que podemos escribir $R = K[X_{ij}, 1/\det]/I$ donde $I = (f_1, ..., f_n)$ es un ideal diferencial maximal de $K[X_{ij}, 1/\det]$ y podemos asumir que $f_i \in K[X_{ij}]$ porque det es una unidad. Empleando la representación matricial de $\mathrm{DGal}(R/K)$, podemos identificar este grupo con el conjunto

$$\{M \in \mathrm{GL}_n(C) : \sigma_M(I) \subset I\} \tag{4.2}$$

donde $\sigma_M \in K[X_{ij}, 1/\det]$ está dado por $\sigma_M(X_{ij}) = (X_{ij})M$. Tenemos que define un conjunto algebraico en $\mathrm{GL}_n(C)$. Tomamos una base $\{e_s\}_{s\in S}$ de R sobre C, vemos que se tiene que $\sigma_M(f_k)+I \in R$ puede expresarse como una suma finita $\sum_s C(M,k,s)e_s$ para cada $k \in \{1, ..., n\}$ con $C(M,k,s) \in C$ dependientes de M. Observamos que $\sigma_M(I) \subset I$ si y solo si $C(M,k,s) = 0$ para cada $k \in \{1, ..., m\}$ y cada s en un subconjunto finito de S.
Se comprueba que $C(M,k,s)$ es una expresión polinomial en las entradas de M con coeficientes en C por como se construye el automorfismo σ_M. ■

Por la Observación 4.28 $\mathrm{DGal}(R/K) \simeq \mathrm{DGal}(L/K)$ y por lo tanto $\mathrm{DGal}(L/K)$ es también un subgrupo algebraico de $\mathrm{GL}_n(C)$.

En general el cálculo del grupo de Galois diferencial no es sencillo pero empleando (4.2) podemos describirlo en algunos ejemplos sencillos.

Ejemplo 4.35. 1. Sea $K = \mathbb{C}(z)$ con la derivación usual y consideremos la ecuación diferencial $y' = (\alpha/z)y$, cuyo grupo diferencial de Galois $\mathrm{DGal} \subset \mathrm{GL}_1(\mathbb{C})$.

Según la descripción del grupo de Galois diferencial como el grupo que deja invariante cierto ideal diferencial (ver Ejemplo 4.17), distinguimos dos casos:

(a) Caso 1: $\alpha = n/m \in \mathbb{Q}$ y $mcd(n,m) = 1$. En este caso, el anillo de Picard-Vessiot era $R = \mathbb{C}(z)\left[T, T^{-1}\right]/(T^m - z^n)$. y entonces el grupo de Galois diferencial es isomorfo a $\mathbb{Z}/m\mathbb{Z} \simeq \{(c) | c^m - 1 = 0\} \subset \mathrm{GL}_1(\mathbb{C})$.

(b) Caso 2: $\alpha \notin \mathbb{Q}$. En este caso el anillo de Picard-Vessiot era $R = \mathbb{C}(z)[T, T^{-1}]$, con $T' = (\alpha/z)T$ y el grupo de Galois diferencial es entonces todo $\mathrm{GL}_1(\mathbb{C})$, es decir, $\mathrm{DGal} = \mathrm{GL}_1(\mathbb{C})$.

2. Consideramos la ecuación diferencial $y' = y$ sobre $K = \mathbb{C}(z)$ con derivada usual. Como antes, se puede comprobar que el grupo de Galois diferencial es $\mathrm{DGal} = \mathrm{GL}_1(\mathbb{C})$.

Teorema 4.36 (Teorema Fundamental de la Teoría de Galois Diferencial)**.** *Sea K un cuerpo diferencial con cuerpo de constantes algebraicamente cerrado C. Sea L una extensión de Picard-Vessiot de K, con grupo de Galois diferencial $G = \mathrm{DGal}(L/K)$. Entonces*

1. *Existe una correspondencia biyectiva entre los subgrupos cerrados de Zariski $H \subseteq G$ y los subcuerpos diferenciales F tales que $K \subseteq F \subseteq L$, dada por:*

$$H \mapsto L^H = \{a \in L \mid \sigma(a) = a \text{ para todo } \sigma \in H\},$$

$$F \mapsto \mathrm{DGal}(L/F) = \{\sigma \in G \mid \sigma(a) = a \text{ para todo } a \in F\}.$$

2. *Un subcuerpo diferencial F, con $K \subseteq F \subseteq L$, es una extensión de Picard-Vessiot de K si y solo si* $\mathrm{DGal}(L/F)$ *es un subgrupo normal de G. En tal caso, se tiene:*

$$\mathrm{DGal}(F/K) \simeq G/\mathrm{DGal}(L/F).$$

Ejemplo 4.37. Consideremos la ecuación diferencial $y' = (\alpha/z)y$ del caso dos del ejemplo anterior, es decir, $\alpha \notin \mathbb{Q}$ sobre el cuerpo $K = \mathbb{C}(z)$. El anillo de Picard-Vessiot R se corresponde con $R = \mathbb{C}(z)[T, T^{-1}]$ y su cuerpo de fracciones es $K(z^\alpha)$, luego $\mathrm{DGal} = \mathrm{GL}_1(\mathbb{C}) = \mathbb{C}^*$. Como los subconjuntos cerrados para la topología de Zariski de $\mathbb{C}^*$ son finitos y los elementos de orden finito de $\mathbb{C}^*$ son raíces de la unidad, deducimos que los subgrupos cerrados de $\mathrm{GL}_1(\mathbb{C}) = \mathbb{C}^*$ son cíclicos y finitos. Esto da lugar a una correspondencia entre subgrupos cerrados del grupo de Galois y extensiones diferenciales intermedias del cuerpo de Picard-Vessiot:

Grupos	$\Longleftrightarrow$	**Cuerpos**
$\{1\}$	$\Longleftrightarrow$	$K(z^\alpha)$
$\cap$	$\Longleftrightarrow$	$\cup$
$\{1, e^{2\pi i/n}, \ldots, e^{2(n-1)\pi i/n}\}$	$\Longleftrightarrow$	$K(z^{n\alpha})$
$\cap$	$\Longleftrightarrow$	$\cup$
$\mathbb{C}^*$	$\Longleftrightarrow$	K

BIBLIOGRAFÍA

[1] M. Atiyah y I. MacDonald. *Introducción al álgebra conmutativa*. Reverté, 1973.

[2] M. A. Barkatou. «An Algorithm for Computing a Companion Block Diagonal Form for a System of Linear Differential Equations». En: *Journal of Symbolic Computation* (1993).

[3] J. A. Gallian. *Contemporary Abstract Algebra*. 2nd. Lexington, Massachusetts: D. C. Heath y Company, 1990.

[4] A. Maurischat. «Picard–Vessiot theory of differentially simple rings». En: *Journal of Algebra* 404 (2014).

[5] E. Picard. *Traité d'analyse, tome 1*. French. Gauthier-Villars, 1891.

[6] M. van der Put y M. F. Singer. *Galois Theory of Linear Differential Equations*. Vol. 328. Grundlehren der mathematischen Wissenschaften. Berlin: Springer, 2002.

[7] J. F. Ritt. *Differential Algebra*. American Mathematical Society, 1950.

[8] M.F Singer. *Introduction to the Galois Theory of Linear Differential Equations*. Expanded version of the 2006 London Mathematical Society Invited Lecture Series, Heriot-Watt University, July 31–August 4, 2006. 2006.

[9] E. Vessiot. «Sur l'intégration des équations différentielles linéaires». Thèse de doctorat ès sciences mathématiques. Paris: Faculté des Sciences de Paris, 1892.